Guihua Zeng

Quantum Private Communication

高等教育出版社
HIGHER EDUCATION PRESS

Guihua Zeng

Quantum Private Communication

Guihua Zeng

Quantum Private Communication

With 96 Figures

高等教育出版社
HIGHER EDUCATION PRESS

Springer

Author
Prof. Guihua Zeng
Department of Electronic Engineering
Shanghai Jiaotong University
Shanghai, 200240, China
E-mail: ghzeng@sjtu.edu.cn

ISBN 978-7-04-025479-2
Higher Education Press, Beijing

ISBN 978-3-642-03295-0 e-ISBN 978-3-642-03296-7
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2009931055

Cover design: Frido Steinen-Broo, EStudio Calamar, Spain

Printed on acid-free paper

Springer is part of Springer Science + Business Media (www.springer.com)

This book is dedicated to my family

Preface

Since Wiesner first found that quantum laws may be applied for protecting legitimate information in 1969, the quantum cryptology — a combination of the quantum physics and classic cryptology — has attracted much attention since then. With further investigations, the infrastructure of the quantum cryptology has become more and more clear. To conclude these research results, some excellent books have been devoted to describe various aspects of the quantum cryptology, such as the *Quantum computation and quantum information* by Nielsen and Chuang, *Quantum cryptography and secret-key distillation using quantum cryptography* by Assche, and *Quantum cryptology* by Zeng. As a main application direction of the quantum cryptology, the quantum private communication which combines the quantum cryptology and communication techniques has recently made great progress. By far, various investigations on this aspect have been presented, even some techniques have been applied in practices. This means that the quantum private communication has entered gradually the commerce field. This book devotes to describe fundamental principles, typical schemes, and technical implementations for the quantum private communication.

Because the quantum private communication has currently become a practical reality with products available commercially, it is important to focus not only on the theoretical topics but also on the practical issues. Accordingly, this book arranges the contents from pure theoretical descriptions to practical applications. To reach this aim, a broad range of materials are covered in this book, including how to protect confidentiality and authentication of the private communication using quantum tools and typical techniques for practical applications of quantum private communication in fiber telecommunication systems, wireless optical communication (including satellite communication), IP networks, and mobile communication systems, etc. Consider that cryptology, quantum physics, and information theory are necessary ingredients to build framework of the quantum private communication, brief introduction on these issues is employed to make the book self-consistent.

This book originated out of a graduate course of lectures in Quantum Secure Communication given at the Shanghai Jiaotong University. The content of this book is based on my investigations on the quantum cryptography as well as the quantum private communication since 1997. It aims at giving an introduction on fundamental principles, typical schemes, technical

implementations, and practical applications of the private communication in quantum ways. Since the quantum cryptography, and subsequently the quantum private communication is a multi-disciplinary subject, in this respect it may benefit readers with various backgrounds. Thus, this book is suitable for researchers and graduate students in the field of quantum cryptography, classic cryptography, communication engineering, computer science, electronic engineering, quantum physics, and mathematics, etc.

This book addresses systemically some hot topics in the private communication implemented using quantum techniques from fundamental theories to practical application techniques. It contains 9 chapters. Chapter 1 tries to build a quantum private communication model by analogy with the Shannon private communication theory. Then an overview of the quantum private communication is presented. Chapter 2 constructs a quantum security theory which is an important fundament for the quantum private communication. Chapter 3 introduces some preliminaries from the viewpoint of quantum bits, which are associated with basic principles of quantum mechanics. Chapter 4 introduces the well-known quantum key distribution which has been investigated widely. Chapter 5 investigates how to protect the confidentiality using quantum cryptographic algorithms. Chapter 6 demonstrates fundamental principles of implementing quantum authentication, including identity verification, message authentication, quantum signature, and channel authentication. Both Chapters 7 and 8 introduce how to implement physically the quantum private communication using single photon signal and continuous variable quantum signals, respectively. Finally, typical quantum private communication systems in practices are introduced in Chapter 9.

Logically, embodied contents in this book may be divided into three parts, i.e., fundamentals, quantum cryptographic schemes, and technical implementations in practical communication systems. Chapters 1 – 3 consist of the first part which is engaged in building a basic theory model for the quantum private communication from three aspects including information theory, complexity theory, and security theory. To make the book self-consistent, some quantum mechanics principles and mathematical backgrounds are introduced briefly. For those readers who have knowledge on these aspects, one may skip the corresponding sections. Chapters 4 – 6 are regarded as the second part which focuses on discussing how to protect basic security requirements, i.e., confidentiality and authentication, of the modern communication system using quantum techniques. To reach this aim, three aspects are addressed in this part. Since protecting the confidentiality and authentication of the private communication using quantum tools needs firstly to generate a keypair, the quantum key management is introduced in Chapter 4. This topic is actually a main research issue in the quantum private communication. After that some typical quantum encryption algorithms and quantum authentication schemes are described in this part. Chapters 7 – 9 consist of the final part which focuses on the technical implementations of the quantum private communication in practices. According to the current development, the quantum

private communication may be applied possibly in the fiber telecommunication, wireless optical communication, IP networks, and mobile communication systems. All these applications are briefly introduced. Each of the three parts in the book is self-consistent. Accordingly, they may be also regarded as independent parts, respectively. Readers may only read the parts interested although the author recommends to read throughout this book. This will not influence the understanding on the corresponding contents.

Guihua Zeng
Shanghai, November 2009

Acknowledgements

I would like to thank many researchers and collaborators who have worked on the research projects as described in this book. They have supplied research results, thoughts, advices, challenges, criticisms, suggestions, or help that have influenced my writing of the book. Especially, Dr. Guangqiang He and Dr. Jin Xiong, who are my staff and long-term cooperators, contribute their thoughts and research results for the book. In addition, Dr. Guangqiang He has checked carefully Chapter 8. While discussions with Prof. Zhiming Zhang, Prof. Weiping Zhang, Prof. Zhongyang Wang, and Prof. Chun Jiang motivate my further considerations on some key issues on the quantum private communication and quantum information processing. Prof. Hiroki Takesue, Prof. Markus Aspelmeyer, and Prof. Gerald S.Buller etc. provide kindly their original figures for me. Mr. Jun Zhu, Mr. Yuan Lu, and Mr. Hu Li who are my students help me to type or plot some figures. All these have improved the organization, readability, and overall quality of this book immeasurably. I apologize if I have forgotten to mention someone else; the oversight is accidental.

I would also like to take this opportunity to thank Mrs. Hongying Chen, Higher Education Press, for her great help in compiling this book. In addition, her help in correcting grammatical mistakes have improved the readability of this book.

If someone alleges to have written a book alone, distrust the person immediately. While an author is working more than 12 hours a day on the writing of the book, someone else needs to see to all the other aspects of life, from simple things like food, clothing and shelter, to complex things like social and family responsibilities. My wife, Yuanyuan Qi, took the time from her professional schedule so that I could devote my full energy to writing. Therefore, it is with great pleasure that I dedicate this book to Yuanyuan, the other half of the team that caused this book to be written.

This book is supported by the Natural Science Foundation of China (No: 60773085, 60801051, 60970109) and NSFC-KOSEF international collaborative research funds (No: 60811140346, F01-2008-000-10021-0).

Contents

1 Introduction

An introduction on the quantum private communication is presented. Issues including security requirements of the modern communication, overview of the quantum private communication, and relationships among the quantum private communication and other disciplines are addressed. In addition, a communication model for the quantum private communication is built by analogy with the Shannon private communication model. Finally, some key notations and notions for the private communication are introduced.

The quantum private communication is a combination of the quantum cryptography and modern communication techniques such as the optical communication, mobile communication, and Internet network techniques. It provides a novel way for protecting the confidentiality and authentication of modern communication systems. Different from the classic private communication, the quantum private communication is closely associated with the physical characteristics of employed quantum signals and involved communication systems, and its security depends on the corresponding quantum physics laws, such as the well-known Heisenberg uncertainty principle and no-cloning theorem. Accordingly, quantum features have naturally become important ingredients in this scenario. In applications, the quantum private communication is always merged with the classic private communication due to limitations on current quantum technologies. Some technologies such as the message encryption using classic algorithm with quantum key distribution and quantum random number generation have become practical in commercial applications. This chapter presents an overview on the quantum private communication and builds a quantum private communication model. The aim is to outline the infrastructure of the quantum private communication from both the theory and the implementation.

1.1 Security Requirements of Communication

Communication is a widely used word in our daily life and engineering. For example, when two persons talk about something, the communication between them for information exchange occurs. Actually, the communication exists everywhere and everytime in activities of the human being. Subse-

quently, the communication has become an interesting topic in many situations.

This book focuses on communication topics where the communication is as an academic subject like physics, chemistry, maths, etc. In this sense, the communication is regarded as an important component of the well-known information science. It is doubtless that the communication plays significant role in the information era. From the viewpoint of information science, the communication is defined as a whole procedure of information generation, processing, transmission, and receiving [**?**]. Generally, the information is represented with a message while the message is encoded into a set of suitable codewords. Then the encoded message (information) is carried by a proper signal for the transmission and processing. The employed signal may be variously physical forms, e.g., optical signals, electromagnetic signals, etc.

Any message exchange procedure is associated with a communication system. With the rapid development of communication technologies and computing technologies, communication systems and the associated communication information processing technologies have been used widely in engineering, commerce and our daily life. Currently, the optical fibre communication system and the wireless communication system are two mainstream ways in the modern communication field. The optical fiber communication uses telecommunication fiber as physical channel, and the transmitted signal is laser light with telecommunication wavelengths, e.g., 1310 nm and 1550 nm. The wireless communication is a topic which includes both radio communication and wireless optical communication. The wireless optical communication is also called the free space optical communication. This kind of optical communication is employed in some special cases which are difficult to pave fiber. For example, the communications in outer space and water, and the communication bestriding a canyon may use the wireless optical communication techniques. Different from the optical fiber communication system, there are no fixed physical channels in the wireless optical communication system. Surely, the wireless communication is commonly implied to the radio communication which uses radio signals to carry the message. This way of communication has been developed rapidly and widely used in our daily life. With the development of communication technologies, both the optical fiber communication and wireless communication have become more and more integrated. For example, the wireless communication system is often used as an access network in the optical fiber communication network system. Especially, the recently developed technique of "radio over fiber" is just a combination of optical fiber communication systems and wireless radio communication systems [**?**], and this technique has been adopted in some commercial communication systems.

As usual, if the transmitted signal in a communication system is the classic signal which obeys the classic physics laws, this kind of communication is called the classic communication. While if the transmitted signal obeys the quantum physics laws, this way is naturally called the quantum communica-

tion [**?**]. It is well-known that the classic communication has been investigated widely and played important roles in the modern communication field. The quantum communication has also attracted much attention since 1990s in the last century [**?**, **?**]. By far, it has become an interesting issue in the communication field. Generally, both a classic communication system and a quantum communication system consist of the message source, channel, and message sink. Their availability and creditability are ensured by coding techniques and secure techniques, respectively.

Performance is an important parameter for a classic communication system or a quantum communication system in the modern communication. To reach an optimal performance one has to ensure at least the availability of the communication system. Usually, the availability is associated with the communication quality which is used to be called the quality of service (briefly called QoS). To guarantee the optimal availability of the communication system, one should depress noise's influences so that the efficient signal can be distilled from a received signal which has a strong noise background. For the sake of finical request and efficiency, the data from the source should be encoded which is called the source encoding. Subsequently, the encoded source should be decoded at the sink side which is called the source decoding. To guarantee the availability of the message transmitted in the channel, a so-called channel encoding and subsequently a channel decoding must be necessary at the transmitter and receivers, respectively. Except for the above operations, other techniques such as modulation and demodulation, are also needed in a communication system. In summarization, an available communication system is always described using the well-known Shannon communication model as shown in Fig.1.1 [**?**]. Note, this communication model is suitable for classic communication systems as well as quantum communication systems.

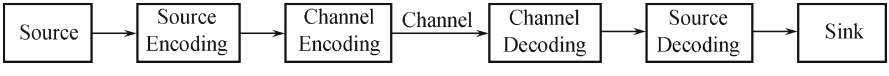

Fig. 1.1. Shannon communication model

Suppose arbitrated two legitimate communicators, i.e., Alice and Bob, want to exchange their information through a communication system. If transmitted messages may be public, which means each communicator may know the content of messages, they can communicate directly with the communication model in Fig.1.1. However, if exchanged messages are secret between Alice and Bob, then such communication is not available since anyone may read easily messages. In this case Alice and Bob would like to let their messages be transmitted privately since transmitted messages contain their secrecy or privacy. Any discovery of the secrecy of transmitted messages may harm communicators' benefits. In addition, illegitimate communicator, called Oscar, will try to forge Alice and Bob's legitimate messages which

are transmitted in the channel so that the attacker — Oscar may benefits himself through forged messages. Especially with the fast development of e-business the security requirements for the modern communication become importunate. However, this problem cannot be automatically solved by communication itself. Obviously, to ensure the legitimate communication between Alice and Bob be secure, a communication with security protection tools is necessary. Such a way is called the secure communication or private communication. Subsequently, to take on the creditability of communication system, one should build a secure communication system.

Generally, to ensure the creditability of a communication system, two aspects, i.e., the confidentiality and authentication should be involved [**?**]:

- *Confidentiality*: When transmitting a message in a communication channel, one does not want an eavesdropper to understand contents of transmitted messages, i.e., transmitted messages should be private.
- *Authentication*: The receiver of a message wants proof that a message comes from a certain party and not from somebody else (even if the original party later wants to deny it), and the received message is not changed.

These two aspects, i.e., the confidentiality and authentication, are basic security requirements for modern communication systems. In principle, a communication system which may ensure the confidentiality and authentication is called the private communication system or the secure communication system. When these requirements are satisfied, the creditability of the communication system is guaranteed. Generally, the communication creditability depends on the capability of the involved communication system against various attack strategies of illegitimate communicators. This will be described in Chapter 2.

The classic private communication which combines the classic cryptology and classic communication techniques has provided a useful way to reach a secure communication way. However, drawbacks of the classic cryptology lead that the security of communication systems cannot be optimal or perfect. This motivates further investigations on new approaches. A promising approach is called the quantum private communication which makes use of quantum techniques to protect private communication procedures.

Analogy to the classic private communication one may define exactly the quantum private communication. That is, the quantum private communication is a combination of the quantum cryptology and modern communication techniques, where the quantum cryptology includes the quantum cryptography and quantum cryptanalysis which is similar to the classic cryptology [**?**]. Some researchers think that the quantum cryptography and quantum key distribution (QKD) are synonymous; however, others think that quantum cryptography also includes other applications of quantum mechanics related to the cryptography, such as the quantum secret sharing, quantum secure protocols, and quantum authentication, which have been investigated widely. To avoid confusion on these notations, we follow the conventional definition

in the cryptography since quantum cryptography is a new and important chapter in the history of the cryptography. Commonly, the quantum private communication is implemented using the quantum cryptology and communication technologies. In narrow definition, the quantum private communication is a special quantum communication which only involves pure quantum effects. In this book, we refer to a definition in wide way for the quantum private communication. That is, the quantum private communication means any secure communication way which involves quantum techniques. For example, when communicators Alice and Bob exchange their secret information via a classic way but the key is generated using quantum techniques, i.e., the well-known QKD scheme, then this kind of private communications is also called the quantum private communication. As mentioned in the above, the classic private communication cannot reach a perfect way for the security and applications in practices. Fortunately, some drawbacks in the classic private communication can be avoided in a quantum private communication system so that the later is more powerful. This is why the quantum private communication can exist even if the traditional private communication is much more mature and powerful.

1.2 Overview of Quantum Private Communication

As an alternative of the classic private communication, the quantum private communication may also guarantee the privacy (equally the confidentiality) and authentication of a communication system, and the resulting effects are more optimal in some situations, such as the security and detection abilities on eavesdroppers' operations. Especially, the quantum private communication may provide a more secure communication since the security is ensured by the quantum physical laws which cannot be broken currently. Generally, the security of the quantum private communication is associated with quantum cryptographic schemes, which have been proven that even if a future quantum computer cannot break such a kind of schemes. These security requirements are satisfied via quantum cryptosystems and quantum authentication systems.

To give a first tour on the quantum private communication we consider the following communication model. Suppose that there is a communication network, and arbitrated communicators Alice and Bob in this network want to communicate secretly via a quantum private communication system so that they can exchange a private message with strong security. This section shows how to implement the secure communication procedure via a quantum private communication way. Clearly, as mentioned above the privacy and authentication are two important ingredients for the secure communication. Thus, we firstly describe how to ensure the confidentiality and authentication of the communication via a quantum private communication system.

To ensure the confidentiality of a transmitted message, an appropriate cryptosystem is necessary. Making use of the chosen cryptographic algorithms the message is encrypted and decrypted, respectively, so that only legitimate communicators may know the confidentiality of transmitted messages while the eavesdropper or even the attacker cannot obtain valid information on transmitted messages. In the classic private communication, the employed cryptosystem may be categorized as symmetrical key cryptosystem and public key cryptosystem [**?**]. The symmetrical key cryptosystem uses same keys or a symmetrical key-pair to encrypt and decrypt transmitted messages. It includes stream cipher algorithm, block cipher algorithm, such as the Vernam cipher, the well-known data encryption standard (DES), and the current international standard algorithm, i.e., the advanced encryption standard (AES). The public key cryptosystem uses two different keys to encrypt and decrypt transmitted messages. One key is the public key while another key is the private key. Usually, the two keys construct a one-way map, but the security of this function depends on computational complexity theories. Accordingly, by far, all proposed public key algorithms in classic cryptology are computationally secure. Some typical public key algorithms are the Rivest, Shamir, and Adleman (RSA) algorithm, elliptic curve algorithm, etc.

Similar to the classic private communication, the confidentiality of transmitted messages is also ensured by the cryptosystem in the quantum private communication. However, the employed cryptosystem in this case is quantum algorithms. Currently, there are two typical approaches, in principle, to ensure the confidentiality of transmitted messages [**?**]. One way is to combine the classic cryptosystem and QKD scheme. Exactly, the encryption and decryption processes use classic algorithms such as the Vernam cipher, DES, AES, etc., while the employed key for the message encryption and decryption which play important roles in the cryptosystem comes from the well-known QKD scheme. For example, when Alice sends her secret messages to Bob, they may choose the well-known classic Vernam cipher to encrypt and decrypt messages, respectively. Since the key management is very difficult in the classic Vernam cipher, Alice and Bob may choose a QKD scheme, e.g., BB84 protocol, to generate and distribute the secret key. Using the secret key obtained with quantum techniques the confidentiality of messages may be ensured. Where the combination of QKD with a one-time pad cipher and an information theoretically secure message authentication scheme (used in QKD) is referred to as quantum cryptography. In this sense, the quantum cryptography is unconditional secure which means that it provides an encryption process that no analysis can break, irrespective of whatever advances are made in mathematics or computer science including quantum computation. However, with today's technology it is impossible to use quantum cryptography as a one-time pad stream cipher encoding typical data traffic, because key generation rates achieved with QKD are too low by many orders of magnitude. Therefore, hybrid systems are always used in practices [**?**], for example, keys are generated and distributed using QKD techniques and generated

keys are employed for conventional encryption algorithms like the well-known AES. Some practical systems for such case have been manufactured in the recent years. The details may be referred to Chapter 9.

The other approach of ensuring the confidentiality is to adopt directly the quantum cryptosystem with pure quantum effects. That is, the encryption and decryption processes are quantum algorithms and the key comes from a QKD scheme, or the encryption and decryption processes and key generation are united in a quantum algorithm. A significant difference between the classic cipher and quantum cipher is that quantum cipher states may be nonorthogonal. Subsequently, the attacker cannot distinguish effectively obtained cipher states. This characteristic is very useful for the security of employed cryptographic algorithms. Therefore, the quantum cryptosystem may be more secure in principle than the classic cryptosystem. Of course, quantum computing technologies are obviously needed in this approach. The quantum computer is out of the anticipation since the difficulties in many aspects such as the quantum memory, integration of quantum circuits, and implementation of entanglement with lager number quanta. Fortunately, it has been shown that some simple quantum computing technologies are available in practices. Subsequently, pure quantum cryptographic algorithms depending on these technologies are implementable physically. According to the characteristics of employed keys, such a kind of algorithms is divided into the quantum symmetrical key algorithm and quantum public key algorithm. The details for these algorithms will be presented in Chapter 5.

The authentication characteristics are ensured by authentication schemes which are associated actually with cryptosystem [**?**]. Authentication techniques are used to verify communicators' identities and integration of transmitted messages so that the forgery is impossible or may be prevented. This is another important aspect for the security of a private communication system. In fact, authentication techniques have become a key element in QKD schemes which are very important for the secure quantum communication system. To ensure the secure QKD procedure the communicators should first share a short authentication key for the channel authentication. Without this authentication procedure, the QKD scheme cannot reach unconditional security even the obtained key is possibly insecure since Man-in-the-mid attacks.

Generally, the authentication includes the identity verification and message authentication. The identity verification is used to identify identifications of legitimate communicators, and the message authentication is employed to certify that a message is from and has not been altered in transit. For most of recorded history, authentication has depended on physical objects that are hard to copy, such as seals and signatures. Such devices provide limited security, and they cannot be used at all for digital electronic documents, such as bank transactions, which are often transmitted over insecure telecommunications lines. Fortunately, several mathematical techniques are available for authenticating digital messages in the classic private communication. Combining classic approaches, there are three ways for implementing

the authentication in a quantum private communication system. One is to use pure classic authentication approaches. In 1979, Wegman and Carter of IBM discovered a digital authentication scheme that does provide provable security [**?**]. It has been shown that this scheme is useful for identity verification in the well-known QKD system. Another is a combination of the classic authentication algorithm with an assistant of QKD techniques. Like the Vernam cipher, the authentication requires that the sender and receiver possess beforehand a shared secret key. Thus Wegman-Carter authentication and QKD can be combined to reach the task of the identity and message authentication. The last approach is a pure quantum approach. Like a pure quantum cryptosystem, a pure quantum authentication scheme is possible. Especially the pure quantum authentication scheme is necessary in a quantum network which has become a hot topic in recent years. In Chapter 6 the identity verification and message authentication will be introduced.

According to the above descriptions one finds that both the confidentiality and authentication properties are associated with cryptographic keys. This gives rise to an important problem: key management. Consequently, except for the confidentiality and authentication properties the key management is also an important ingredient for implementing the quantum private communication. Actually, the key management has become a crucial issue in the classic cryptography as well as quantum cryptography. For instance, the well-known Vernam cipher becomes no practical since difficulty of the key management. Generally, the key management includes mainly the key generation, key distribution, key exchange, key storage, and key update in secure ways. According to current techniques, one cannot construct a good key management system only using quantum way since some techniques (e.g., the qubit storage) are not available. However, the secure key generation, distribution, and exchange are implementable using QKD techniques [**?**]. Generation and distribution of secure key via quantum techniques will be discussed in Chapter 3.

As the quantum private communication has become a practical subject with products available commercially, it is important to focus not only on theories but also on practical issues. Thus, the physical implementation of the quantum private communication is also an important part. Different from the classic private communication system where the physical implementation is not important, the implementation of the quantum private communication is associated closely with physical signals. Presently, two kinds of quantum signals, i.e., discrete variable quantum signals and continuous variable quantum signals, are always employed. Using the discrete variables quantum signals one may implement the so-called single photon quantum secure communication, while if one use continuous variable quantum signals (e.g., coherent state and squeezed state signals) a kind of continuous variables quantum secure communication can be implemented. How to generate and transmit single photon signals and continuous variable quantum signals will be discussed in Chapters 7 and 8. While fundamental physics principles for these quantum

signals and their transmission and detection properties will be presented in Chapter 2 from viewpoints of quantum bits (briefly called qubits).

In practices, the quantum private communication is usually implemented in a communication network, e.g., an optical fiber network or/and a wireless optical network which are over the Internet network based on Internet Protocol (IP) techniques. Thus the combination of quantum secure schemes with practical communication network techniques becomes a new issue which should be solved to implement a quantum private communication system. In the modern communication network, the standard network model [**?**], i.e., the OSI model which is actually a 7-layer network model, including physical layer, link layer, network layer, transport layer, session layer, presentation layer, and application layer, is always employed. The physical layer focuses on the signal transmission and processing. From the physical viewpoint, if transmitted signals obey classic physics laws, this communication is called the classic communication. While if transmitted signals obey quantum physics laws, this kind of communication ways may be called the quantum communication. Since the main network is over the Internet network, to implement the quantum private communication in a practical communication system, one should consider the combination of quantum protocols with the IP protocol and IPSec protocol. In addition, some new techniques, e.g., the quantum virtual private network (QVPN) should be investigated. These notations will be introduced in Chapter 9. Some international organizations such as the European Telecommunications Standards Institute (ETSI) are considering to make standard for the application of QKD techniques in practical telecommunication networks [**?**].

Different from the common communication, the security is a kernel ingredient for a private communication system. Although many researchers (especially the physicists) only believe the unconditional security of the quantum cryptographic scheme, from the viewpoints of engineering and cryptology, some quantum schemes with computational security based on the quantum complexity theory are also very useful. Thus, this book will concern both the unconditional security and quantum computational security. But please note, the quantum computational security relies on the quantum complexity theory which depends on the quantum Turing machine which will be described in Section 2.5.1. In addition, to support the security of quantum schemes for the quantum private communication, the quantum information theory and quantum complexity theory are naturally necessary. Clearly, this is different from the classic computational security associated with the classic Turing machine [**?**]. Of course, it is noted that the classic computational security has played an important role in the practical private communication. Some quantum cryptographic algorithms with quantum computational security have been proposed based on the quantum complexity theory. Using the quantum complexity theory, one may also build the security theory for the quantum cryptography which will be introduced in Chapter 2.

In conclusion, a glimpse on the quantum private communication is pre-

sented in this section. To construct a perfect quantum secure communication system in a practical network system, one should not only concern the cryptographic scheme and security of the quantum private communication which are associated with the confidentiality and authentication but also technical implementations and engineering issues. In remainder chapters how to solve these problems will be introduced in detail.

1.3 Private Communication Models

In order to investigate characteristics of the private communication, a private communication model should be built. In the classic scenario, it has been modeled mathematically by Shannon in 1949. This section tries to construct a quantum private communication model so that various quantum private communication systems can be modeled in a united way. To reach this aim, the quantum private communication model is constructed by analogy with the Shannon private communication model. Accordingly, a brief introduction on the classic private communication model is necessary before describing the quantum private communication model.

1.3.1 Classic Secure Communication Model

In a private communication system, three participators are usually involved, i.e., communicators (including sender and receiver) and a cryptanalyst. An illegitimate cryptanalyst is always called the attacker. The attacker will try to break the private communication system so that he can steal effective information or forge transmitted messages. The aim is to benefit himself with employed attack strategies. Generally, there are two class attack strategies on the private communication system. The attack for breaking the confidentiality is called the passive attack which only eavesdrop transmitted messages without changing it. In contrast, the attack for destroying the authentication is called the active attack which will change transmitted messages.

To protect the confidentiality of transmitted messages, a well-known private communication model was first presented by Shannon in 1949 [**?**]. This model with slight revision is shown in Fig.1.2. Shannon's private communication model consists of six elements, i.e., message source, encryption algorithm, channel, decryption algorithm, cryptanalyst, and message sink. In detail, a message m generated by the message source is encrypted by the encryption algorithm E_k which is controlled under the key k, consequently, a ciphertext c is created. After transmitted in the channel, the ciphertext c is decrypted by the decryption algorithm $D_{k'}$, which is controlled under the key k', then the plaintext m is recovered by the sink. Here, the decryption key k' might be the same as the encryption key k, i.e., $k' = k$, this case corresponds to the

symmetrical key cryptosystem. Also, the decryption key k' might be different from the encryption key k, i.e., $k \neq k'$, which corresponds to the unsymmetrical key cryptosystem. In practices, a cryptanalyst will break the private communication system using the obtained information from the channel and some prior knowledge so that he may benefit himself.

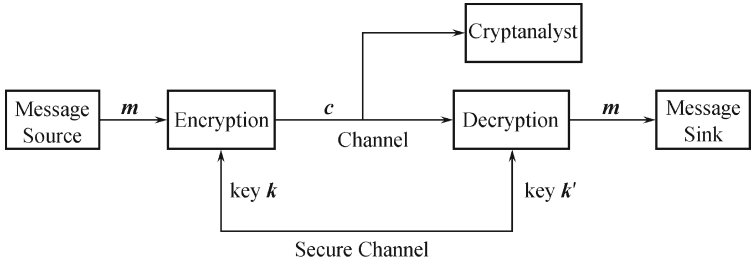

Fig. 1.2. Schematic for classic private communication

To ensure the authentication of the private communication system, active attacks should be prevented. Generally, there are two kinds of attack strategies, i.e., impersonative fraudulent attacks and substitution fraudulent attacks. Initially, the authentication model was founded by Simmons in 1979 [**?**]. This model uses the authentication code which is similar to the error-correction code. Its diagram is very similar to the Shannon's private communication model with substitutions of encryption and decryption using the authentication coding and authentication decoding, respectively. In practices the authentication is always ensured using cryptosystem. In this case the authentication procedure may be described in Fig.1.2.

As well-known, the Shannon private communication model has become one of foundations of classic private communication systems. Combining the private communication model presented in Fig.1.2 with assistant of the complexity theory used in public key cryptosystem and the authentication theory, the confidentiality and authentication issues in the classic communication may be solved in principle.

1.3.2 Quantum Private Communication Model

The private communication aims at preventing various attack strategies so that legitimate messages transmitted in a communication channel is protected. Generally, there are two kinds of attack strategies, i.e., the passive attack and active attack. To defend the passive attacks a cryptosystem for the encryption and decryption processing is necessary. While to defend the active attacks an authentication system for authenticating the identity of communicators or authenticity of messages is necessary. All these cryptographic procedures are associated with a key-system which is symmetrical or

unsymmetrical.

No exceptions for the quantum private communication. To protect legitimate messages, a cryptosystem is needed. As described previously, two approaches are involved. One is the combination of classic encryption algorithms controlled by a key which is obtained using QKD protocols. Since techniques of classic algorithms are mature, the key problem in this case is the QKD procedure. Another is directly to employ the quantum encryption algorithm to protect legitimate messages. To prevent the active attacker, quantum authentication approaches are needed although the classic authentication may play roles in some scenarios.

The book mainly considers the quantum private communication model which is associated with the QKD, quantum cryptosystem, and quantum authentication. The quantum private communication model may be defined using a similar way of the classic private communication. Combining the investigation on the QKD, quantum encryption, and quantum authentication, a quantum private communication model is demonstrated in Fig.1.3. In this figure, the states ρ and ρ' denote respectively message states and cipher states, they may be pure states or mixed states. Components of the quantum operations correspond to the encryption and decryption processes. While controllers A and B play the similar roles of keys. Comparing to Fig.1.2 one finds that the quantum private communication model is similar to the classic private communication model. But here the quantum features are involved.

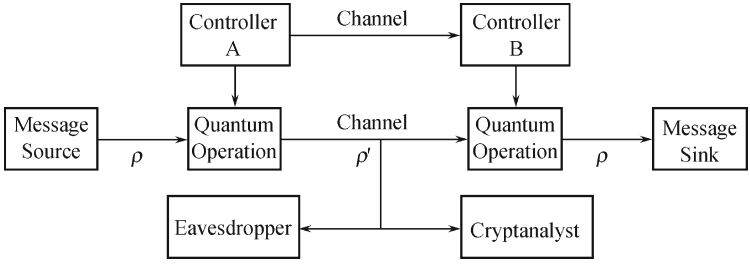

Fig. 1.3. Schematic for quantum private communication

Fig.1.3 has integrated the QKD procedure, quantum cryptosystem, and quantum authentication. For the quantum cryptosystem and quantum authentication, Controllers A and B are respectively the encrypting key and decrypting key like that in the Shannon private communication model, and quantum operations play roles of encryption algorithms and decryption algorithms like that in Fig.1.2. For the QKD scheme, there is some special characteristics. In this case, Controllers A and B imply random numbers which are used to control the choice of measurement bases by the communicators called Alice and Bob, and quantum operations are actually random measurements operated by the communicators.

Integrating the above ingredients, one may imagine the following patterns

for the quantum private communication. Suppose arbitrated two communicators called Alice and Bob in a communication network want to establish a secure communication in quantum ways, they should ensure two security ingredients, i.e., confidentiality and authentication, of the communication system so that the involved communication system is secure. Clearly, to guarantee the confidentiality a proper cryptosystem should be employed, while to ensure the authentication the authentication schemes must be involved. At the same time, protections of both the confidentiality and authentication need secure key management systems. Accordingly, to implement a quantum private communication, cryptosystems, authentication schemes, and secure key management systems are three basic ingredients. All involved operations in these ingredients may be in classic ways or quantum ways, but at least one of these ingredients should have quantum characteristics. Therefore, the quantum private communication may be defined as follows: a kind of communication which ensures its confidentiality and authentication in quantum ways.

1.4 History of Quantum Private Communication

Fundament of the classic private communication is a classic cryptology. Similarly, the quantum private communication depends on the quantum cryptology which is a special chapter in the history of the cryptology. Accordingly, the private communication originated from the cryptology which has a long history.

The art of cryptology began at about 3000 years ago and has played an important role in history ever since. However, all presented cryptosystems are not provable security until the Vernam cipher was presented. In 1917 during World War I, Vernam of American Telephone and Telegraph Company and Mauborgne of the U.S. Army Signal Corps developed the first truly unbreakable code called the Vernam cipher. One distinctive feature of the code is that the cipher needs a key which is long as the message being transmitted, and the key cannot be reused for another message. This feature leads the Vernam cipher to be impractical in commercial applications since the distribution and storage of the private key is very expensive.

Academic interests in cryptology grew more intense in the mid-1970s, when Diffie, Hellman, and Merkle discovered the principle of public-key cryptosystems (PKC) [**?**]. Soon afterward, in 1978, Rivest, Shamir, and Adleman devised a practical implementation called RSA algorithm [**?**]. The distinctive feature of PKC is that there are two keys: one is private and another is public. This feature leads the convenience of cryptosystems in practices. Offsetting this advantage is the fact that public-key systems have not been proven to be secure. Indeed, in 1982 Shamir cracked one of the early public-key cryptosystem, the snapsack cipher [**?**]. In addition, the computational

complexity of public key cryptosystems is very high although the well-known NTRU algorithm is faster [**?**].

Several years before the discovery of PKC, another striking development had quietly taken place: the union of cryptography with quantum mechanics. Around 1970 Wiesner, then at Columbia University, presented a paper entitled "Conjugate coding", explaining how quantum physics could be used, at least in principles, to accomplish two tasks that were impossible from the perspective of classic physics [**?**]. One task was a way to produce bank notes, which was called "quantum bank notes". A picture for a quantum bank note, which stores 100 Chinese Yuan (RMB), is plotted in Fig.1.4. Since the no-cloning theorem the so-called quantum bank note would be physically impossible to counterfeit. Another task in Wiesner's paper was associated with the multiplexing channel which was employed to combine two bits classic messages into a single quantum transmission from which the receiver could extract either message but not both. This scheme is very similar to the principle of the classic 1-out-2 obvious transfer proposed by Even, Goldreich and Lempel in 1985 [**?**]. Although Wiesner opened a new era in cryptography, unfortunately, his paper was rejected by the journal to which he submitted it, and it went unpublished until 1983.

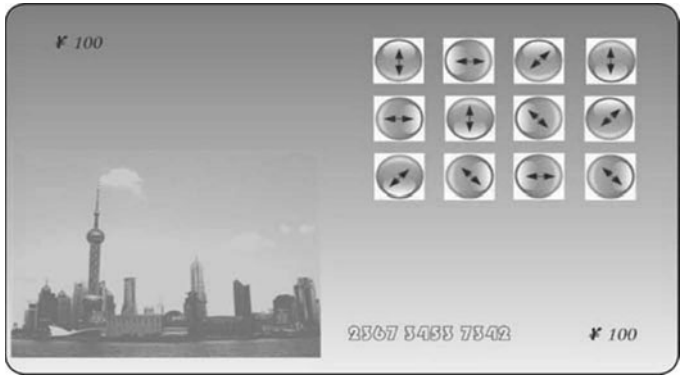

Fig. 1.4. A quantum bank note according to Wiesner's proposal

In 1979, Bennett and Brassard, who knew of Wiesner's ideas began thinking of how to combine them with PKC [**?**]. At the beginning their realizations were impractical for they focused on PKC with quantum state storage techniques. In 1984, Bennett and Brassard realized that the transmission of quantum states is very important. Subsequently, they devised the first QKD scheme which is called the BB84 protocol lately [**?**]. This scheme was experimental implemented in 1989 which was published in 1992 [**?**].

Motivated by idea of the BB84 protocol, the theoretical ideas of Deutsch of the University of Oxford led Ekert to conceive of different QKD scheme which is implemented using correlation of Einstein-Podosky-Rosen (EPR)

pair [?]. In 1991, utilizing the idea conceived by Palma of the University of Palermo, Rarity and Tapster of the British Defence Research Agency started experiments implementing Ekert's scheme [?]. Lately, Ekert's scheme is called the EPR protocol.

Currently, the BB84 protocol and EPR protocol are two basic QKD protocols. After 20 years of basic research, quantum cryptography has meanwhile led to first commercial products. By far, one may generate quantum key over 200 km in a telecommunication optical fibre [?] and over 1480 km in a free-space between the Matera Laser Ranging Observatory of the Italian Space Agency and the satellite Ajisai, a low-Earth orbit geodetic satellite [?]. These experiments will be described in Chapter 9. In addition, a theory construction for the quantum cryptology has been built gradually.

As the main application of the quantum cryptology, the quantum private communication which combines the quantum cryptology and communication techniques has become gradually a hot topic. Like that in the classic scenario the aim of the quantum private communication is to protect the confidentiality and authentication for practical communication systems. With the development of quantum cryptographic techniques, the quantum private communication enters gradually into the field of practical application. Currently, its applications in optical communication systems, mobile communication systems and IP network systems have been developing. For example, the quantum private communication in the well-known passive optical network (PON), which is an important access network for the all-optics communication, has been implemented experimentally, and the quantum private communication over the IP network has been building under a DAPA project supported by the Department of Defense (DoD) in USA.

1.5 Relationship with Other Subjects

It is well-known that the interdiscipline is a main feature of the cryptology. No exception for the quantum cryptology. Subsequently, the quantum private communication based on the quantum cryptology is a typical cross-discipline which is associated with many subjects. This characteristic is similar to the classic private communication. Since the quantum private communication involves not only theoretical topics but also practical issues, it is associated with at least three kinds of subjects. One is the fundamental subject such as quantum mechanics, information theory, complexity theory, etc. Another is associated with technical subjects, e.g., laser physics, nonlinear optics, etc. The last one is practical application subjects, for instance the optics communication, wireless communication, Internet network, etc.

The relationships of the quantum private communication with other subjects are sketched from three different routes. Firstly, from the viewpoint of the information science, the quantum private communication which depends

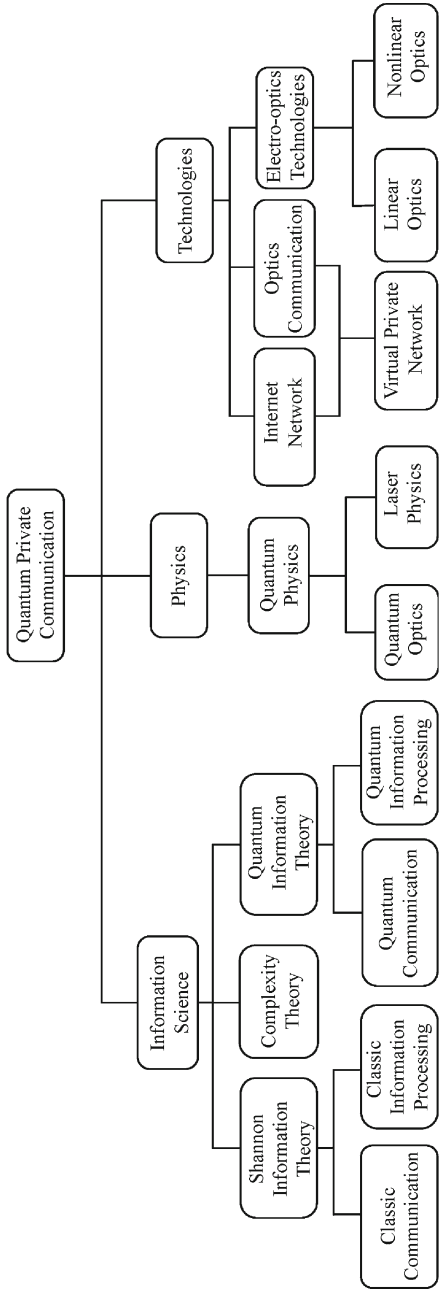

Fig. 1.5. Correlation of quantum private communication and other subjects

closely on the quantum cryptography is a new information processing technique. This technique processes the quantum information and classic information using quantum approaches. The novel characteristic of quantum effects leads a more powerful secure communication way than the classic secure communication. Accordingly, the quantum private communication is associated with the Shannon information theory, complexity theory, and quantum information theory. Secondly, since the quantum private communication is a combination of quantum physics, cryptology and communication techniques, surely, it is associated with the quantum physics, quantum optics, and laser physics. Some physical effects from these subjects are often used to design the protocols or algorithms. Actually, the quantum physics laws are fundament of the quantum private communication as well as the quantum cryptography. Finally, to implement the quantum private communication in technique, some technical subjects and communication subjects are associated. These subjects include such as the optical communication, electro-optics technology, linear optics, nonlinear optics, and network technique. In addition, some important access networks, such as the passive optical network and Virtual private network, are also related with the the quantum private communication.

According to the above descriptions, the relationships of the quantum private communication with other subjects are plotted in Fig.1.5 with an inverse tree structure. Of course, one should note that this figure is not complete, i.e., not all related subjects are contained. Especially, with further investigation more subjects might be associated with the quantum private communication.

1.6 Notations and Conventions

Most notations and notions have been listed in the index part. Since the following notations and conventions play important roles in the cryptology as well as the private communication, and will be often implicated, we here present a section to describe them in detail. After that these notations and notions will be applied directly without explanation in the book.

1.6.1 Random Variables

The random variable is a widely used notation in information science. It is also an important conception in the book. Mathematically, random variables are used in the study of probability. They were developed to assist in the analysis of games of chance, stochastic events, and results of scientific experiments by capturing only mathematical properties necessary to answer probabilistic questions. Essentially, a random variable is not a variable but rather a function, which assigns unique numerical value to all possible outcomes of a random experiment under fixed conditions.

There are two types of random variables, i.e., the discrete random variable and continuous random variable. A discrete random variable takes values from a countable set of specific values, each with some probability greater than zero. A continuous random variable takes values from an uncountable set, and the probability of any one value is zero, but a set of values can have positive probability. Clearly, a random variable has an associated probability distribution and frequently also a probability density function. Probability density functions are commonly used for continuous variables. Random variables can also be "mixed", having attributes of both discrete and continuous random variables.

Mathematically, a random variable is thought of as a function mapping the sample space of a random process to real numbers. Let $(\mathscr{P}, \mathfrak{F}, P)$ be a probability space and $(\mathscr{N}, \Sigma)$ be a measurable space, where $\mathscr{P}$ denotes a probability set with event set $\mathfrak{F}$, $\mathscr{N}$ is a number set, $P \in \mathscr{P}$ and Σ is a nonempty collection of all possible subsets of $\mathscr{N}$ (including $\mathscr{N}$ itself) that is closed under complementation and countable unions of its members. Then a random variable X is formally defined as a measurable function $X : \mathscr{P} \to \mathscr{N}$. An interpretation of this is that the preimage of "well-behaved" subsets of $\mathscr{N}$ (elements of Σ) are events (elements of $\mathfrak{F}$), and hence are assigned a probability by P.

A discrete random variable $X(x_i, p(x_i))$ implies a finite set $\boldsymbol{x}$ consists of N elements $\{x_i \in \boldsymbol{x} | i = 1, 2, \ldots, N\}$, the probability distribution for each element is $p(x_i)$ with $\sum_i p_i = 1$. Similarly, the continuous random variable $X(x, p(x))$ is defined as an uncountable set $\boldsymbol{x}$ together with a probability density function $p(x)$ on x.

1.6.2 Cryptosystem and Cipher

The aim of the private communication is to ensure the confidentiality and authentication of transmitted messages in a communication system. As mentioned in Section 1.2, both the confidentiality and the authentication are associated with cryptosystem. Accordingly, the cryptosystem is an often used notion in the private communication. This section introduces this notion and the correlated notions.

A cryptosystem refers to a suite of algorithms needed to implement a particular form of encryption and decryption. Typically, a cryptosystem consists of three algorithms: one for key generation and/or distribution, one for encryption, and one for decryption. In cryptography, the key generation and distribution algorithm is a process of how to generate and distribute secure keys or key-pair. The encryption is a process of transforming information (referred to as plaintext) using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information (referred to as ciphertext).

In many contexts, the word encryption also implicitly refers to the reverse process, decryption (e.g., "software for encryption" can typically also perform decryption), to make the encrypted information readable again (i.e., to make it unencrypted). Encryption, by itself, can protect the confidentiality of messages, but other techniques are still needed to protect the integrity and authenticity of a message; for example, verification of a message authentication code (MAC) or a digital signature. Standards and cryptographic software and hardware to perform encryption are widely available, but successfully using encryption to ensure security may be a challenging problem. A single slip-up in system design or execution can allow successful attacks.

A classic cryptosystem means involved algorithms, i.e., the key generation algorithm, encryption algorithm, and decryption algorithm, are implemented in classic ways. While a quantum cryptosystem implies the encryption and decryption processes are implemented in classic ways with quantum keys or all involved algorithms are implemented in pure quantum ways. Generally, the classic cryptosystem as well as the quantum cryptosystem are divided into two categories, i.e., the symmetrical key cryptosystem and public key cryptosystem. In the former, the encryption key and decryption key are symmetrical or the same, but the encryption key and decryption key are different in the later.

In a cryptosystem, other notions such as plaintext, ciphertext, and key are always involved in. The so-called plaintext is a coded message without encryption process. Combining the quantum cryptology, the plaintext consists of qubits or/and classic bits. The particles which carry plaintexts is called as the plaintext particle, and the quantum state of plaintext particles is called as the plaintext state. The plaintext space is a set consists of all possible coded messages. Similarly, the ciphertext consists of qubits or/and classic bits, and ciphertext particles mean the particles carried the ciphertext, and the ciphertext state means the quantum state of ciphertext particles. It is noted that plaintext particles and ciphertext particles may be the same, but the plaintext state and ciphertext state must be different. The ciphertext space is a set consists of all possible cipher.

Finally, this book have to mention two often used notions, i.e., the cipher and cryptosystem. The term cipher (sometimes cypher) is often used to refer to a pair of algorithms, one for encryption and one for decryption. Therefore, the term "cryptosystem" is most often used when the key generation algorithm is important. In addition, one should note that differences between the cryptosystem and the cryptographic system. A cryptographic system implies any computer system that involves cryptography.

References

[1] Proakis J (1994) Digital communication. Wiley, New York

[2] Park C S, Oh C K, Lee C G, et al (2005) A photonic up-converter for a WDM radio-over-fiber system using cross-absorption modulation in an EAM. IEEE Photonics Technology Letters, 17(9): 1950 – 1952

[3] Nielsen M A, Chuang I L (2000) Quantum computation and quantum information. Cambridge University Press, London

[4] Hughes R J, Doolen G, Awschalom D, et al (2004) Quantum information science and technology roadmap. http://qist.lanl.gov/. Accessed 20 January 2009

[5] Zoller P, Fazio R, Calarco T, et al (2005) ERA-Pilot Roadmap: quantum information sciences and technologies. http://qist.ect.it/. Accessed 20 January 2009

[6] Shannon C E (1948) A mathematical theory of Communication. Bell System Technical Journal, 27(4): 397 – 423

[7] Schneier B (1994) Applied cryptography: protocols, algorithms, and source code in C. Wiley, New York

[8] Zeng G H (2006) Quantum cryptology. Science Press, Beijing

[9] Shields A, Yuan Z (2007) Key to the quantum industry. Physics World, 20(24): 24 – 29

[10] Assche G V (2006) Quantum cryptography and secret-key distillation using quantum cryptography. Cambridge University Press, London

[11] Wegman M N, Carter J, L (1979) New classes and applications of hash functions. Proceedings of the 20th Annual Symposium on Foundations of Computer Science, Puerto Rico, 29 – 31 October 1979, pp 175 – 182

[12] Gisin N, Ribordy G, Tittel W, et al (2002) Quantum cryptography. Reviews of Modern Physics, 4: 145 – 195

[13] Douglas E C (1997) Computer networks and Internets. Prentice Hall, New Jersey

[14] http://www.etsi.org/WebSite/NewsandEvents/ISG_QKD.aspx. Accessed 12 February 2009

[15] Wegener I. Complexity theory (2005) Springer, Heideburg

[16] Shannon C E (1949) Communication theory of secrecy system. Bell System Technical Journal, 28(4): 656 – 715

[17] Simmons G J (1979) Authentication without secrecy: A secure communication problem uniquely solvable by asymmetric encryption techniques. Proceedings of IEEE EASCON 79, Washington DC, 9 – 11 October 1979, pp 661 – 662

[18] Diffie W, Helman M E (1976) New directions in cryptography. IEEE Transactions on Information Theory, 22(6): 644 – 654

[19] Rivest R L, Shamir A, Adelman L (1978) A method for obtaining digital signature and public key cryptosystems. Communications of the ACM, 21(2): 120 – 126

[20] Shamir A (1982) A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem. Advances in Cryptology-Proceedings of Crypto 82, Santa Barbara, California, 24 – 26 August 1982, pp 279 – 288

[21] Hoffstein J H, Pipher J P, Silverman J H S (1998) NTRU: a Ring based Public Key Cryptosystem. Proceedings of Algorithmic Number Theory: Third Ihternational Symposium, Portland, 21 – 25 June 1998, Springer, LNCS 1423: 267 – 288

[22] Wiesner S (1983) Conjugate coding. Sigact News, 15: 78 – 88

[23] Even S, Goldreich O, Lempel A (1985) A randomized protocol for signing contracts. Communications of the ACM, 28(6): 637 – 647

[24] Bennett C H, Brassard G, Breidbart S, et al (1982) Quantum cryptography, or unforgeable subway tokens. Advances in Cryptology-Proceedings of Crypto 82, Santa Barbara, California, 24 – 26 August 1982, pp 267 – 275

[25] Bennett C H, Brassard G (1984) An update on quantum cryptography. Advances in Cryptology-Proceedings of Crypto 84, Barbara, California, 19 – 22 August 1984. Lecture Notes in Computer Science (LNCS), Springer, Heidelberg, 196: 475 – 480

[26] Bennett C H, Bessette F, Brassard G, et al (1992) Experimental quantum cryptography. Journal of Cryptology, 5: 3 – 28

[27] Ekert A K (1991) Quantum cryptography bases on Bell's theorem. Physical Review Letters, 67: 661 – 664

[28] Ekert A K, Rarity J G, Tapster P R, et al (1992) Practical quantum cryptography based on two-photon interferometry. Physical Review Letters, 69: 1293 – 1295

[29] Takesue H, Nam S W, Zhang Q, et al (2007) Quantum key distribution over a 40-dB channel loss using superconducting single photon detectors. Nature photonics, 1: 343 – 368

[30] Villoresi P, Jennewein T, Tamburini F, et al (2008) Experimental verification of the feasibility of a quantum channel between space and Earth. New Journal of Physics, 10: 1 – 2

2 Quantum Security Theory

This chapter devotes to building a security infrastructure for the quantum private communication. To reach this aim, some fundamental subjects including quantum mechanics, quantum information theory and quantum complexity theory are introduced. Of these fundamental subjects, the quantum mechanics is the cornerstone. With these fundamental subjects, a security theory for the quantum private communication is built.

In previous chapter, an overview of the quantum private communication has been presented and a quantum private communication model has been constructed. This chapter investigates the security theory for the quantum private communication. For convenience, this kind of security theory is called a quantum security theory in this book. As usual, both the information-theoretic security and computational security which is very useful in practical applications are contained in the quantum security theory. Different from the scenarios in the classic private communication, however, the information-theoretic security and computational security are here based on the quantum information theory and quantum complexity theory, respectively. To construct the quantum security theory, three aspects are involved including the information theory, complexity theory, and security model. The information theory contains both the Shannon information theory and quantum information theory. The complexity theory is associated with the classic complexity and quantum complexity theory which is based on the quantum Turing machine (TM). And the security model is a general description for the quantum security theory based on the information theory and complexity theory. Before describing in detail the quantum security theory, some fundamentals including the mathematical backgrounds and quantum mechanics are described. They are actually the cornerstones of the quantum security theory.

2.1 Introduction

A communication model for the quantum private communication has be constructed in Chapter 1. This model provides a clearly physical picture for the communication procedure of the private communication implementing in

quantum ways. As well known, the security is extremely important in classic private communication systems. There is no exception for the quantum private communication system. In fact, any private communication system is not useful without a powerful security guarantee. Herewith, this chapter investigates the quantum security theory for the quantum private communication.

Previously, investigations concerning the security for a quantum private communication system are mainly focused on the security problems of the quantum key distribution schemes. In this scenario, various approaches, which have been proposed from viewpoints of physics, mathematics, or information theory, have proven that the proposed quantum key distribution protocols are unconditional security, or say information-theoretic security which is closely associated with the information theory. However, this is not all for the quantum security theory. Like the classic private communication, cryptographic algorithms with computational security should be always employed in a practical quantum private communication systems. Actually, some algorithms for the quantum private communication, e.g., quantum public key cryptosystems, have been investigated. The security of these algorithms depends on the quantum complexity theory. Thus, like the security theory for the classic private communication, the security for the quantum private communication is also associated with both the information theory and complexity theory. However, here both the information theory and complexity theory are referred to the quantum information theory and quantum complexity theory depending on quantum mechanics, respectively. Thus, this chapter first introduced fundamentals of quantum information theory and quantum complexity theory, and then tries to construct a quantum security theory.

As mentioned in the above, the quantum information theory and quantum complexity theory are closely associated with quantum mechanics. Accordingly, quantum mechanics are briefly introduced with describing several postulates. In addition, consider that the linear algebra is the fundament of quantum mechanics, some mathematical background combining quantum notations are presented so that readers who have no such basis can read this book. In the mathematical background, properties of the Hilbert space are mainly presented.

2.2 Mathematical Background

This section introduces briefly some linear algebraic knowledge for the quantum private communication. For those readers who have such knowledge may skip this section. As the fundament of quantum mechanics two import notations are always employed, i.e., the Hilbert space and operators. For the details on the linear algebra one may refer to Ref.[**?**]

2.2.1 Hilbert Space

In the quantum information processing, the most interest space is the complex number space denoted $\mathbb{C}^n$: the space of all n-tuples of complex numbers. Denote $\mathbb{C}^n = (c_1, c_2, \ldots, c_n)$ with $c_k = a_k + \mathrm{i}b_k$ and $k = 1, 2, \ldots, n$, where a_k and b_k are real numbers. Let $\mathbb{V}$ denotes a linear space, one has

$$\mathbb{C}^n \subset \mathbb{V}. \tag{2.2.1}$$

The element of a linear complex space is called as a vector. A vector can be denoted using a one column matrix $\boldsymbol{v}$

$$\boldsymbol{v} = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}. \tag{2.2.2}$$

Since the main motivation in this book for introducing linear algebra is for the quantum private communication, notations should be following the quantum standard. Making using of quantum notations, the vector v is denoted $|v\rangle$ called **ket**, where the symbol $|\cdot\rangle$ is a Dirac notation and v is a label for a vector. A concomitant expression for the vector $|v\rangle$ is $\langle v|$ called **bra**, which denotes the dual vector of the **ket**. In addition, $(|v\rangle)^* = (c_1^*, c_2^*, \ldots, c_n^*)^{\mathrm{T}}$ and $(|v\rangle)^\dagger = ((c_1^*, c_2^*, \ldots, c_n^*)^{\mathrm{T}})^{\mathrm{T}} = \langle v|$ denotes the complex conjugate and Hermitian conjugate of the vector $|v\rangle$, respectively.

An inner product is a kind of operations on vectors in the complex space. In details, the inner product is defined as follows.

Definition 2.2.1 Let $\mathbb{V}$ be a linear space over complex number field $\mathbb{C}$, and $|\phi\rangle$ and $|\psi\rangle$ be arbitrary vectors in the space $\mathbb{V}$. The function $G : \mathbb{V} \times \mathbb{V} \to \mathbb{C}$ is defined as an inner product, where

$$G : C = (|\phi\rangle, |\psi\rangle) \equiv \langle\phi|\psi\rangle. \tag{2.2.3}$$

Theorem 2.2.1 Any inner product is conjugate-linear, i.e.,

$$\left(\sum_i \lambda_i |w_i\rangle, |v_i\rangle\right) = \sum_i \lambda_i \left(|w_i\rangle, |v_i\rangle\right). \tag{2.2.4}$$

If a complex space is defined with operations of the inner product, this kind of vector space calls inner product space.

Definition 2.2.2 If the inner product has been defined in the linear space $\mathbb{V}$, and following conditions are satisfied for arbitrary vectors $|\phi\rangle$ and $|\psi\rangle$ in a complex number space: 1) $\langle\psi|\phi\rangle = (\langle\phi|\psi\rangle)^*$, where $(\langle\phi|\psi\rangle)^*$ is the complex conjugate of $\langle\psi|\phi\rangle$; 2) $\langle\psi|\psi\rangle \geq 0$ with equality if and only if $|\psi\rangle = 0$;

and 3) $(|\phi\rangle, \sum_{i=1}^{n} \alpha_i |\psi_i\rangle) = \sum_{i=1}^{n} \alpha_i (|\phi\rangle, |\psi_i\rangle)$ for arbitrary $|\phi\rangle, |\psi_i\rangle \in \mathbb{V}$ and $\alpha_i \in \mathbb{C}$. Then $\mathbb{V}$ is called as an inner product space.

In quantum mechanics as well as the quantum information, Hilbert space is an important notation. The Hilbert spaces is defined as follows.

Definition 2.2.3 A Hilbert space is exactly the same thing as an inner product space. Usually the Hilbert space is denoted as $\mathscr{H}$.

For examples, the 2-dimension Hilbert space which is often employed in the quantum information processing is denoted $\mathscr{H}_2$, and an n-dimension Hilbert space is denoted $\mathscr{H}_n$.

2.2.2 Properties of Hilbert Space

A linear space is spanned by some basic vectors, and this is the same for the Hilbert space. In the Hilbert space a vector is usually called a state vector. This notation is employed in the follows.

1) Basic vectors

Let $|\psi\rangle$ be an arbitrary vector in Hilbert space, i.e., $|\psi\rangle \in \mathscr{H}$, its Hermitian conjugate is $\langle\psi|$. They have the following relations

$$(|\psi\rangle)^{\dagger} = \langle\psi|. \tag{2.2.5}$$

If $|\psi\rangle = 0$, the vector $|\psi\rangle$ is called the zero vector. Please note $|0\rangle \neq 0$, since $|0\rangle$ is always employed to denote a non-zero vector, while 0 denotes only a number.

The length of the vector $|\psi\rangle$ in Hilbert space is defined as follows,

$$L_{\psi} = \sqrt{|\langle\psi|\psi\rangle|}, \tag{2.2.6}$$

where L_{ψ} is also called the norm of the vector $|\psi\rangle$. Distance of arbitrary two vectors $|\psi\rangle, |\phi\rangle$ in Hilbert space is given by

$$\Delta L = \sqrt{|\left(\langle\psi| - \langle\phi|\right)\left(|\psi\rangle - |\phi\rangle\right)|}. \tag{2.2.7}$$

The angle of two arbitrated vectors reads

$$\cos\theta = \frac{|\langle\psi|\phi\rangle|}{L_{\psi} L_{\phi}}. \tag{2.2.8}$$

2) Vector operation

Since the Hilbert space is a linear space, operations defined in the linear space are completely suitable for vectors in the Hilbert space. Let $|\phi_1\rangle$, $|\phi_2\rangle$, …, $|\phi_n\rangle \in \mathscr{H}$ and $c_1, c_2, \ldots, c_n \in \mathbb{C}$, the linear combinator (addition)

$|\Psi\rangle$ of these vectors is still a vector in the Hilbert space, and the addition vector is denoted as

$$|\Psi\rangle = c_1|\phi_1\rangle + c_2|\phi_2\rangle + \ldots + c_n|\phi_n\rangle. \tag{2.2.9}$$

There are two kinds of vector multiplication operations, i.e., the inner product and tensor product. The inner product has been introduced in previous, so that we here focus on the tensor product.

Definition 2.2.4 Let $|\phi\rangle, |\psi\rangle \in \mathscr{H}$, then $|\Phi\rangle = |\phi\rangle \otimes |\psi\rangle$ is called the tensor product of two vectors $|\phi\rangle, |\psi\rangle$.

The tensor product is a way of putting vector spaces together to form larger vector space. This is very useful for the multi-particle quantum system which is always involved in the quantum information processing. Since the vector may be denoted in matrix form, the tensor product of state vectors is associated with the tensor product of matrices. It has properties as follows,

$$\begin{cases} c|\phi\rangle \otimes |\psi\rangle = (c|\phi\rangle) \otimes |\psi\rangle = |\phi\rangle \otimes (c|\psi\rangle), \\ |\phi\rangle \otimes (|\psi_1\rangle + |\psi_2\rangle) = |\phi\rangle \otimes |\psi_1\rangle + |\phi\rangle \otimes |\psi_2\rangle, \\ |\phi\rangle^{\otimes k} = \underbrace{|\phi\rangle \otimes |\phi\rangle \otimes \ldots \otimes |\phi\rangle}_{k}. \end{cases} \tag{2.2.10}$$

3) Representation

Suppose there are n vectors $|v_1\rangle, |v_2\rangle, \ldots, |v_n\rangle$ in the linear space, they may be linearly dependent or linearly independent, which is defined as follows.

Definition 2.2.5 A set of non-zero vectors $\{|v_1\rangle, |v_2\rangle, \ldots, |v_n\rangle\}$ is linearly dependent if there exists a set of complex numbers $a_1, a_2, \ldots, a_n$ with $a_i \neq 0$ for at least one value of i, such that

$$a_1|v_1\rangle + a_2|v_2\rangle + \ldots + a_n|v_n\rangle = 0. \tag{2.2.11}$$

Otherwise, it is linearly independent.

If a vector set $\{|v_1\rangle, |v_2\rangle, \ldots, |v_n\rangle\}$ in the Hilbert space $\mathscr{H}$ is linearly independent, the vector elements satisfy orthogonal-normalized condition, i.e.,

$$\langle v_i|v_j\rangle = \delta_{ij} = \begin{cases} 0, & i \neq j, \\ 1, & i = j. \end{cases} \tag{2.2.12}$$

In this case, the vector set consists a basis in the Hilbert space $\mathscr{H}$, and the vector set is called an orthogonal and normalized vector set.

Since the linearly independent vector set $\{|v_1\rangle, |v_2\rangle, \ldots, |v_n\rangle\}$ is regarded as a basis in the Hilbert space $\mathscr{H}$, any vector in the space $\mathscr{H}$ can be denoted using the basis, i.e.,

$$|\psi\rangle = \sum_{i=1}^{n} a_i|v_i\rangle. \tag{2.2.13}$$

As an example, in a 2-order Hilbert space $\mathscr{H}_2$, a basis $\{|v_1\rangle, |v_2\rangle\}$ is denoted by the following forms,

$$|v_1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |v_2\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \tag{2.2.14}$$

then arbitrary vector $|v\rangle$ is denoted using this basis,

$$|v\rangle = a_1|v_1\rangle + a_2|v_2\rangle. \tag{2.2.15}$$

Generally, a vector space has many different spanning sets. For example, the vector presented in the above example may be represented in following way. Given a new basis $\{|\tilde{v}_1\rangle, |\tilde{v}_2\rangle\}$ which is denoted by the following forms,

$$|\tilde{v}_1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \qquad |\tilde{v}_2\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}. \tag{2.2.16}$$

The same vector denoted in Eq.(2.2.15) is represented as

$$|v\rangle = \frac{a_1 + a_2}{\sqrt{2}}|\tilde{v}_1\rangle + \frac{a_1 - a_2}{\sqrt{2}}|\tilde{v}_2\rangle. \tag{2.2.17}$$

Eq.(2.2.13) implies that every vector in the Hilbert space is denoted using the basis, which means the space is spanned by this basis. Thus the basis of the Hilbert space is also called a spanning set. In details, the spanning set is defined as follows.

Definition 2.2.6 A spanning set is a set of vectors $\{|v_i\rangle, |i = 1, 2, \ldots, n\}$ such that any vector $|v\rangle$ can be written as a linear combination.

Using the basis, the inner product of any two vectors can be denoted. Let $|v\rangle$ and $|w\rangle$ be arbitrary vectors in the Hilbert space $\mathscr{H}$, the inner product is given by

$$\begin{aligned} \langle v|w\rangle &= \left(\sum_i v_i|i\rangle, \ \sum_j w_j|j\rangle \right) \\ &= \sum_{i,j} v_i^* w_j \langle i|j\rangle = \sum_{i,j} v^* w_j \delta_{ij} = \sum_i v_i^* w_i. \end{aligned} \tag{2.2.18}$$

The tensor product can also be denoted using the basis. Let $|w_i\rangle, |v_i\rangle$ be two orthogonal bases in vector spaces $\mathbb{V}$ and $\mathbb{W}$, respectively, then two arbitrary vectors are denoted $|\phi\rangle = \sum_i c_i|v_i\rangle$ and $|\psi\rangle = \sum_i d_i|w_i\rangle$. Thus, tensor products of these vectors are

$$|\phi\rangle \otimes |\psi\rangle = \sum_{ij} c_i d_j |i\rangle \otimes |j\rangle = \sum_{ij} c_i d_j |i, j\rangle. \tag{2.2.19}$$

The above analysis shows that the basis is very important. Therefore, the construction of orthogonal basis is an important issue. Let $\{|w_1\rangle, |w_2\rangle, \ldots,$

$|w_n\rangle\}$ be a basis set for some vector space $\mathscr{H}$. To construct an orthogonal basis, an approach called Gram-Schmidt procedure is often employed. Define $|v_1\rangle = |w_1\rangle/L_{w_1}$, and for $1 \leq k \leq d-1$ define $|v_{k+1}\rangle$ which satisfies the following relations,

$$|v_{k+1}\rangle = \frac{|w_{k+1}\rangle - \sum_{i=1}^{k}\langle v_i|w_{k+1}\rangle|v_i\rangle}{\left||w_{k+1}\rangle - \sum_{i=1}^{k}\langle v_i|w_{k+1}\rangle|v_i\rangle\right|}. \tag{2.2.20}$$

Then any finite dimensional vector space of d-dimension has an orthogonal basis. Using the constructed orthogonal basis, a Hilbert space is spanned and any state vector in the Hilbert space can be expressed in such the basis.

2.2.3 Operators

In many situations, the vector needs to be transformed. To perform such a task transforms or called operations are necessary. This section introduces some useful operations which are often employed in the quantum information processing. Especially those are associated closely with the quantum cryptology and quantum private communication are described.

1) Linear operators

A linear transform is actually a liner operation, which is often denoted using a linear operator A defined as follows.

Definition 2.2.7 A linear operator between linear spaces $\mathbb{V}$ and $\mathbb{W}$ is defined to be any function $A : \mathbb{V} \to \mathbb{W}$ which is linear in its inputs, i.e.,

$$A\left(\sum_i a_i|v_i\rangle\right) = \sum_i a_i A|v_i\rangle. \tag{2.2.21}$$

2) Properties of Linear operators

(1) Eigenvector and Eigenvalues

For a linear operator A, if

$$A|v\rangle = \lambda|v\rangle, \tag{2.2.22}$$

then $|v\rangle$ is an eigenvector and λ is a corresponding eigenvalue. The eigenvector and eigenvalues can be solved using the characteristic function,

$$c(\lambda) = \det|A - \lambda I|. \tag{2.2.23}$$

(2) Composition

There are two kinds of composition for different operators, i.e., multiplication and tensor operator. The multiplication of two operators is defined as following. Let $A : \mathbb{V} \to \mathbb{W}$, $B : \mathbb{W} \to \mathbb{X}$, $BA : \mathbb{V} \to \mathbb{X}$. Then

$$BA|v\rangle = B(A|v\rangle \to C = BA. \tag{2.2.24}$$

The tensor operator may be described as follows. Suppose that $|v\rangle$ and $|w\rangle$ are vectors in $\mathbb{V}$ and $\mathbb{W}$, and A and B are linear operators on spaces $\mathbb{V}$ and $\mathbb{W}$, respectively. If these operators satisfy the following condition,

$$(A \otimes B)(|v\rangle \otimes |w\rangle) = A|v\rangle \otimes B|w\rangle, \tag{2.2.25}$$

then the tensor operator $C = A \otimes B$ is a linear operator.

(3) Commutator and anti-commutator

Define two relationships which are often used in quantum mechanics,

$$\begin{cases} [A, B] = AB - BA, \\ \{A, B\} = AB + BA. \end{cases} \tag{2.2.26}$$

If $[A, B] = 0$, the operator A commutes with the operator B. While if $\{A, B\} = 0$, the operator A anti-commutes with the operator B.

3) Representations of Linear operators

In the quantum private communication, there are three kinds of representations for a linear operator. One is the operator representation form which is often used in the quantum mechanics subsequently called briefly the "quantum form" or operator form, and the remainder is the matrix representation form the outer product form.

(1) Operator Form

This is a general representation form, which is widely used in quantum mechanics. For example, the position is denoted by $\hat{x}$. More details will be introduced in next section.

(2) Matrix representation

Suppose that $A : \mathbb{V} \to \mathbb{W}$ is a linear transform between vector spaces $\mathbb{V}$ and $\mathbb{W}$, and $|v_j\rangle$ with $j = 1, 2, \ldots, m$ is a basis for $\mathbb{V}$ and $|w_i\rangle$ with $i = 1, 2, \ldots, n$ is a basis for $\mathbb{W}$, one easily has

$$A|v_j\rangle = \sum_i A_{ij}|w_i\rangle, \tag{2.2.27}$$

where $A_{ij} = \langle w_i|A|v_j\rangle$ is the element of a matrix representation of the operator A. Apparently, given the operator A and two involved bases, i.e., $|v_j\rangle$ and $|w_i\rangle$, the matrix representation of the operator A is calculated.

If A has eigenvectors, the operator A must be diagonalized, i.e.,

$$A|j\rangle = \lambda_j|j\rangle \Rightarrow A_{ij} = \lambda_j \delta_{ij}. \tag{2.2.28}$$

That is, the matrix representation is diagonalized.

(3) Outer product

Let A be a linear transformation from vector space $\mathbb{V}$ to $\mathbb{W}$, and $|v\rangle \in \mathbb{V}$, $|w\rangle \in \mathbb{W}$. Then the linear operator is represented by

$$A = |v\rangle\langle w|.$$

This form is called the outer product. Obviously, the outer product is different from the inner product. The former is an operator and the later is a complex number. Applying this operator on a state $|k\rangle$ gives

$$A|k\rangle = (|v\rangle\langle w|)|k\rangle = |v\rangle(\langle w|k\rangle). \tag{2.2.29}$$

Completeness relation If $A|i\rangle = \lambda_i|i\rangle$, one has $A = \sum_i \lambda_i|i\rangle\langle i|$. When $\lambda_i \equiv 1$,

$$I = \sum_i |i\rangle\langle i|. \tag{2.2.30}$$

Let $|i\rangle$ be any orthogonal basis for the vector space $\mathbb{V}$, and $|v\rangle = \sum_i c_i|i\rangle$, $|w\rangle = \sum_j d_j|j\rangle$, then

$$A = |v\rangle\langle w| = \sum_i c_i|i\rangle \left(\sum_j d_j|j\rangle\right)^* = \sum_{i,j} c_i d_j^*|i\rangle\langle j|. \tag{2.2.31}$$

In addition,

$$A = I_w A I_v = \sum_{ij} \langle w_j|A|v_i\rangle|w_j\rangle\langle v_i|. \tag{2.2.32}$$

There is a useful tool which is called Cauchy-Schwarz inequality: Any two vectors $|v\rangle$ and $|w\rangle$ satisfy

$$|\langle v|w\rangle|^2 \leq \langle v|v\rangle\langle w|w\rangle. \tag{2.2.33}$$

(4) Operator function

The so-called operator function is defined as follows. It is employed in many situations.

Definition 2.2.8 Give an operator A, if its matrix representation may be dialogized, one may define an operator function $f(A)$. Let $A = \sum_i^n a_i|i\rangle\langle i|$, the operator function has the following form,

$$f(A) = \sum_i^n f(a_i)|i\rangle\langle i|. \tag{2.2.34}$$

As an example, giving an operator Z,

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{2.2.35}$$

one may write out

$$\exp(\theta Z) = \begin{pmatrix} \mathrm{e}^{\theta} & 0 \\ 0 & \mathrm{e}^{-\theta} \end{pmatrix}. \tag{2.2.36}$$

(5) Trace of matrix

Definition 2.2.9 The trace of operator A is defined to be the sum of its diagonal elements, i.e.,

$$Tr(A) = \sum_{i}^{n} A_{i,i}. \tag{2.2.37}$$

The trace has the following properties.

$$\begin{cases} Tr(AB) = Tr(BA), \\ Tr(A+B) = Tr(A) + tr(B), \\ Tr(zA) = zTr(A), \\ Tr(ABC) = Tr(BCA) = tr(CAB), \\ Tr(A|\psi\rangle\langle\psi|) = \sum_{i} \langle i|A|\psi\rangle\langle\psi|i\rangle = \langle\psi|A|\psi\rangle. \end{cases} \tag{2.2.38}$$

2.2.4 Several Important Operators

Making use of the above theory for linear operators, some important operators which are often employed in the quantum cryptology and quantum private communication are introduced.

1) Identity Operator

Let $|\varphi\rangle$ be any vector in space $\mathbb{V}$. If the following relation exists,

$$I|\varphi\rangle = |\varphi\rangle, \tag{2.2.39}$$

the operator I is called the identity operator. The matrix representation of the identity operator is

$$I = (I_{ii}). \tag{2.2.40}$$

And its outer product representation is

$$I = \sum_{i} |i\rangle\langle i|. \tag{2.2.41}$$

2) Hermitian Operator

To define the Hermitian operator, the complex conjugate operator needs first to be defined. Let A be an operator, the complex conjugate operator of A is complex conjugate and then transpose it, i.e.,

$$A^{\dagger} = (A^{*})^{\mathrm{T}}, \tag{2.2.42}$$

where superscripts $*$ and T denote the complex conjugate and transpose, respectively.

Using the complex conjugate operator, the Hermitian operator is defined as follows,

$$A^{\dagger} = A. \tag{2.2.43}$$

One may also define the Hermitian operator using the notation in the inner product of vectors. Let $|\phi\rangle$ be an any vector in the space $\mathbb{V}$, if the following relation exists,

$$(|\phi\rangle, A|\varphi\rangle) = (A|\phi\rangle, |\varphi\rangle), \tag{2.2.44}$$

the operator A is a Hermitian operator.

3) Unitary Operator

Let U be a linear operator, if the following condition satisfies,

$$U^{\dagger}U = UU^{\dagger} = I, \tag{2.2.45}$$

the operator U is a unitary operator.

Example 1 The Hadamard matrix H is a unitary matrix. In the matrix form, it is denoted,

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{2.2.46}$$

In the outer product form, above equation yields,

$$H = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|) = \frac{1}{\sqrt{2}} \sum_{i,j=0}^{1} (-1)^{i \cdot j} |i\rangle\langle j|. \tag{2.2.47}$$

In addition, one may easily check that

$$H^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{i,j=0}^{1} (-1)^{i \cdot j} |i\rangle\langle j|. \tag{2.2.48}$$

Example 2 The permutation matrices are unitary matrices. For the 2 by 2 permutation matrices,

$$P_2^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad P_2^1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{2.2.49}$$

The 3 by 3 permutation matrices

$$P_3^0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \; P_3^1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \; P_3^2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}. \tag{2.2.50}$$

4) Project Operator

If $|\psi\rangle = a|\phi\rangle + b|\varphi\rangle$, then $P|\psi\rangle = a|\phi\rangle$ and $P|\psi = b|\varphi\rangle$. The project operator is a special Hermitian operator.

$$P = \sum_{i=1}^{d} |i\rangle\langle i|. \tag{2.2.51}$$

One may easily check that

$$P^\dagger = P, \;\; P^2 = P. \tag{2.2.52}$$

For example, the basis is $\{|0\rangle, |1\rangle\}$ in the 2-dimension $\mathscr{H}_2$. For an arbitrary vector $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, applying a project operator $P = |0\rangle\langle 0|$ on it yields $P|\psi\rangle = (|0\rangle\langle 0|)(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle$. If $P = |0\rangle\langle 1|$, one may obtain $P|\psi\rangle = \beta|1\rangle$.

5) Positive Operator

For any $|\phi\rangle \in \mathscr{H}$, if $(|\phi\rangle, L|\phi\rangle) \geq 0$, the operator L is called the positive operator. If $(|\phi\rangle, L|\phi\rangle) > 0$, L is a positive-definite operator.

The positive operator has been widely used in the positive operator value measurement which is a basic tool for some quantum key distribution scheme such as B92 protocol (please refer to Chapter 4).

6) Normal Operator

Let N be an operator on a finite-dimensional inner product space, N is said to be normal if $N^\dagger N = NN^\dagger$. One can show that N is normal if and only if it is unitarily diagonalizable: using the Schur decomposition gives

$$N = UTU^\dagger, \tag{2.2.53}$$

where U is unitary and T is upper-triangular. Since N is normal, one has

$$TT^\dagger = T^\dagger T. \tag{2.2.54}$$

Therefore T must be diagonal. The converse is straightforward.

In other words, N is normal if and only if there exists a unitary matrix U such that

$$N = U\Lambda U^\dagger, \tag{2.2.55}$$

where Λ is a diagonal matrix, the entries of which are the eigenvalues of N. The column vectors of U are eigenvectors of N, and they are orthogonal. Unlike the Hermitian case, the entries of N need not be real.

7) Pauli Matrices

Pauli matrices are defined as follows,

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{2.2.56}$$

$$\sigma_2 = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}, \qquad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{2.2.57}$$

where σ_0 is actually an identity matrix with order 2. The special unitary group $SU(2)$ is a Lie group, and its Lie algebra is the set of the anti-Hermitian 2×2 matrices with trace 0. Direct calculation shows that the Lie algebra $SU(2)$ is a 3-dimension real algebra spanned by the set $\mathrm{i}\sigma_j$. In symbols, $SU(2) = span\{\mathrm{i}\sigma_1, \mathrm{i}\sigma_2, \mathrm{i}\sigma_3\}$. Accordingly, $\mathrm{i}\sigma_j$ can be seen as infinitesimal generators of $SU(2)$. Together with the matrix $\mathrm{i}\sigma_0$, four Pauli matrices are generators of Lie algebra $U(2)$ group.

Pauli matrices have the following properties,

$$\sigma_0^2 = \sigma_1^2 = \sigma_2^2 = \sigma_3^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{2.2.58}$$

$$\sigma_1\sigma_2 = \mathrm{i}\sigma_3, \qquad \sigma_2\sigma_3 = \mathrm{i}\sigma_1, \qquad \sigma_3\sigma_1 = \mathrm{i}\sigma_2, \tag{2.2.59}$$

and

$$\sigma_i\sigma_j = -\sigma_j\sigma_i, \tag{2.2.60}$$

where $i, j \in \{1, 2, 3\}$ and $i \neq j$. The above properties can be summarized by

$$\sigma_i\sigma_j = \mathrm{i}\varepsilon_{ijk}\sigma_k + \delta_{ij}I. \tag{2.2.61}$$

The Pauli matrices obey the following commutation and anticommutation relations,

$$[\sigma_i, \sigma_j] = 2\mathrm{i}\varepsilon_{ijk}\sigma_k, \tag{2.2.62}$$

$$\{\sigma_i, \sigma_j\} = 2\delta_{ij}I, \tag{2.2.63}$$

where ε_{ijk} is a Levi-Civita symbol and δ_{ij} is a Kronecker delta.

Making use of Pauli matrices, a quadric form is constructed,

$$T^{(2)} = \mathrm{i}\sigma_3, \qquad T^{(3)} = \mathrm{i}\sigma_2, \qquad T^{(4)} = \mathrm{i}\sigma_1. \tag{2.2.64}$$

With these nontrivial matrices, a 2^L-dimension matrix representations of $\mathrm{Clifford}_{2L-1}$ is constructed as follows [**?**],

$$\begin{aligned} G^{(2k)} &= \mathrm{i}^{k-1} I_2^{\otimes(L-1-k)} \otimes T^{(3)} \otimes \left(T^{(2)}\right)^{\otimes(k-1)}, \\ G^{(2k+1)} &= \mathrm{i}^{k-1} I_2^{\otimes(L-1-k)} \otimes T^{(4)} \otimes \left(T^{(2)}\right)^{\otimes(k-1)}, \end{aligned} \tag{2.2.65}$$

where the symbol $A^{\otimes m}$ denotes m times Kronecker products of the matrix A. The constructed matrices may be employed in the orthogonal code designs of the signal processing in the communication system.

2.2.5 Matrices Decomposition

As well known, an arbitrary linear transformation can be expressed formally by $\mathbf{y} = M\mathbf{x}$, where $\mathbf{x}, \mathbf{y}$ are vectors and M denotes a transformation matrix. When the size of the matrix M is very larger the issue of the matrix decomposition becomes significant. Especially, the so-called fast decomposition algorithm is necessary in the practical application.

The matrix decomposition is a kind of factorization of that an arbitrary matrix is decomposed into some canonical form. Generally, there are many factorization approaches for a factorable matrix. Of those factorization ways, the fast matrix decomposition algorithm plays an important role in the information transformation and information processing, such as the well-known fast Fourier transformation (FFT).

1) Spectral Decomposition

Theorem 2.2.2 Any normal operator N on a vector space $\mathbb{V}$ is diagonal with respect to some orthogonal bases for $\mathbb{V}$. Conversely, any diagonalized operator is normal [**?**].

Let $N = \sum_i \lambda_i |i\rangle\langle i|$, λ_i are the eigenvalues of N, and $|i\rangle$ is an orthogonal basis for $\mathbb{V}$, then

$$N = \sum_i \lambda_i |i\rangle\langle i| = \sum_i \lambda_i P_i, \tag{2.2.66}$$

where P_i are projectors.

2) Singular Value Decomposition

In linear algebra, the singular value decomposition (SVD) is an important factorization of the rectangular real or complex matrix, with several applications in signal processing and statistics.

The SVD can be seen as a generalization of the spectral theorem to arbitrary, not necessarily square, matrices. The spectral theorem says that normal matrices can be unitarily diagonalized using a basis of eigenvectors.

Suppose that M is an m-by-n matrix whose entries come from the field $\mathbb{K}$, which is either the field of real numbers or the field of complex numbers. Then there exists a factorization of the form

$$M = U\Sigma V^\dagger, \tag{2.2.67}$$

where U is an m-by-m unitary matrix over $\mathbb{K}$, the matrix Σ is m-by-n with nonnegative numbers on the diagonal and zeros off the diagonal, and $V^\dagger$ denotes the conjugate transpose of V, an n-by-n unitary matrix over $\mathbb{K}$. Such a factorization is called a singular-value decomposition of M.

3) Polar Decomposition

The polar decomposition of complex matrix A is a matrix decomposition of the form

$$A = UP, \tag{2.2.68}$$

where U is a unitary matrix and P is a positive-definite Hermitian matrix. This decomposition exists and is unique as long as A is invertible. The matrix P is given by

$$P = \sqrt{A^\dagger A}. \tag{2.2.69}$$

This expression is meaningful since a positive-definite Hermitian matrix has a unique positive square root.

Note that

$$\det A = \det P \det U = r\mathrm{e}^{\mathrm{i}\theta} \tag{2.2.70}$$

gives the corresponding polar decomposition of the determinant of A, since

$$\det P = r = |\det A| \tag{2.2.71}$$

and

$$\det U = \mathrm{e}^{\mathrm{i}\theta}. \tag{2.2.72}$$

This is why it is called as the polar decomposition for a matrix or linear operator.

2.3 Introduction to Quantum Mechanics

Since quantum mechanics is the cornerstone of the quantum cryptography and quantum private communication, this section introduces briefly the fundamental principles of quantum mechanics. Mainly, notions of quantum system, evolution and measurement of the quantum system are focused.

2.3.1 Quantum Systems

Some readers who have no physical background often give rise to the following question when they first meet the quantum system, that is: what is "quantum"? It seems that the notion quantum is so strange to them since it deviates from the reality so far. Yes, the quantum is certainly an unusual notion, since it is associated with the basic physics properties of a quantum system, i.e., the famous wave-particle duality proposed by Einstein [**?**]. Briefly, a quantum is a system which integrates characteristics of the particle-like behavior and wavelike behavior. Such a system is often called a quantum system.

To define exactly the quantum system is difficult. Generally, a physical system which must be described using quantum mechanics may be called the quantum system. For example, a single particle system is a quantum system, such as both "one photon" system and "one electron" system are all quantum systems. Actually, some multi-particles systems, such as the system with a few photons, and the system with a few electrons, are also quantum systems.

In addition, some physical freedoms of particles, such as phase or polarization of photon may be regarded as a quantum system.

To understand a quantum system one has to know the state at a certain time and the evolution way of the quantum system. In addition, from the viewpoint of the information, one has still to know how to retrieve the useful information which is carried beforehand by the quantum system. However, there are no theory, no logic derivation, and just postulates for describing the quantum system! This subsection describes these postulates and the basic theory followed by these postulates.

Postulate 1 Associated to any isolated physical system is a complex vector space with the inner product (i.e., Hilbert space $\mathscr{H}$) known as the state space of a system. A system is completely described by its state vector, which is a unit vector in the system's state space. This kind of states is called as the pure state.

Example Consider a single particle system, e.g., a quantum system with one photon or one electron. In such a kind of quantum systems, suppose that the state may be described in the 2-dimension Hilbert space, i.e., $\mathscr{H}_2$. Since the basis in a 2-dimension Hilbert space may be denoted as $\{|0\rangle, |1\rangle\}$, then an arbitrary vector in $\mathscr{H}_2$ is expressed as

$$|\psi_2\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{2.3.1}$$

where $|\alpha|^2 + |\beta|^2 = 1$, which is obtained from the normalization condition $\langle\psi_2|\psi_2\rangle = 1$. According to Postulate 1, the state vector $|\psi_2\rangle \in \mathscr{H}_2$ describes the state of the introduced quantum system, and it is a pure state.

In a 3-dimension Hilbert space $\mathscr{H}_3$, the basis is $\{|0\rangle, |1\rangle, |2\rangle\}$, and an arbitrary vector in such a kind of the Hilbert space is expressed as

$$|\psi_3\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle, \tag{2.3.2}$$

with the normalization condition $|\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1$

Generally, in a q-dimension Hilbert space $\mathscr{H}_q$, if the basis may be denoted $\{|0\rangle, |1\rangle, \ldots, |q-1\rangle\}$, an arbitrary vector is expressed as

$$|\psi_q\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \ldots + \alpha_{q-1}|q-1\rangle, \tag{2.3.3}$$

with the normalization condition $|\alpha_1|^2 + |\alpha_2|^2 + \ldots + |\alpha_{q-1}|^2 = 1$.

Postulate 2 The state space of a composite system is the tensor product of state space of component physical systems. Moreover, if one has system numbered 1 through n, and system number j is prepared in a pure state, then the joint system of the total system is a tensor product of these pure states.

A multi-particle system is a kind of composite quantum systems, to describe such a kind of quantum systems, one may follow the postulate 2. Consider here a two-particle system, i.e., particle 1 and particle 2. In a

2-dimension Hilbert space, the states of particle system are denoted,

$$\begin{cases} |\psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle, \\ |\psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle. \end{cases} \tag{2.3.4}$$

Then state of the total system may be written as

$$|\Psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle = \alpha_1\alpha_2|00\rangle + \alpha_1\beta_1|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle. \tag{2.3.5}$$

Generally, the state $|\Psi\rangle$ of two particles in $\mathscr{H}_2$ can be expressed as

$$|\Psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle = \sum_{i,j=0}^{1} a_{i,j}|i\rangle|j\rangle. \tag{2.3.6}$$

If the state $|\Psi\rangle$ can be decomposed into tensor product of two particle states $|\psi_1\rangle$ and $|\psi_2\rangle$, i.e., $|\Psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$, the total state is called the product state. In this case, two particles are independent. However, if the decomposition is impossible, such kind of quantum systems is called the entangled quantum system. The corresponding state is called the entanglement state. The entanglement state is very important in the quantum information. The well-known Bell states are important two particles entanglement states. They have the following forms

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right), \tag{2.3.7}$$

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right). \tag{2.3.8}$$

Another important entanglement state is the so-called Greenberger-Horne-Zeilinger (GHZ) triplet state which is a 3-particle system in $\mathscr{H}_2$. One of such states is expressed as follows

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle \pm |111\rangle\right). \tag{2.3.9}$$

Generally, a q-particle system in $\mathscr{H}_2$ can be expressed as

$$|\Psi\rangle = \sum_{i_1,i_2,\ldots,i_k=0}^{1} \alpha_{i_1 i_2 \ldots i_k}|i_1\rangle|i_2\rangle \ldots |i_k\rangle. \tag{2.3.10}$$

In the 3-dimension Hilbert space $\mathscr{H}_3$, let $\{|0\rangle, |1\rangle, |2\rangle\}$ be the basis in $\mathscr{H}_3$ and the state of an arbitrary single quantum system be

$$|\psi_1\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle\},$$

then the state of a total system for a 3-particle system is

$$|\Psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes |\psi_3\rangle, \tag{2.3.11}$$

where $|\psi_2\rangle$ and $|\psi_3\rangle$ have similar expressions as the state $|\psi_1\rangle$. As an example, one may write out the Aharonov state which is a well-known entanglement state for the three-particle quantum system in $\mathscr{H}_3$,

$$|\Psi\rangle = \frac{1}{\sqrt{6}}\left(|012\rangle + |120\rangle + |201\rangle - |012\rangle - |102\rangle - |210\rangle\right). \tag{2.3.12}$$

A composite system is not always a pure state. If all components of the composite system are integrated with certain probabilities $p_i, i = 1, 2, \ldots, n$, the composite system is a mixed state. In this case, a new notion called the density matrix ρ is introduced to describe the state of the composite system. The pure state is an especial case of the mixed state. For the pure state, we have demonstrated that the state of the quantum system may be described using a vector $|\psi\rangle \in \mathscr{H}$. In this case, the corresponding density is just the outer product of the state vector, i.e., $\rho_0 = |\psi\rangle\langle\psi|$. In the general situation, the state of the quantum system reads

$$\rho = \sum_{i=1}^{n} p_i \rho_i, \tag{2.3.13}$$

where p_i and ρ_i are, respectively, the probability and density of the ith subsystem of the total quantum system. The involved subsystems may be pure states.

2.3.2 Dynamic Characteristics of Quantum Systems

The evolution of quantum systems implies state change of involved quantum systems with time. With the evolution one may know the dynamics behaviors of quantum systems. To describe the evolution one has to understand a new postulate.

Postulate 3 The evolution of a closed quantum system is described by a unitary transformation. That it, the state $|\psi\rangle$ of the system at a time t_1 is related to the state $|\psi'\rangle$ of the system at a time t_2 by a unitary operator U which depends only on the time t_1 and t_2,

$$|\psi'\rangle = U|\psi\rangle \tag{2.3.14}$$

Postulate 3 may be presented in differential equation form. This leads the well-known Schrödinger equation. In the following, we show how to derive this equation although it actually is a postulate without derivation.

Denote t_1 by t_0, and t_2 by $t_0 + \Delta t$, Eq.(2.3.14) is rewritten as

$$|\psi(t_0 + \Delta t)\rangle = U(t_0 + \Delta t, t_0)|\psi(t_0)\rangle. \tag{2.3.15}$$

In addition,

$$|\psi(t_0)\rangle = U(t_0, t_0)|\psi(t_0)\rangle. \tag{2.3.16}$$

Then

$$\lim_{\Delta t\to 0}\frac{|\psi(t_0+\Delta t)\rangle-|\psi(t_0)\rangle}{\Delta t}$$
$$=\lim_{\Delta t\to 0}\frac{U(t_0+\Delta t,t_0)-U(t_0,t_0)}{\Delta t}|\psi(t_0)\rangle. \tag{2.3.17}$$

Above equation gives

$$\frac{\partial|\psi(t)\rangle}{\partial t}=\frac{\partial U(\Delta t,t_0)}{\partial t}|\psi(t_0)\rangle. \tag{2.3.18}$$

Generally, a unitary operator and a Hermitian operator has the following relationship,

$$U=\mathrm{e}^{\mathrm{i}\alpha K}, \tag{2.3.19}$$

where K is a Hermitian operator. Then

$$U(t)=\mathrm{e}^{\mathrm{i}\alpha H(t-t_0)}, \tag{2.3.20}$$

and

$$\frac{\partial U(\Delta t,t_0)}{\partial t}=\mathrm{i}\alpha H\mathrm{e}^{\mathrm{i}\alpha H(t-t_0)}, \tag{2.3.21}$$

with H being a Hermitian operator called the Hamiltonian operator which is independent on the time t. Subsequently, one has

$$\frac{\partial|\psi(t)\rangle}{\partial t}=\mathrm{i}\alpha HU(t,t_0)|\psi(t_0)\rangle=\mathrm{i}\alpha H|\psi(t)\rangle. \tag{2.3.22}$$

Finally, one obtains the Schrodinger equation

$$\mathrm{i}\hbar\frac{\partial|\psi(t)\rangle}{\partial t}=H|\psi(t)\rangle. \tag{2.3.23}$$

where $\alpha=-1/\hbar$ is used and $\hbar$ denotes the planck constant.

Note:

l) Hamiltonian operator H is associated with the energy of the quantum system, it has a spectral decomposition of energy eigenvectors $H=\sum_i E_i|i\rangle\langle i|$.

2) Eq.(2.3.20) gives the unitary matrix form $U(t)=\mathrm{e}^{-\mathrm{i}H(t-t_0)}/\hbar$, it is unitary.

3) Unitary operation must associate with more than two systems, these systems construct a closed system.

For an open quantum system whose state is a mixed state, the evolution equation is given by the well-known Liouville equation,

$$\frac{\partial\rho}{\partial t}=\mathrm{i}\hbar[H,\rho], \tag{2.3.24}$$

where ρ is a density matrix and H is a Hamiltonian of the mixed system.

2.3.3 Information Retrieval of Quantum Systems

To retrieve useful information, such as the physical information (e.g., physical variables), classic information (e.g., Shannon entropy), and quantum information (e.g., accessible information), from a quantum system, one has to operate this system using proper quantum ways. A quantum operation is denoted using a quantum operator. Generally, the quantum operation includes unitary operation (refer to closed system) and non-unitary operation (refer to opened system). Typical non-unitary operation is the well-known quantum measurement operation. Actually, to obtain wanted information from involved quantum systems, the quantum measurement is always employed.

The quantum measurement is a kind of operations of obtaining information from quantum systems. Similarly, there are no derivations for the quantum measurement. It relies on the following postulate.

Postulate 4 Quantum measurement is described by a collection $\{M_j\}$ of measurement operators. These operators acting on the state space of the system being measured. The index j refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\psi\rangle$ immediately before the measurement then the probability that result j occurs is given by

$$p(j) = \langle\psi|M_j^\dagger M_j|\psi\rangle, \tag{2.3.25}$$

and the state of the system after the measurement is

$$|\psi_j\rangle = \frac{M_j|\psi\rangle}{\sqrt{\langle\psi|M_j^\dagger M_j|\psi\rangle}}. \tag{2.3.26}$$

The measurement operators satisfy the completeness equation

$$\sum_j M_j^\dagger M_j = I. \tag{2.3.27}$$

Postulate 4 illustrates that the quantum measurement destroys the original quantum state, and this is different from the classic measurement. It is worth stressing that the output state of the quantum measurement is probabilistic before performing a suitable measurement. This has been shown clearly in Eq.(2.3.25). However, after having finished the measurement the output is determined.

There is an important property for the quantum measurement which is shown in the following theory.

Theorem 2.3.1 Cascaded measurement is a single measurement: Suppose that $\{L_j\}$ and $\{M_j\}$ are two sets of measurement operators. Then a measurement defined by the measurement operators $\{L_j\}$ followed by a measurement defined by the measurement operators $\{M_j\}$ is physically equivalent to a single measurement defined by measuring operators $\{N_j\}$ with the representation

$$N_j = M_j L_j. \tag{2.3.28}$$

Typically, there are three kinds of quantum measurements, i.e., the general measurement, projective measurement, and positive operator value measurement (POVM). Sometimes the quantum nondemolition (QND) measurement is employed. Follows are definitions of these quantum measurement ways.

1) General measurement

Given a collection $\{M_j\}$ of measurement operators, if the measurement satisfies the completeness equation $\sum_j M_j^\dagger M_j = I$, such kind of measurements is called as the general measurement.

NOTE: There is no restriction for the measurement operator $\{M_j\}$.

2) Projective measurement

Given a Hermitian operator $\{M_j\}$, if M_j can be denoted in spectral decomposition representations: $M_j = \sum_j P_j$ and $M_j M_{j'} = \delta_{jj'} M_j$, where P_j is a projective operator, and $P_j = |j\rangle\langle j|$, then this kind of quantum measurement is called the projective measurement.

For example, the output state of the quantum system $|\psi\rangle$ under the projective measurement is $\dfrac{P_j|\psi\rangle}{\sqrt{p(j)}}$ with probability $p(j) = \langle\psi|P_j\rangle$.

3) POVM measurement

Given a collection of positive operator $\{E_j\}$, and E_j satisfies $\sum_j E_j = I$. Using this kind of operators to measure the quantum system. The corresponding measurement is called the POVM. The probability of outcome j is $p(j) = \langle\psi|E_j|\psi\rangle$ and the state is $\dfrac{E_j|\psi\rangle}{\sqrt{\langle\psi|E_j|\psi\rangle}}$.

For example, given a quantum system described by the vector $|\psi\rangle = |0\rangle$, and construct a POVM operator set $\{E_1, E_2, E_3\}$, where

$$\begin{cases} E_1 = \dfrac{\sqrt{2}}{1+\sqrt{2}}|1\rangle\langle 1|, \\ E_2 = \dfrac{\sqrt{2}}{1+\sqrt{2}}\dfrac{(|0\rangle - |1\rangle)(\langle 0| - \langle 1|)}{2}, \\ E_3 = I - E_1 - E_2. \end{cases} \tag{2.3.29}$$

Obviously, $\sum_{j=1}^{3} E_j = I$ and the elements are positive operators. With measurement operations, the probability of the result of $j = 1$ is $p(1) = \langle\psi|E_1|\psi\rangle = 0$, the result of $j = 2$ is $p(2) = \langle\psi|E_2|\psi\rangle = \sqrt{2}/[2(1+\sqrt{2})]$, and the result of $j = 3$ is $p(3) = \langle\psi|E_3|\psi\rangle = (2+\sqrt{2})/(2+2\sqrt{2})$.

4) Quantum Nondemolition Measurement

Different from the above measurement there is a novel quantum measurement called the QND measurement. The QND measurement is a kind of

measurements on a quantum system, which preserves the integrity of systems and values of measured observable. This allows the exact same system to be measured repeatedly. It is important to note that the term nondemolition does not imply that the wave function fails to collapse. In fact, the QND measurement is best thought of as the ideal quantum projective measurement. For example, most devices are capable of detecting a single particle and measuring its position destroy the particle in the measurement process. Less dramatically, the measurement may simply perturb the particle so that it is not in the measured eigenstate even immediately after the measurement. A perfect QND measurement of a particle's position, in contrast, would leave the particle in its measured position. QND measurements are extremely difficult to carry out experimentally.

In quantum mechanics, the process of a measurement is a subtle interplay between an extraction of the information and a disturbance of the state of quantum systems. A QND measurement minimizes this disturbance by using a particular system-detector interaction that preserves the eigenstate of a suitable operator of the quantum system. This leads to an ideal projective measurement [**?**].

Since every measurement can only give a probabilistic result, to reach a more exact measurement one has to perform a multi-times measurement operation. Generally, N times measurements on a variable A give an average measurement result,

$$E(A) = \sum_j \lambda_j p(j), \tag{2.3.30}$$

where λ_j $(j = 1, 2, \ldots, n)$ is the eigenvalue of the operator A. For a projective measurement,

$$E(A) = \langle A \rangle = \sum_i \lambda_i \langle \psi | P_i | \psi \rangle = \langle \psi | M | \psi \rangle. \tag{2.3.31}$$

and the variance is defined by

$$Var(A) = (\Delta A)^2 = \langle (A - \langle A \rangle^2) \rangle = \langle A^2 \rangle - \langle A \rangle^2, \tag{2.3.32}$$

where $E(\cdot), Var(\cdot)$ denote the average and variance of the variable A, respectively.

The previous descriptions focus on the measurement on a single variable, however, many situations have to suffer measurements for multi-variable. Consider the two-variable quantum system corresponding to two operators A and B. There are two instances. If A commutes with B, i.e., $[A, B] = 0$, then A and B can be exactly measured in simultaneous operations. If A does not commute with B, i.e., $[A, B] = C \neq 0$, then A and B cannot be exactly measured in simultaneous operations. In this scenario, the measurement on A and B gives rise to deviations ΔA and ΔB, and these deviations follow the well-known **Heisenberg uncertainty principle**, i.e.,

$$V(A)V(B) \geq \frac{1}{4} |\langle [A, B] \rangle|^2. \tag{2.3.33}$$

The uncertainty principle states the pairs of conjugate variables cannot both be measured with arbitrary precision. That is, the more precisely one variable is known, the less precisely the other is known. This is not a statement about the limitations of a observer's ability to measure particular quantities of a system, but rather about the nature of system itself. Any measurement on the variable corresponding to the operator A with accuracy of very small $V(A)$ collapses the quantum state and cause to the standard deviation $V(B)$ of the variable corresponding to the operator B larger than.

Let $|\psi\rangle$ and $|\phi\rangle$ be two different quantum states. If $|\psi\rangle$ and $|\phi\rangle$ are orthogonal, they can be distinguished. If $|\psi\rangle$ and $|\phi\rangle$ are non-orthogonal, i.e., $\langle\phi|\psi\rangle \neq 0$, they cannot be distinguished.

Theorem 2.3.2 Any two orthogonal states can be distinguished, but any two non-orthogonal states cannot be distinguished exactly.

Proofs Let $|\psi\rangle$ and $|\phi\rangle$ be two arbitrary states. If $\langle\phi|\psi\rangle = 0$, i.e., $|\psi\rangle$ and $|\phi\rangle$ are orthogonal. Construct a measurement operator $E_1 = |\phi\rangle\langle\phi|$ and $E_2 = I - |\psi\rangle\langle\psi|$, then E_1 and E_2 satisfy the completeness equation. Since $\langle\phi|E_1|\phi\rangle = 1$ and $\langle\psi|E_2|\psi\rangle = 1$, the states can be distinguished. If $\langle\phi|\psi\rangle \neq 0$, suppose that $|\psi\rangle$ and $|\phi\rangle$ can be distinguished. Defining E_i $(i = 1, 2)$ as previous. Then one has

$$\langle\phi|E_1|\phi\rangle = 1, \qquad \langle\psi|E_2|\psi\rangle = 1. \tag{2.3.34}$$

Since $\sum_i E_i = I$, it follows that $\sum_i \langle\phi|E_i|\phi\rangle = 1$. Since $\langle\phi|E_1|\phi\rangle = 1$, we have $\langle\phi|E_2|\phi\rangle = 0$. This gives $\sqrt{E_2}|\phi\rangle = 0$. Let $|\psi\rangle = a|\phi\rangle + b|\phi^{\perp}\rangle$, we have $\sqrt{E_2}|\psi\rangle = \sqrt{E_2}|\phi^{\perp}\rangle$. Thus $\langle\psi|E_2|\psi\rangle = b^2 \neq 1$, this contradicts the suppose.

2.3.4 Fundament of Quantum Optics

Like in the Shannon private communication, continuous variables are always adopted in the quantum private communication. For convenience, some quantum optical notions are recalled briefly. The involved continuous variable quantum states include coherent states and squeezed states. They may be described in a uniform way. According to quantum optics theory [**?**], the quantized optical electromagnetic field is represented,

$$E(r,t) = \mathrm{i}\sum_k \left(\frac{\hbar\omega_k}{2\varepsilon_0}\right)[\hat{a}_k\mu_k(r)\mathrm{e}^{-\mathrm{i}(\omega_k t)} - \hat{a}_k^{\dagger}\mu_k^{*}(r)\mathrm{e}^{\mathrm{i}(\omega_k t)}], \tag{2.3.35}$$

where k represents a set of optic field modes, ε_0 is dielectric constant, and i is a unit of imaginary number. A set of vector mode functions $\mu_k(r)$ which correspond to the frequency ω_k satisfy the transversality condition,

$$\bigtriangledown \cdot \mu_k(r) = 0,$$

and the mode functions form a complete orthogonal set,

$$\int \mu_k(r)\mu_k^*(r)\mathrm{d}r = \delta_{kk'}.$$

In the classical electromagnetic theory, a_k and a_k^* are Fourier amplitudes which are complex vectors. In quantization of the electromagnetic field, $\hat{a}_k$ and $\hat{a}_k^\dagger$ are annihilation operators and creation operators, respectively, which are satisfied with boson commutation relation,

$$[\hat{a}_k, \hat{a}_{k'}] = [\hat{a}_k^\dagger, \hat{a}_{k'}^\dagger] = 0, \qquad [\hat{a}_k, \hat{a}_{k'}^\dagger] = \delta_{kk'}. \tag{2.3.36}$$

Therefore, in quantum optics theory, dynamical behaviors of amplitudes are described by an ensemble of independent quantum harmonic oscillators which are expressed in terms of infinite dimension creation and annihilation operators, obeying the above commutation relationships. The quantum state of each mode may be described by a state vector $|\varphi\rangle_k$ in infinite dimension Hilbert spaces.

Let us further illuminate the meaning of quantum harmonic oscillators by looking at a single frequency mode of the electric field for a single polarization. The Hamiltonian for the electromagnetic field in each mode is given by

$$\hat{H}_k = \hbar\omega_k \left(\hat{a}_k^\dagger \hat{a}_k + \frac{1}{2}\right) = \hbar\omega_k \left(\hat{n} + \frac{1}{2}\right), \tag{2.3.37}$$

where the number operator $\hat{n} = \hat{a}_k^\dagger \hat{a}_k$ and $\frac{1}{2}\hbar\omega_k$ denotes the energy of the vacuum fluctuations in each mode.

It is well known that the complex amplitude of classical electromagnetic is sum of real part and imaginary part which is called as "position" and "momentum", respectively. Similarly, define a family of operators with the commutation relations in terms of "position" and "momentum" operators,

$$\begin{cases} \hat{a}_k = \dfrac{1}{\sqrt{2}}\left(\sqrt{\dfrac{\omega_k}{\hbar}}\hat{x}_k + \mathrm{i}\sqrt{\dfrac{1}{\hbar\omega_k}}\hat{p}_k\right), \\ \hat{a}_k^\dagger = \dfrac{1}{\sqrt{2}}\left(\sqrt{\dfrac{\omega_k}{\hbar}}\hat{x}_k - \mathrm{i}\sqrt{\dfrac{1}{\hbar\omega_k}}\hat{p}_k\right). \end{cases} \tag{2.3.38}$$

Now define a pair of conjugate variables in infinite dimension Hilbert spaces,

$$\begin{cases} X_k \equiv \sqrt{\dfrac{\omega_k}{2\hbar}}\hat{x}_k = \mathrm{Re}\{\hat{a}_k\}, \\ P_k \equiv \dfrac{1}{\sqrt{2\hbar\omega_k}}\hat{p}_k = \mathrm{Im}\{\hat{a}_k^\dagger\}, \end{cases} \tag{2.3.39}$$

where $\mathrm{Re}\{\cdot\}$ and $\mathrm{Im}\{\cdot\}$ denotes taking the real and imaginary parts, respectively. According commutation relation in Eq.(2.3.36), one obtains

$$[X_k, P_{k'}] = \frac{\mathrm{i}}{2}\delta_{kk'}. \tag{2.3.40}$$

Inserting Eq.(2.3.40) into Eq.(2.3.33) yields the uncertainty relation for X_k and P_k,

$$V(X_k)V(P_k) \geq \frac{1}{4}|\langle[X_k, P_k]\rangle|^2 = \frac{1}{16}. \tag{2.3.41}$$

For clearly, the single mode case, i.e., the case of $k = k' = 1$, is described in the follows. Making use of Eq.(2.3.39) one may easily obtains

$$\begin{cases} X = \dfrac{1}{2}(\hat{a} + \hat{a}^\dagger), \\ P = \dfrac{1}{2\mathrm{i}}(\hat{a} - \hat{a}^\dagger). \end{cases} \tag{2.3.42}$$

For the single mode electromagnetic field, these operators have the following commutation relations,

$$[X, P] = \frac{\mathrm{i}}{2}. \tag{2.3.43}$$

The canonical quantum quadratures X and P obey the Heisenberg uncertainty relation

$$\Delta X \Delta P \geq \frac{1}{4}, \tag{2.3.44}$$

where $\Delta X = \sqrt{\langle(X - \langle X\rangle)^2\rangle}$ and $\Delta P = \sqrt{\langle(P - \langle P\rangle)^2\rangle}$ are variances of X and P, respectively.

Applying a displacement operator $\hat{D}(\alpha) = \exp(\alpha\hat{a}^\dagger - \alpha^*\hat{a})$ on an arbitrary input mode $\hat{a}_{in}$ yields

$$\hat{a}_{out} = \hat{D}(\alpha)^\dagger \hat{a}_{in} \hat{D}(\alpha) = \hat{a}_{in} + \alpha, \tag{2.3.45}$$

where $\hat{a}_{out}$ denotes the output mode, and α is an arbitrary complex number. The input and output modes have the following relationships,

$$\begin{cases} X_{out} = X_{in} + \mathrm{Re}\{\alpha\}, \\ P_{out} = P_{in} + \mathrm{Im}\{\alpha\}. \end{cases} \tag{2.3.46}$$

Similarly, applying a two-mode squeezing operator $\hat{S}(\xi) = \exp[\kappa t(\hat{a}^\dagger_{in1}\hat{a}^\dagger_{in2} - \hat{a}_{in1}\hat{a}_{in2})]$ on two arbitrary input modes $\hat{a}_{in1}$ and $\hat{a}_{in2}$ yields

$$\begin{cases} \hat{a}_{out1} = \hat{a}_{in1}\cosh(r) + \hat{a}^\dagger_{in2}\sinh(r), \\ \hat{a}_{out2} = \hat{a}_{in2}\cosh(r) + \hat{a}^\dagger_{in1}\sinh(r). \end{cases} \tag{2.3.47}$$

where $r = \kappa t$ is a squeezed parameter. These modes have the following relationships,

$$\begin{cases} X_{out1} = X_{in1}\cosh(r) + X_{in2}\sinh(r), \\ P_{out1} = P_{in1}\cosh(r) - P_{in2}\sinh(r), \\ X_{out2} = X_{in2}\cosh(r) + X_{in1}\sinh(r), \\ P_{out2} = P_{in2}\cosh(r) - P_{in1}\sinh(r). \end{cases} \tag{2.3.48}$$

In this case, the outputs of two modes are entangled. They consist of Einstein-Podosky-Rosen (EPR) states for continuous variables. Generally, with the squeezed parameter r increasing, the EPR correlation between $\hat{a}_{out1}$ and $\hat{a}_{out2}$ becomes increasingly perfect, i.e.,

$$\begin{cases} \lim_{r\to+\infty} X_{out1} = X_{out2}, \\ \lim_{r\to+\infty} P_{out1} = -P_{out2}. \end{cases}$$

Apparently, the condition of $X_{out1} = X_{out2}$ and $P_{out1} = -P_{out2}$ implicates that the employed continuous-variable EPR pair is an ideal entanglement state, i.e., a maximal entanglement state.

To describe generally the entanglement degree of the continuous variables EPR pair, an important parameter is defined,

$$F = \langle(\Delta(X_{out1} - k_1 X_{out2}))^2\rangle_{min} \langle(\Delta(P_{out1} + k_2 P_{out2}))^2\rangle_{min}, \qquad (2.3.49)$$

where k_1 and k_2 are coefficients employed for giving minimum variances of $\Delta X = X_{out1} - k_1 X_{out2}$ and $\Delta P = P_{out1} + k_2 P_{out2}$, respectively. Eq.(2.3.49) gives the lower bound of the parameter F, i.e., $F_l = 0$, at the conditions of the prepared continuous variables EPR pair being a maximal entanglement state and $k_1 = k_2 = 1$, where F_l denotes the lower bound. However, this lower bound $F_l = 0$ is difficult to reach in practices since F_l is associated with the squeezed parameter $r = \kappa t$. Generally, a bigger r corresponds to a smaller lower bound F_l, but there is always $F_l > 0$ in practices. For instance, when two input quantum states are vacuum states, i.e, $\langle(\Delta X_{ink})^2\rangle = \langle(\Delta P_{ink})^2\rangle = \frac{1}{4}, k = 1, 2$, the lower bound $F_l = 4.42 \times 10^{-3}$ with $r = 1$ and $F_l = 2.325 \times 10^{-18}$ with $r = 10$. Once the entanglement correlation was destroyed, F would quickly increases. While two modes are independent, F approaches to infinity. Therefore, the parameter F may be employed to describe the entanglement degree of two-mode entanglement systems [**?**].

2.4 Introduction to Information Theory

The classic information theory, which was founded initially by Shannon, has become an important foundation of the modern communication. The two most important questions answered by this theory are how much can be compressed for a given data source and how much data can be transmitted in a given communication channel. Information theory is of central importance in quantum cryptography as well as quantum private communication. Using this theory one can calculate the security of the employed quantum scheme and information leaked to the attacker. In this section, a combination information theory of classic information theory and quantum information theory is presented.

2.4.1 Entropy

One of basic notions in the information theory is the entropy, which is used to describe the undetermined degree of information systems. There are two kinds of entropies, i.e., the Shannon entropy and von Neumann entropy. The Shannon entropy describes the classic information of message sources or random variables while the von Neumann entropy describes the quantum information of message sources or quantum random variables.

1) Shannon Entropy

Consider a discrete random variable $X = X\{x_i|i = 1, 2, \ldots, n\}$. Let the probability of a variable x_i be p_i, the Shannon entropy of the random variable X is given by the following definition,

$$H(X) = -\sum_{i=1}^{n} p_i \log_2 p_i. \tag{2.4.1}$$

If the random variable X is a continuous variable, i.e., $X = X(x), x \in [a, b]$, the Shannon entropy is defined as follows,

$$H(X) = -\int_a^b p(x) \log p(x) \mathrm{d}x. \tag{2.4.2}$$

When one deals with the information of multi-variable, the conditional entropy $H(X|Y)$ and joint entropy $H(X, Y)$ are necessary. For the discrete variables X and Y, if the joint probability of the variables X and Y is $p(x_i, y_j)$, the conditional entropy is described by

$$H(X\,|Y\,) = -\sum_{i,j} p(x_i, y_j) \log p(x_i\,|y_j\,), \tag{2.4.3}$$

and the joint entropy is

$$H(X, Y) = -\sum_{i,j} p(x_i, y_j) \log p(x_i, y_j). \tag{2.4.4}$$

For the continuous variables X and Y, the conditional entropy is

$$H(X\,|Y\,) = -\iint_s p(x, y) \log p(x\,|y\,) \mathrm{d}x\mathrm{d}y. \tag{2.4.5}$$

While the joint entropy $H(X, Y)$ is defined by

$$H(X, Y) = -\iint_s p(x, y) \log p(x, y) \mathrm{d}x\mathrm{d}y. \tag{2.4.6}$$

The entropy $H(X)$ or $H(Y)$, the conditional entropy $H(X|Y)$ or $H(Y|X)$ and the joint entropy $H(X,Y)$ have the following relations,

$$H(X,Y) = H(X) + H(Y|X) \tag{2.4.7}$$
$$= H(Y) + H(X|Y). \tag{2.4.8}$$

In addition,

$$H(X|Y) \leq H(X), \tag{2.4.9}$$
$$H(Y|X) \leq H(Y). \tag{2.4.10}$$

2) von Neumann Entropy

Suppose that there is a quantum system, its state is described by the density matrix ρ, then the undetermined degree of the quantum system is described by the von Neumann entropy defined as follows,

$$S(\rho) = -Tr\rho \ln \rho, \tag{2.4.11}$$

where Tr denotes the trace of the matrix. Suppose that λ_k $(k = 1, 2, \ldots,)$ are eigenvalues of the matrix ρ, the von Neumann entropy is rewritten as

$$S(\rho) = -\sum_k \lambda_k \ln \lambda_k. \tag{2.4.12}$$

If the state of quantum systems is a pure state, the von Neumann entropy becomes the same as the Shannon entropy in this case.

2.4.2 Mutual Information

In a communication system, the information exchange plays more important role than the entropy. To describe the information exchange the so-called mutual information is employed. Suppose there are two random variables X and Y, the classic information exchange is described using the Shannon mutual information $I(X,Y)$ defined as

$$I(X,Y) = \sum p(x,y) \log_2 \frac{p(y|x)}{p(y)}. \tag{2.4.13}$$

For the continuous variables X and Y, the mutual information $I(X,Y)$ may be expressed as

$$I(X,Y) = \iint_s p(x)p(y\,|x\,) \log \frac{p(y\,|x\,)}{p(y)} \mathrm{d}x\mathrm{d}y. \tag{2.4.14}$$

Similarly, one may acquires

$$I(Y,X) = \sum p(x,y) \log_2 \frac{p(x|y)}{p(x)}. \tag{2.4.15}$$

Using definitions of the entropy, conditional entropy, and joint entropy, one obtains the following expressions,

$$I(X,Y) = H(X) - H(X|Y) \tag{2.4.16}$$
$$= H(Y) - H(Y|X) \tag{2.4.17}$$
$$= H(X) + H(Y) - H(X,Y) \tag{2.4.18}$$

The relationship among the joint entropy, conditional entropy, and Shannon mutual information is plotted in Fig.2.1.

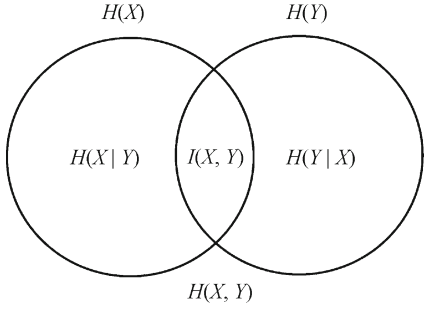

Fig. 2.1. Relationship of entropy and mutual information

As an example, consider a Gaussian source X which satisfies the following distribution,

$$p(x) = \frac{1}{\sqrt{2\pi}\Sigma} \mathrm{e}^{-\frac{x^2}{2\Sigma^2}}, \tag{2.4.19}$$

where Σ denotes the variance of the Gaussian source. Suppose that the channel is an additive white Gaussian noise (AWGN) channel, and the noise distribution satisfies

$$N(x) = \frac{1}{\sqrt{2\pi}\sigma} \mathrm{e}^{-\frac{x^2}{2\sigma^2}}. \tag{2.4.20}$$

Then the conditional probability density is

$$p(y\,|x\,) = \frac{1}{\sqrt{2\pi}\sigma} \mathrm{e}^{-\frac{(y-x)^2}{2\sigma^2}}. \tag{2.4.21}$$

In this case the joint probability density of between the source X and sink Y reads as

$$p(x,y) = p(y\,|x\,)p(x) = \frac{1}{2\pi\Sigma\sigma} \mathrm{e}^{-[\frac{x^2}{2\Sigma^2} + \frac{(y-x)^2}{2\sigma^2}]}. \tag{2.4.22}$$

According to Eq.(2.4.22) one obtains the probability density of the sink Y,

$$p(y) = \int_{-\infty}^{+\infty} p(x,y)\mathrm{d}x = \frac{1}{\sqrt{2\pi}\sqrt{\Sigma^2+\sigma^2}} \mathrm{e}^{-\frac{y^2}{2(\Sigma^2+\sigma^2)}}. \tag{2.4.23}$$

Then, the entropies of the source and sink are respectively,

$$H(X) = -\int_{-\infty}^{+\infty} p(x)\log p(x)\mathrm{d}x = \frac{1}{2}\ln(2\mathrm{e}\pi\Sigma^2), \tag{2.4.24}$$

$$H(Y) = -\int_{-\infty}^{+\infty} p(y)\log p(y)\mathrm{d}x = \frac{1}{2}\ln[2\mathrm{e}\pi(\Sigma^2+\sigma^2)], \tag{2.4.25}$$

the conditional entropy is given by

$$H(X\,|Y\,) = -\iint\limits_s p(x,y)\log p(x\,|y\,)\mathrm{d}x\mathrm{d}y = \frac{1}{2}\ln\left(\frac{2\mathrm{e}\pi\Sigma^2\sigma^2}{\Sigma^2+\sigma^2}\right), \tag{2.4.26}$$

$$H(Y\,|X\,) = -\iint\limits_s p(x,y)\log p(y\,|x\,)\mathrm{d}x\mathrm{d}y = \frac{1}{2}\ln\left[\frac{2\mathrm{e}\pi(\Sigma^2+\sigma^2)\sigma^2}{\Sigma^2+\sigma^2}\right], \tag{2.4.27}$$

the joint entropy is

$$H(X,Y) = -\iint\limits_s p(x,y)\log p(x,y)\mathrm{d}x\mathrm{d}y = \frac{1}{2}\ln[(2\mathrm{e}\pi)^2\Sigma^2\sigma^2], \tag{2.4.28}$$

and the Shannon mutual information is

$$I(X,Y) = \iint\limits_s p(x)p(y\,|x\,)\log\frac{p(y\,|x\,)p(x)}{p(x)p(y)}\mathrm{d}x\mathrm{d}y = \frac{1}{2}\ln\left(1+\frac{\Sigma^2}{\sigma^2}\right). \tag{2.4.29}$$

To describe the information exchange between two quantum systems, e.g., $\mathfrak{Q}$ and $\mathfrak{R}$, one may use the notation of the quantum entropy exchange. Suppose that the initial state of the quantum system $\mathfrak{Q}$ is ρ and the quantum system $\mathfrak{R}$ applies an operation $\mathcal{E}$ on the quantum system $\mathfrak{Q}$. Let the element of the operation $\mathcal{E}$ be $\{\mathbf{E}_i|i=1,2,\ldots,n\}$, then the information exchange arisen by the operation $\mathcal{E}$ is expressed as

$$S(\rho,\mathcal{E}) = S(\mathbf{W}), \tag{2.4.30}$$

where $W_{i.j} \equiv Tr(\mathbf{E}_i\rho\mathbf{E}_j^\dagger)$. Using the quantum information exchange $S(\rho,\mathcal{E})$, a so-called coherence information is defined,

$$I_c(\rho,\mathcal{E}) = S(\mathcal{E}(\rho)) - S(\rho,\mathcal{E}). \tag{2.4.31}$$

The classic information and quantum information are united perfectly in the Holevo bound theorem.

Theorem 2.4.1 (The Holevo bound) [8] Suppose that there is a set of qubits $X = \{(\rho_i,p_i)|i=0,1,2,\ldots,n\}$, where ρ_i, p_i are density and probability of ith qubit, respectively. The observer performs POVM measurement

described by elements $\{E_j\} = \{E_0, E_1, \ldots, E_m\}$ on the qubit X, with measurement output Y. Holevo bound states that for any such measurement, the accessible information $H(X, Y)$ is bounded by the following relations,

$$H(X, Y) \leq S(\rho) - \sum_{i=1}^{n} p_i S(\rho_i), \tag{2.4.32}$$

where $\rho = \sum_i p_i \rho_i$.

The Holevo bound is an exceedingly useful upper bound on the accessible information that plays an important role in many applications of quantum information theory. Since it has been presented in many books, the proof for this theorem is not presented here. One may refer to Ref.[?].

2.4.3 Quantum Fano Inequality

The fidelity is used to describe the similarity of the initial state and final state of a quantum system. Suppose that a quantum system subjects to a quantum operation $\mathcal{E}$, then the fidelity of the state of the quantum system is

$$F(\rho, \mathcal{E}) = Tr\sqrt{\rho^{1/2}\mathcal{E}(\rho)\rho^{1/2}}. \tag{2.4.33}$$

Let $\rho' = \mathcal{E}(\rho)$. If $\rho\rho' = \rho'\rho$, the states ρ and ρ' may be expressed using the same basis,

$$\rho = \sum_i r_i |i\rangle\langle i|, \qquad \rho' = \sum_i s_i |i\rangle\langle i|. \tag{2.4.34}$$

Then one has

$$F(\rho, \rho') = Tr\left(\sum_i \sqrt{r_i s_i |i\rangle\langle i|}\right) = \sum_i \sqrt{r_i s_i}. \tag{2.4.35}$$

In this case, the quantum fidelity is the same as the classic fidelity.

Suppose that the initial state ρ is a pure state $|\psi\rangle$ but the final state ρ' is a mix state. In this case,

$$F(|\psi\rangle, \rho') = Tr\sqrt{\langle\psi|\rho'|\psi\rangle|\psi\rangle\langle\psi|} = \sqrt{\langle\psi|\rho'|\psi\rangle}. \tag{2.4.36}$$

If the initial state and final state are all pure states, i.e., $\rho = |\psi\rangle\langle\psi|$ and $\rho' = |\psi'\rangle\langle\psi'|$, the fidelity is given by

$$F(|\psi\rangle, |\psi'\rangle) = \sqrt{\langle\psi|\psi'\rangle\langle\psi'|\psi\rangle} = |\langle\psi|\psi'\rangle|. \tag{2.4.37}$$

The Fano inequality is an important relation. In the Shannon theory, the Fano inequality reads

$$H(X|Y) \leq H(p_e) + p_e \log_2(|X| - 1), \tag{2.4.38}$$

where p_e is the error probability and $|X|$ is the length of the random variable X. In the quantum information theory, the Fano inequality is given by following expression [**?**],

$$S(\rho, \mathcal{E}) \leq H(F(\rho, \mathcal{E})) + (1 - F(\rho, \mathcal{E})) \log_2(d^2 - 1), \tag{2.4.39}$$

where d is the dimension of the channel, and $H(X)$ is given by

$$H(X) = -X \log_2 X - (1 - X) \log_2(1 - X).$$

2.5 Introduction to Complexity Theory

Complexity theory is concerned with the inherent cost required to solve information processing problems where the cost is measured in terms of various well-defined resources. From the viewpoint of security, two categories of cryptographic algorithms are concerned. One is independent of the computational resources so that its security may reach the unconditional security. Another is associated with the computational resources so that its security relies on the computational complexity theory. It is well-known that securities of many classically cryptographic algorithms are guaranteed by the intractable problems which depend on the classic complexity theory. For instance, the well-known RSA algorithm is associated with the factor decomposition of larger integer which is a class NP. Similarly, when a quantum computer which may be possibly manufactured in the future is employed to analyze the classic or quantum cryptosystem, the quantum complexity theory becomes necessary. This section introduces some basic knowledge on the complexity theory. Based on the quantum complexity theory some quantum cryptosystems, which will be described in Chapter 5, have been proposed.

2.5.1 Turing Machine

In the complexity theory, all problems are reduced to language recognition, where a language is defined as a set of strings over some alphabet, typically $\{0, 1\}$. For example, $L_1 = \{0, 00, 000, \ldots\}$ is the language that contains all strings that contain only the letter 0. Once one has a language L, there are some interesting questions one may ask about it. As an example, given an input x, can a machine decide if $x \in L$? If so, how long does it take to make this decision with respect to the size of the input $|x|$? In order to answer these questions, it is necessary to define a model of computation.

There are many useful models for the computation. Some examples include Boolean circuits, push-down automata with two stacks, Java programs, and TMs. Among these models, the TM is often employed as a basic model. All reasonable deterministic models are essentially equivalent, since

they can simulate one another in polynomial time. Considering that the motivation of this book is for the quantum private communication two kind of Turing machines, i.e., the classic TM and quantum TM are described.

There are many standard variations to the definition of the deterministic TM, none of which affect their computational power. Here TMs with a two-way infinite tape and a single tape head which must move left or right one square on each step are presented. Also, a standard definition for interpreting the input, output, and running time of a deterministic TM is given. As usual, let the TMs with tape head movements $\{L, R\}$, then one arrives at the definition of the deterministic TM.

Definition 2.5.1 A deterministic TM is defined formally by a 3-tuple $DTM = \{\mathscr{Q}, \Sigma, \delta\}$, where, $\mathscr{Q}$ is a finite set of states with an identified initial state q_0 and final state $q_f \neq q_0$, Σ is a finite set of the tape alphabet/symbol with an identified blank symbol #, and δ is a partial function called the transition function,

$$\delta : \mathscr{Q} \times \Sigma \rightarrow \Sigma \times \mathscr{Q} \times \{L, R\}, \tag{2.5.1}$$

with that L and R denote the left shift and right shift, respectively. Note, a relatively uncommon variant allows "no shift", say N, as a third element of the latter set in above expression.

In some scenarios, the probabilistic TMs are often considered. Different from the deterministic TM, a probabilistic TM randomly chooses between the available transitions at each point according to some probability distribution. A probabilistic TM is also called nondeterministic TM which is defined exactly as follows.

Definition 2.5.2 A nondeterministic TM is formally defined as a 3-tuple $PTM = \{\Sigma, \mathscr{Q}, \delta\}$, where $\mathscr{Q}$ is a finite set of states with an identified initial state q_0 and final state $q_f \neq q_0$, Σ is a finite alphabet with an identified blank symbol #, and δ, the nondeterministic transition function, is a probabilistic function

$$\delta \subseteq (\mathscr{Q} \backslash F \times \Sigma) \times (\Sigma \times \mathscr{Q} \times \{L, R\}), \tag{2.5.2}$$

with that F is a set of final states or accepting states.

In the case of equal probabilities for the transition, it can be defined as a deterministic TM having an additional "write" instruction where the value of the write is uniformly distributed in the TM's alphabet (generally, an equal likelihood of writing a "1" or a "0" on to the tape). Another common reformulation is simply a deterministic TM with an added tape full of random bits called the random tape. As a consequence, a probabilistic TM can have stochastic results; on a given input and instruction state machine, it may have different run times, or it may not halt at all. Further, it may accept an input in one execution and reject the same input in another execution.

The quantum TM was introduced firstly by Deutsch [**?**] and was studied by many researchers. Bernstein and Vazirani showed that some theories in

the classic TM can be expanded to the quantum TM [**?**] and they proved that there exists universal quantum TM which computes the functions given by its codes as input data. In 2007, Iriyama and Ohya proposed a generalized quantum TM [**?**]. A quantum TM is an abstract machine used to model the effect of a quantum computer. It provides a very simple model which captures all of the power of quantum computation. Any quantum algorithm can be expressed formally as a particular quantum TM. Thus, the quantum TMs have the same relation to quantum computation that the normal TMs have to classical computation. In addition, the quantum TM can be related to classical and probabilistic TM in a framework based on transition matrices, shown by Lance Fortnow. Actually, a quantum computer is another model of computation that is inherently probabilistic. Exactly, a quantum TM may be defined formally as follows.

Definition 2.5.3 A quantum TM is defined by a triplet $QTM = \{\Sigma, \mathscr{Q}, \delta\}$, where Σ is a finite alphabet with an identified blank symbol $\#$, $\mathscr{Q}$ is a finite set of states with an identified initial state q_0 and final state $q_f \neq q_0$, and δ, the quantum transition function, is a function,

$$\delta : \mathscr{Q} \times \Sigma \to \mathbb{C}^{\Sigma \times \mathscr{Q} \times D}, \tag{2.5.3}$$

with that $D = \{L, R\}$ is the direction in which the tape head moves, and the $\mathbb{C}$ denotes the complex number field whose kth bit can be computed in time polynomial in k.

The configuration of the quantum machine is a superposition of configurations, where a configuration is an element of $\Sigma^{\mathbb{Z}} \times \mathscr{Q} \times \mathbb{Z}$, the first member of which corresponds to the tape contents, the second corresponds to the state, and the last corresponds to the tape head position, where $\mathbb{Z}$ denotes the integer field. The function δ must be unitary. A quantum machine halts when its state is a superposition of only those configurations that are in the final state. The output of the machine is the corresponding superposition of the tape contents. For a decider, the output contains a 0 in the start cell if it rejects, and 1 if it accepts. The probability that the decider accepts is the total amplitude of accepting configurations in its output superposition.

In application, quantum TMs are not always used for analyzing quantum computation. Actually, the quantum circuit is a more common model. Both of these models are computationally equivalent. Some simple quantum circuits are described in Chapter 3. More details may refer to Ref.[**?**].

2.5.2 Classic Complexity

Once have determined that a language is computable with a kind of TMs, how much it costs to decide the language becomes an interesting issue. There are two resources of interest, i.e., the amount of time required, and the amount of space necessary to compute the language. Language are classified into com-

plexity classes according to how much of each of the resources they require. In classic complexity theory, the complexity classes may be divided into the class P, class NP, NP-Complete Language, class BPP, class PSPACE, etc.

If a set of all language that can be computed in a polynomial time on a deterministic TM, such a set is called the class P. For example, sorting a list of elements, computing the maximum flow between two points in a network of pipes and finding the shortest path between two points in a graph are all problems in the class P. Since the class P can be computed in polynomial time, problems in this class cannot be employed for the cryptology and private communication.

The class NP is the set of all languages that can be computed in polynomial time on a nondeterministic TM. Alternatively, the classic NP contains all languages that are verifiable in polynomial time on a deterministic machine. This means that given an input and a certificate of the input's membership in a language, a machine can check if the certificate is valid in polynomial time. Since a deterministic TM is just a specific type of nondeterministic machine, one has $P \subseteq NP$.

The hardest problems in NP are known as the NP-complete (briefly, NPC) language. These languages have an interesting characteristic, i.e., a solver for an NPC language can be used to solve any problem in NP, with only polynomial overhead.

The bounded-error probabilistic polynomial-time (BPP) is the class of decidable problems solvable by a probabilistic TM in polynomial time with an error probability of at most 1/3. Exactly, the class BPP may be described as follows. A language L is in the complexity class BPP, if there exists a probabilistic TM denoted M, that runs in polynomial time such that:

(1) If x is in L, then M accepts x with probability $p \geq 2/3$.

(2) If x is not in L, then M accepts x with probability $p \leq 1/3$.

Note the constant 1/3 is arbitrary. Actually, any constant value in the range $(0, 1/2)$ given an equivalent definition for the class BPP, since repeated executions of the probabilistic machine M on x can bring the probability of correct behavior arbitrarily close to 1.

The class PSPACE is the set of decision problems that can be solved by the TM using a polynomial amount of tape, given an unlimited amount of time. Analogously, the class EXPSPACE is the set of decision problem that can be solved by a TM using an exponential amount of tape with giving an unlimited amount time.

According to the above definitions of various classes, following relations among these classes are presented,

$$P \subseteq NP, \tag{2.5.4}$$

$$P \subseteq BPP, \tag{2.5.5}$$

$$BPP \subset PSPACE, \tag{2.5.6}$$

$$NP \subseteq PSPACE, \tag{2.5.7}$$

$$PSPACE \subset EXPSPACE, \tag{2.5.8}$$

However, the following questions are open,

$$P = NP, \tag{2.5.9}$$

$$BPP \subseteq NP, \quad \text{or}, \quad NP \subseteq BPP, \tag{2.5.10}$$

$$BPP = PSPACE. \tag{2.5.11}$$

The proofs for these relations will not be presented here, the readers who are interesting in these issues may refer to the documents, e.g., Ref.[**?**]

One of the central questions of complexity theory is whether randomness adds power; that is, is there a problem which can be solved in polynomial time by a probabilistic TM but not a deterministic TM? or can deterministic TMs efficiently simulate all probabilistic TMs with at most a polynomial slowdown? It is currently widely believed by researchers that the latter is in the case, which would imply $P = BPP$. The same question for logarithm space instead of polynomial time (does $L = BPLP$?) is even more widely believed to be true. On the other hand, the power randomness gives to interactive proof systems and the simple algorithms it creates for difficult problems such as polynomial-time primarily testing and log-space graph connectedness testing suggest that randomness may add power.

2.5.3 Quantum Complexity

To survey the quantum computability the quantum complexity theory has been investigated by several researchers. The quantum computability depends on the quantum TM which has been defined in previous. Only a few classes such as the class QP and class BQP, have been investigated by far because of the difficulties on investigations. With the obtained results on the class P and class BQP, one may have a glimpse on the quantum computability. Similar to the classic complexity theory, if a set of all languages that can be computed in polynomial time on a quantum TM, such a set is called the class QP. Comparing the class P and class QP, Deutsch has proven the following result [**?**],

$$P \subseteq QP. \tag{2.5.12}$$

The quantum analog to BPP is the class BQP. This consists of all languages for which a quantum machine gives the right answer at least 2/3 of the time. It is currently known that BQP sits between BPP and PSPACE in the complexity hierarchy. Thus one has the following relations,

$$BPP \subseteq BQP \subseteq PSPACE. \tag{2.5.13}$$

For the sake of clarity, this relationship is demonstrated without strictly proofs but with a qualitative description. Bennett showed that any classical circuit can be converted into an equivalent reversible circuit, and further

that this conversion can be done efficiently [**?**]. Immediately, one may conclude that a quantum computer is at least as powerful as a classical computer. Accordingly, there naturally have $BPP \subseteq BQP$ since anything that can be computed on a classical machine can be computed on a quantum machine with little overhead. However, it is not known whether or not this containment is strict. For example, the well-known Shor's algorithm proves that the factorization is in BQP [**?**], while it is not known to be in BPP. In addition, there are problems such as factoring and computing a discrete logarithm that are in BQP but not known to be in BPP, no one has actually proven that these problems are not in BPP.

Similarly, the relation between NP and BQP is unknown. The argument of Bennett, Bernstein, Brassard, and Vazirani that a brute force approach to quantum computation results in only quadratic gains suggests that BQP does not contain NP [**?**]. However, the relationship between NP and BPP is currently unknown, so whether or not NP contains BQP is also unknown.

The follows exemplify the proof that $BQP \subseteq PSPACE$. First, assume that one is simulating a quantum TM $M \in BQP$ for which the transition amplitudes can be computed exactly in polynomial time. Assume that M runs in time $p(n)$, then the depth of $M's$ computational tree is at most $p(n)$. One uses a depth-first search on this computational tree, using at most $p(n)$ space, and adds the amplitude of this path to a running total if the final configuration is accepting. Since this amplitude can be computed exactly in polynomial time, the total only requires polynomial space to store. Now given an arbitrary quantum TM $M' \in BQP$, Bernstein and Vazirani showed that it suffices to use a machine that is similar to M' but for which each transition amplitude can be calculated exactly, and to then compare the total amplitude was computed to 7/12 in Ref.[**?**]. If the amplitude is at least this amount, one accepts. The total space required for this simulation is polynomial, so $BQP \subseteq PSPACE$. Note that the total time required for this simulation is exponential, since the number of possible final configurations is in $O(p(n) \cdot 2^{p(n)})$.

Thus, the class BQP contains all of P and BPP, and potentially some problems in NP but probably none that are NP-complete, and perhaps some problems in PSPACE that are not in NP. The latter two postulations, however, have not been proven.

According to the obtained results for the quantum complexity theory, an initial description on the quantum computability, which is associated with the security of quantum cryptosystem, is presented. It has been shown that any classic circuit can be converted into an equivalent reversible circuit, and further that this conversion can be done efficiently. Accordingly, a quantum computer is at least as powerful as a classic computer.

2.6 Security Model

As mentioned in Chapter 1, the aim of the private communication is to provide confidentiality and authentication during the information exchange procedures among various communicators via a physical communication system. Accordingly, the security for a cryptographic system or a private communication system is significant. Without security guarantee the employed cryptographic system or private communication system is not useful. This has been shown clearly in the classic cryptology and classic private communication. Apparently, there is no exception in the quantum cryptology and quantum private communication. Thus we try to construct a security model for the quantum private communication in this section.

Since Shannon published his paper titled "communication theory of secrecy system" in 1948 [**?**], a trivial model for security has been built. However, the security theory is complex since the exact definition of security would depend on the cryptosystem in question. Actually, a cryptographic system leads a unique security model. Therefore, various systems give rise to many definitions for the security. Some important notions for security have been involved, including, e.g., the information-theoretic security, unconditional security, perfect security, theoretical security, provable security, computational security, etc. This section describes the security model from two aspects: information-theoretic security and computational security. These notions are available for both classic scenarios and quantum scenarios.

2.6.1 Information-theoretic Security

The information-theoretic security is often used interchangeable with unconditional security. However, the latter term can also refer to systems that do not rely on unproven computational hardness assumptions. Today these systems are essentially the same as those that are information-theoretic secure. However, it does not always have to be that way. For example, if one day RSA might be proved secure, then it thus becomes unconditional secure, but it will never be information-theoretic secure. The information-theoretic security may be defined formally as follows.

Definition 2.6.1 A cryptosystem is information-theoretically secure if its security derives purely from information theory. That is, it is secure even when the adversary has unbounded computing resources.

An interesting case in the information-theoretic security is perfect security: an encryption algorithm is perfectly secure if a ciphertext produced using it provides no information about the plaintext without knowledge of the key. If E is a perfectly secure encryption function, for any fixed message m there must exist for each ciphertext c at least one key such that $c = E_k(m)$. It is quite possible, and common for a cryptosystem to leak some informa-

tion, but nevertheless have the property that whatever security properties it achieves hold even when the adversary is computationally unbounded. Such a cryptosystem would have information theoretic but not perfect security.

There are varieties of cryptographic tasks for which information theoretic security or privacy is a meaningful and useful requirement. A few of these are: secret sharing schemes such as Shamir's schemes are information theoretically secure (in fact perfectly secure) in that less than the requisite number of shares of the secret provide no information about the secret. More generally, secure multiparty computation protocols often, but not always have information theoretic security. The private information retrieval with multiple databases can be achieved with information theoretic privacy for the user's query. Symmetric encryption can be constructed under an information theoretic notion of security called entropic security, which assumes that the adversary knows almost nothing about messages being sent. The goal here is to hide all functions of the plaintext rather than all information about it.

When possible, an algorithm or protocol with information theoretic security has advantages: it does not depend on unproven assumptions about computational hardness, and it is not vulnerable to developments in the quantum cryptography and quantum private communication.

Informatically, a cryptosystem with information theoretic security should satisfy the following condition according to the above definition, i.e.,

$$I(M, C) = 0, \tag{2.6.1}$$

which means that the obtained information on the message $m \in M$ is zero when the cipher $c \in C$ is given. Since $I(M, C) = H(M) - H(M|C)$, one may easily obtain

$$H(M) = H(M|C). \tag{2.6.2}$$

Clearly, to guarantee the unconditional security of a cryptographic scheme one should let the ciphertext distribute uniformly. This is concluded with the following theorem.

Theorem 2.6.1 A necessary condition for a cryptographic scheme with perfect privacy is

$$H(K) \geq H(M). \tag{2.6.3}$$

Proof Given the key and cipher are given, one has

$$H(M|KC) = 0,$$

then

$$H(K|C) = H(K|C) + H(M|KC) = H(MK|C).$$

Since

$$H(MK|C) = H(M|C) + H(K|MC) \geq H(M|C),$$

one obtains

$$H(K|C) \geq H(M|C).$$

In addition,

$$I(M,C) = H(M) - H(M|C),$$

and

$$I(K,C) = H(K) - H(K|C).$$

Combining the last three equations reaches the conclusion of the theorem.

In the classic cryptology, the Vernam cipher which is also called one-time pad for binary plaintexts may reach the unconditional security, and this is the only one with unconditional security in the classic cryptology. The perfect privacy has been proven firstly by Shannon in 1948. This algorithm will be discussed in detail in Chapter 6.

Given an arbitrary cryptosystem, the parameter l_0 defined as follows is called unicity distance of the given system under the ciphertext-only attack strategy,

$$l_0 = \min\{l_c \in \mathbb{N} : H(K|C) \approx 0\}, \tag{2.6.4}$$

where $\mathbb{N}$ denotes the set of all positive integers.

According to the above definition, one has $H(K|C) \approx 0$ at $l_c = l_0$, which implies that the key can be determined in principle when $l_c \geq l_0$. Subsequently, the involved cryptographic scheme may be broken. However, when $l_c < l_0$ the key cannot be determined since there are multi-solutions. In this case, the cryptographic scheme cannot be broken.

Eq.(2.6.4) shows that the security (or privacy) of a given cryptosystem depends on the parameter l_0. Thus, one may call the parameter l_0 to be a threshold value for the security of the cryptosystem.

2.6.2 Computational Security

In the cryptography, the system with information-theoretic security is not always necessary in some sense since a practical adversary cannot possess of unbounded computation resources. Consequently, the cryptosystem with computational security is always adopted to reduce the overhead of cost. In fact, secure cryptosystems are defined in terms of their required security properties (e.g., anonymity of voters in an electronic voting system) and what the adversary can do in the system (e.g., voting authorities colluding to find out the vote of an individual). This leads the cryptosystem with computational security.

Generally, a computationally secure cryptosystem is designed under an intractable mathematical problem which is associated with the complexity theory, e.g., the NP problem, class NPC, etc. Of these mathematical problems, some have been proven mathematically. However, most of these problems are only widely believed to be hard to solve but without strictly mathematical proofs, e.g., factorizing a large number or extracting a discrete logarithm. Consequently, many computationally secure cryptosystems

are proposed without strict proofs. In addition, with the development of the complexity theory, some cryptosystems will become insecure since the intractable problem has become a tractable problem. For example, the well-known RSA algorithm is computational security since its factorization of the larger number is regarded as a NP problem. However, when the quantum computer becomes practical, the shor's quantum factorization algorithm leads this NP problem to become a QP problem as described in previous. Thus, in computationally secure cryptosystems a successful attacker in the system can also break another system that is known, i.e., proved in its own right, to be secure, or solve a mathematical problem. Proofs in computationally secure framework are asymptotic and, though sufficient for feasibility results, have to be further refined into an exact or concrete security approach. This refinement allows the key sizes to be quantified in terms of adversary's power. One should note that the quantum computationally secure cryptosystem depends on the quantum complexity theory.

An interesting case in the computational security is the provable security. In cryptosystems with provable security it is shown that a successful attack is not possible. This is a hot topic in current investigations in the classic cryptology.

2.6.3 Attack Strategy Analysis

Essentially, all attack strategies proposed in the classic cryptology as well as quantum cryptology can be categorized mainly as three categories, i.e., the principle-based attack strategy, implementation-based attack strategy and assistant-system-based attack strategy. In the principle-based attack strategy, the attacker tries to break the cryptosystem with the possible drawbacks caused by imperfectness of the employed fundamental, e.g., mathematical problems or physical laws. The algorithm-based attack strategy uses the possible drawbacks of the algorithm. While the assistant-system-based attack strategy depends on an assistant-system such as the Trojan horse, bug, etc. Of course, since the exact definition of security depends on the cryptosystem in question, the attack strategy in the security theory is complex. Some typical attack strategies for quantum key distribution will be introduced in Chapter 4.

The principle-based attack strategy makes use of drawbacks associated with the fundamentals to break the cipher and obtain useful information. For examples, the classic cryptosystem is based on the assumption of intractable problems being hard, which have not been proven strictly. In this scenario, drawbacks associated with the fundamentals are usually contained. With the development of mathematics these drawbacks become possibly a means of breaking the cryptosystem [18]. In the quantum cryptology, there exists also such kind of attack strategies [**?**]. For example, since the qubit can be entan-

gled using unitary operations, there are coherent attack strategies including collective attack and joint attack. In addition, since any quantum measurement outputs some available information, there is also incoherent attack, i.e., the individual attack. Clearly, the incoherent and coherent attacks are associated with the quantum laws. Accordingly, any attack operations under these strategies are associated with the physical fundamentals. Consequently, such kind of attack strategies is called the principle-based attack strategy. Fortunately, the presented investigations have illustrated that all these attacks cannot be succeeded in against quantum cryptography schemes, especially the quantum key distribution schemes. The details on the coherent and incoherent attacks, including individual attack, collective attack and joint attack, will be introduced in Chapter 4.

In private communication, any cryptographic system should be implemented using hardware or software ways. In the hardware way, the employed apparatus and devices are always imperfect. This may lead drawback of the system. For example, the single photon quantum cryptography needs generation of strict single photon for each laser pulse. However, to reach this idea hardware condition is very difficult in practice unless one employs other mechanisms to generate a single photon pulse. Subsequently, the photon-number splitting (PNS) attack is activated and has become an important attack strategy for the quantum cryptography [20 – 22]. Similarly, the drawbacks of devices have also been suffered in the classic private communication. For example, the weak electromagnetism leaking of IC card for cryptography aim will influence the security of system. In software way a suitable algorithm is always adopted. Then the algorithm-based attack strategy may break the system using obtained signal or leaked information. The well known ciphertext-only attack, known ciphertext attack, known-plaintext, and chosen plaintext attack belongs to this scenario.

The assistant-system-based attack strategy relies on an assistant system to break the cryptosystem. One of typical approaches in this scenario is the Trojan horse attack strategy (THAS) [**?**]. Let us firstly consider what is Trojan horse in information protection. In data security the Trojan horse is defined as a small program inserted by an attacker in a computer system. It performs functions not described in the program specifications, taking advantage of rights belonging to the calling environment to copy, misuse or destroy data not relevant to its stated purpose. For example, a Trojan horse in a text editor might copy confidential information in a file being edited to a file accessible to another. More generally, the so-called Trojan horse is a "robot horse" which can become a part of the legitimate users' systems. Then the "robot horse" can be surreptitiously exploited the legitimate authorizations of operation, e.g., measurement, detection, etc., to the detriment of security. For example, break the system via feeding back information to the attacker, e.g., the dishonest manufacturer or even the adversary, or directly destroying the legitimate data. To the legitimate users' system the Trojan horse is actually an additional system with passive effects. Many things, such as devices

and small programs inserted in the users' system, probing signals entering users' system through a public channel etc., or even the attacker, can become Trojan horse. However, it is impossible for any Trojan horse to play a same role as legitimate users since the Trojan horse is only a small part of the legitimate system.

There are mainly two kinds of Trojan horses, i.e., pre-lurked Trojan horse and online Trojan horse. The pre-lurked Trojan horse is a "robot horse" which is pre-inserted in legitimate users' systems, such as programs, apparatuses, or even offices. At an appropriate condition, the lurked Trojan horse is activated automatically by the legitimate system, and then it feeds back available information to the attacker even destroy the users' systems. The online Trojan horse is actually a probing signal which may enter the confidential system without awareness of legitimate communicators and then back-reflect to the attacker. Both kinds of Trojan horses may be classic as well as quantum. In addition, the Trojan horse may also be a combination of the "quantum Trojan horse" and "classic Trojan horse".

If a Trojan horse can be inserted successfully in users' system, the attacker can break the employed cryptosystem and obtain available information by means of the feedback information of the "robot horse". There are two kinds of THASs, i.e., the strategy relied on a pre-lurked Trojan horse and the strategy depended on the probing signal. While the attacking ways may be classic approaches or quantum approaches determined by the features of the employed Trojan horses. For example, if employing a pointer state of the legitimate system as a Trojan horse, or a pre-inserted tiny device as a Trojan hose, which is exploited to detect the quantum state of the qubits as the key, the attacker can obtain useful messages by analyzing the feedback information of the Trojan horse. If sending light pulses (probing signal) into the fiber entering legitimate users's apparatuses, then the attacker can analyze the backreflected light [**?**]. Of course, without the Trojan horse this strategy can do nothing since the feedback information of the Trojan horse is very important in this attacking strategy. Obviously, this strategy is different from the strategies which always involved in the quantum cryptography, e.g., the intercept/resend attack and the entanglement attack, where the attacker can directly obtain the information for attacking.

References

[1] Hoffman K M, Kunze R (1971) Linear Algebra, 2nd edn. Prentice Hall, New Jersey

[2] Jafarkhani H (2005) Space-Time Coding: Theory and Practice. Cambridge University Press, London

[3] Nielsen M A, Chuang I L (2002) Quantum computation and quantum information. Cambridge University Press, London

[4] Einstein A (1905) On a Heuristic Viewpoint Concerning the Production and

Transformation of Light. Annals of Physik, 17: 132 – 148

[5] Lupacu A, Saito S, Picot T, et al (2007) Quantum non-demolition measurement of a superconducting two-level system. Nature Physics, 3: 119 – 125

[6] Walls D F, Milburn G J (1997) Quantum Optics. Springer, New York

[7] He G Q, Zhu J, Zeng G H (2006) Quantum secure communication using continuous variable EPR correlations. Physical Review A, 73: 1 – 7

[8] Holevo A S (1973) Statistical problems in quantum physics. Proceedings of the second Japan-USSR Symposium on probability theory, Kyoto, 2 – 9 1972. In: Maruyama G, Prokhorov J V (eds) Lecture Notes in Math. Springer, Berlin, 330: 104 – 119

[9] Wegener I (2005) Complexity Theory. Springer, Heideburg

[10] Deutsch D (1985) Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer. Proceedings of the Royal Society A, 400: 97 – 117

[11] Bernstein E, Vazirani U (1993) Quantum Complexity Theory. Proceedings of 25th ACM Symposium on Theory of Computation, San Diego, 2 – 11 May 1993, pp 11 – 20

[12] Iriyama S, Ohya M (2007) On generalized quantum Turing machine and its language classes. Proceedings of the 11th WSEAS International Conference on Applied Mathematics, Dallas, 22 – 24 March 2007, pp 22 – 24

[13] Bennett C H (1973) Logical reversibility of computation. IBM Journal of Research and Development, 17: 525 – 532

[14] Shor P W (1997) Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal of Computing, 26: 1484 – 1509

[15] Bennett C H, Bernstein E, Brassard G, et al (1997) Strengths and weaknesses of quantum computation. SIAM Journal on Computing, 26(5): 1510 – 1523

[16] Bernstein E, Vazirani U (1997) Quantum complexity theory. SIAM Journal on Computing, 26(5): 1411 – 1473

[17] Shannon C E (1948) A mathematical theory of Communication. Bell System Technical Journal, 27(4): 397 – 423

[18] Schneier B (1994) Applied Cryptography:protocols, algorithms, and source code in C. Wiley, New York

[19] Shor P W, Preskill J (2000) Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. Physical Review Letters, 85: 441 – 444

[20] Brassard G, Lütkenhaus N, Mor T, et al (2000) Limitations on practical quantum cryptography. Physical Review Letters, 85: 1330 – 1333

[21] Lütkenhaus N (2000) Security against individual attacks for realistic quantum key distribution. Physical Review A, 61: 1 – 10

[22] Wang X B (2005) Beating the PNS attack in practical quantum cryptography. Physical Review Letters, 94: 1 – 4

[23] Zeng G H (2004) Security of quantum cryptographic algorithm against Trojan horse attacking. Journal of Software, 15: 1259 – 1264

[24] Gisin N, Ribordy G, Tittel W, et al (2002) Quantum cryptography. Reviews of Modern Physics, 4: 145 – 195

3 Quantum Bits

Bit is a basic notion in the information science and has been widely used in the computation, communication, and information processing. By analogy with the definition of the classic bit, this chapter defines definitely the so-called quantum bit which plays an important role in the quantum information processing. Then, physical properties, mathematical properties, and information properties of the quantum bit are described in detail. In addition, the transformation of qubits is discussed using typical quantum logic gates.

It is well-known that the quantum state is a basic notion in quantum mechanics. Once a quantum state of the involved quantum system is given, any quantum properties of this quantum system can be obtained theoretically. Since the quantum information processing is a combination of quantum mechanics and the classic information processing, the quantum state is also an important notion in the quantum information science. Usually, a new notion called the quantum bit (briefly qubit or qbit) is always exploited in this field. Physically, the qubit is the same as the quantum state. By analogy with the definition of the classic bit, the qubit is defined definitely in this chapter. There is slight deviation between definitions in this book and the traditional definitions. In the traditional definition, the qubit is used to described only quantum states in 2-dimension Hilbert space. Other quantum states are often named the tribit, multibit, or ebit, etc. dependently on its physical attributes. In this book, however, the qubit is referred to an arbitrary quantum state in Hilbert space. To distinguish various kinds of quantum states, several special notions such as the Binary qubit, P-ary qubit, and composite qubit are defined. Making use of these notions, the physical attributes of qubit are desquamated, so that such definition is more suitable for the general descriptions from the viewpoint of information science.

The qubit is a basic notion in the quantum information processing. To understand clearly the qubit, the mathematical property, physical property and information property of the qubit are described, and the transformation of qubits is analyzed using quantum logic gates. Some of these properties, especially the physical property, are important foundations for the theoretical schemes designing, security analysis, and technical implementation of quantum cryptographic algorithms and protocols in quantum private communication systems.

3.1 Classic Bits

In a communication system, the information is always expressed using message which is carried by a suitable signal, such as an optical signal, electronic signal, or electromagnetic signal, etc. Basically, information itself has two characteristics, i.e., nondeterminism and uncertainty. The nondeterminism indicates that the information must be described using statistic theory instead of the deterministic theory—Laplace theory. While the uncertainty means the receiver does not pre-know content of the received information so that information should be described using probabilistic approaches. This naturally gives rise to the following problems: how uncertain for the transmitted information and how to describe the uncertainty of information. This motivated Shannon to establish the well-known Shannon information theory in 1948 [**?**]. In this theory, the notion "bit" was employed as a basic unit to measure quantitatively the uncertainty of information.

The bit is a basic notion in the classic information theory, i.e., Shannon information theory. Initially, the bit was employed as a unit for measuring quantitatively information. With the development of computation technology, especially in the logic computation, the symbols "0" and "1" are always used. Since each symbol can offer 1 bit information in the logic computation. Subsequently, the bit is also used to describe mathematically the possible state of an information system.

First, consider the case of bit as an information unit. According to the Shannon information theory, if the probabilistic distribution of a random variable $X(x)$ is $p(x)$, the information carried by this random variable is

$$I(x) = -\log_2 p(x) \quad \text{(bit)}. \tag{3.1.1}$$

For example, in the binary system, let probabilities of "0" and "1" be same, i.e., $p(0) = p(1) = 1/2$, then the carried information of each symbol is

$$I(0) = I(1) = -\log_2 \frac{1}{2} = 1 \quad \text{(bit)}. \tag{3.1.2}$$

This is why the symbol 0 or 1 is always called as the notion "bit". However, the information carried by the symbol "0" or "1" is not always 1 bit. For example, let $p(0) = 1/3, p(1) = 2/3$, then one has

$$\begin{cases} I(0) = -\log_2 \dfrac{1}{3} = 1.585 \quad \text{(bit)}, \\ \\ I(1) = -\log_2 \dfrac{2}{3} = 0.585 \quad \text{(bit)}. \end{cases} \tag{3.1.3}$$

Except the unit "bit" there are other units for the information, i.e., "nat" and "hart", which corresponds the logarithm with base EXP and 10, respec-

tively. The relations among "bit", "nat" and "hart" are as follows,

$$\begin{cases} 1 \text{ nat} = 1.44 \text{ bit}, \\ 1 \text{ hart} = 3.32 \text{ bit}. \end{cases} \tag{3.1.4}$$

When the bit is as a symbol for describing the state of the information system, the symbol "0" and "1" carry 1 bit information, respectively. For example, Fig.3.1 demonstrates a basic logic circuit which uses "0" and "1" as symbol to perform addition calculations. Note, in this scenario the bit is only a mathematical conception. In physical, the bit can be implemented in many ways, such as "high" and "low" of the signal voltage, "strong" and "weak" of the signal power, etc.

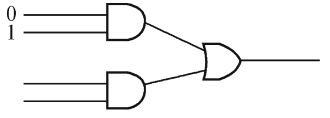

Fig. 3.1. Example of logic gate drawing

3.2 Quantum Bit Definition

By analogy with the classic bit in the Shannon information theory, a similar notion called "qubit" (or qbit) is employed in the quantum information theory. It is noted that the qubit is only employed to describe states of a quantum system, and it has not yet been used as an informational unit in the quantum information processing. Physically, a qubit is actually a quantum state which has been studied in the previous chapter. Consequently, a qubit holds all attributes of the quantum state. This leads that a qubit possesses of many novel characteristics than a classic bit. These characteristics plays important role in the quantum private communication.

Currently, definition of the qubit is not clear since various meanings of qubit are employed in the quantum information field. According to physical expressions of quantum states qubits are often called as various notions. For instance, quantum states in Hilbert spaces $\mathscr{H}_2$ and $\mathscr{H}_n (n \geq 3)$ are called the qubit and tribit (or multibit), respectively; while an entanglement state is often called ebit. Clearly, these definitions are incomplete and confused. For example, according to the above definitions, the following quantum states $|\phi_1\rangle = \sum_{i=1}^{3} \alpha_i |i\rangle$ and $|\phi_2\rangle = \sum_{i=1}^{4} \beta_i |i\rangle$ are all multibits, naturally one has to ask how to define them exactly? Clearly, the above definitions cannot solve this problem.

To present a clear description, the qubit is defined definitely in mathematical ways while its physic connotations are neglected. Throughout this

book the qubit is regarded as an abstractly mathematical conception, i.e., any quantum state is called a qubit. To define further the qubit in an exact way we adopt the following rule: Binary qubit, P-ary qubit, and composite qubit.

3.2.1 Binary Qubit

In the classic information theory, the bits "0" and "1" are defined as binary bits. Similarly, the binary qubit is defined as follows.

Definition 3.2.1 Let $|\psi\rangle$ be a quantum state in the 2-dimension Hilbert space $\mathscr{H}_2$. Then the quantum state $|\psi\rangle$ is called a binary qubit, briefly, B-qubit, or B-qbit.

Denote the basis $\{|0\rangle, |1\rangle\}$ of the 2-dimension Hilbert space, a general B-qubit is expressed as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{3.2.1}$$

with $|\alpha|^2 + |\beta|^2 = 1$.

Eq.(3.2.1) illustrates the B-qubit is a superposition state of $|0\rangle$ and $|1\rangle$, which means the B-qubit may be in the state $|0\rangle$ or $|1\rangle$ with probability of $|\alpha|^2$ or $|\beta|^2$, respectively. Also it may be in the state $|\psi\rangle$ with probability 1.

Generally, the basis in a space is not unique. For example, in the 2-dimension Hilbert space $\mathscr{H}_2$, $\{|+\rangle, |-\rangle\}$ is another basis which is always called computational basis. Since $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$, the B-qubit can be denoted in the basis $\{|+\rangle, |-\rangle\}$ as

$$|\psi\rangle = \alpha'|+\rangle + \beta'|-\rangle = \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle, \tag{3.2.2}$$

with $|\alpha'|^2 + |\beta'|^2 = 1$.

Physically, a B-qubit composes of one particle (quanta), it can be implemented in various ways, such as polarizations, phases, two-level atom, etc. For the physical implementation of a basic qubit, please refer to Chapters 7 and 8.

3.2.2 P-ary Qubit

In the classic case, except for the binary number, i.e., $\{0, 1\}$, there introduces various number systems such as the Decimal system, Hexadecimal system, etc. Generally, they are called P-ary number. Refer to these classic definitions, the so-called P-qubit which expresses the quantum state in the P-ary numeral system is defined as follows.

Definition 3.2.2 Let $|\psi^p\rangle$ be a single quantum state in the p-dimension Hilbert space $\mathscr{H}_p$. Then the quantum state $|\psi^p\rangle$ is called a P-ary qubit,

briefly, P-qubit, or P-qbit.

Generally, a P-qubit is denoted

$$|\psi^p\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \ldots + \alpha_p|p-1\rangle, \tag{3.2.3}$$

with $\sum_{i=0}^{p-1} |\alpha_i|^2 = 1$. For example, a 3-qubit is denoted as

$$|\psi^3\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle. \tag{3.2.4}$$

This state has been employed in the quantum secret sharing scheme. The quantum secret sharing scheme is an important component in the quantum cryptology. Since this book refers to the quantum private communication which focuses on the topics of how to protect the confidentiality and authentication of communication, this issue is not addressed in the book. However, a multi-party quantum key distribution scheme based on the quantum secret sharing is presented in Section7.7. The interesting readers on the quantum secret sharing may have further readings referred to Ref.[2,3].

3.2.3 Composite Qubit

If the considered quantum system is a multi-particle system, the corresponding quantum state is a multi-particle state. In this case, a so-called composite qubit is defined to describe such a situation.

Definition 3.2.3 The quantum state of an n-particle quantum system is defined as a composite qubit, briefly, C_n^p-qubit, or C_n^p-qbit, where the subscript n and superscript p denote the number of particles and P-ary, respectively.

Like the composite state of quantum systems, there are different composite ways. Firstly, consider the composite qubit in $\mathscr{H}_2$. If an involved n quantum system is independent, the composite qubit is a direct product of these n basis qubits. Denote n basis qubits by $|\psi_i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle$ $(i = 1, 2, \ldots, n)$, then the composite qubit is denoted as

$$|\Psi_n^2\rangle = \bigotimes_{i=1}^{n} |\psi_i\rangle. \tag{3.2.5}$$

This is actually a superposition state of binary codes. If an associated n quantum system is entangled, the composite qubit is an entanglement state of the n quantum system. For example, a two-particle composite qubit in $\mathscr{H}_2$ is denoted as

$$|\Psi_2^2\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|01\rangle + \alpha_{11}|11\rangle, \tag{3.2.6}$$

with $\sum_{i_1,i_2=0}^{1} |\alpha_{i_1 i_2}|^2 = 1$. Obviously, Bell states and Greenberger-Horne-Zeilinger(GHZ) states are C_2^2-qubit and C_3^2-qubit, respectively.

Generally, in the 2-dimension Hilbert space a composite qubit can be denoted as

$$|\Psi\rangle = \sum_{i_1,i_2,\ldots,i_n=0}^{1} \alpha_{i_1,i_2,\ldots,i_n}|i_1,i_2,\ldots,i_k\rangle. \tag{3.2.7}$$

Compare to the classic case, the composite qubit likes a codeword, e.g., the codeword $c = i_1 i_2 \ldots i_k$. However, a composite qubit is a superposition state of 2^{i_k} classic codewords! This feature brings some novel properties for the quantum bits. In the quantum information processing the quantum error-correction code is a typical composite qubit.

In a p-dimension Hilbert space $\mathscr{H}_p$, the binary base should be changed to the P-ary numeral system. Generally, a composite qubit consisting of n quantum systems in the p-dimension Hilbert space $\mathscr{H}_q$ may be denoted as

$$|\psi_n^p\rangle = \sum_{i_1,i_2,\ldots,i_n=0}^{p-1} \alpha_{i_1,i_2,\ldots,i_n}|i_1,i_2,\ldots,i_k\rangle. \tag{3.2.8}$$

Example 1 A composite qubit consists of two quantum systems in the 3-dimension Hilbert space $\mathscr{H}_3$ is

$$|\psi_2^3\rangle = \sum_{i_1,i_2=0}^{2} \alpha_{i_1,i_2}|i_1,i_2\rangle. \tag{3.2.9}$$

Example 2 The Aharonov state may be regarded as a C_3^3-qubit,

$$|\Psi_3^3\rangle = \frac{1}{\sqrt{6}}\left(|012\rangle + |120\rangle + |201\rangle - |012\rangle - |102\rangle - |210\rangle\right). \tag{3.2.10}$$

3.3 Quantum Bit Transformation

In the quantum information processing, such as the quantum private communication, quantum computation, and quantum data compression, the quantum transform is always employed, e.g., changing form of a qubit or transforming two B-qubits into a C-qubit, etc. To perform such a kind of transformations needs unitary operations. Generally, a quantum transforms may be defined as follows.

Definition 3.3.1 Let $|X\rangle$ and $|Y\rangle$ be arbitrary qubit with $|X\rangle$ inputs and $|Y\rangle$ output, then an arbitrary quantum transform is defined as

$$|Y\rangle = F|X\rangle, \tag{3.3.1}$$

where F is an arbitrary matrix form for a quantum transform, its size depends on the dimensions of the qubits $|X\rangle$ and $|Y\rangle$.

Let U_N denote a unitary matrix of quantum transforms, where N denotes the size of the unitary matrix. Generally, the matrix representation of the quantum transform may be any size. However, only $N = 2^n$ size unitary matrices are considered in current quantum information processing, since the B-qubits are employed in many situations.

3.3.1 Quantum Logic Gates

The quantum transform must be a unitary matrix since a qubit should satisfy the normalization condition. In quantum mechanics, a quantum transform corresponds a quantum operator. While in the quantum information such a operator is called the quantum logic gate, briefly called the quantum gate. There are several kinds of quantum gates: single-qubit gate, two-qubit gate, multi-qubit gate. Based on these basic quantum gates, a quantum circuit may be constructed. The quantum circuit is different from the electron circuit since a qubit is different from the classic bits.

1) Classic Bit Gates

In the classic information processing, the basic unit for information processing is the so-called logic gate. A logic gate performs a logical operation on one or more logic inputs and produces a single logic output. The logic operation normally performed is the Boolean logic and is most commonly found in digital circuits. Logic gates are primarily implemented electronically using diodes or transistors, but can also be constructed using electromagnetic relays, fluidics, optical, or even mechanical elements. A Boolean logical input or output always takes one of two logic levels. These logic levels can go by many names including: on/off, high(H)/low(L), one(1)/zero(0), true(T)/false(F), positive/negative, positive/ground, open circuit/close circuit, potential difference/no difference, etc. For consistency, the names 1 and 0 will be used below.

A logic gate takes one or more logic-level inputs and produces a single logic-level output. Because the output is also a logic level, an output of one logic gate can connect to the input of one or more other logic gates. Two outputs cannot be connected together, however, as they may be attempting to produce different logic values. In electronic logic gates, this would cause a short circuit.

NAND and NOR logic gates are two pillars of logic, in that all other types of Boolean logic gates (i.e., AND, OR, NOT, XOR, XNOR) can be created from a suitable network of just NAND or just NOR gate(s). They can be built from relays or transistors, or any other technology that can create an inverter and a two-input AND or OR gate. These functions are demonstrated in Table 3.1. OR, AND, NAND, and NOR gates may have more than two inputs. All gates have exactly one output.

Table 3.1. Logic gates and their functions

OR	Any high input will drive output high
NOR	Any high input will drive output low
AND	Any low input will drive output low
NAND	Any low input will drive output high
XOR	Only 1 high input will drive output high
XNOR	Only 1 high input will drive output low

Six typical symbols of logic-gates are demonstrated in Fig.3.2. All these are basic logic gates and play important roles in the classics information processing.

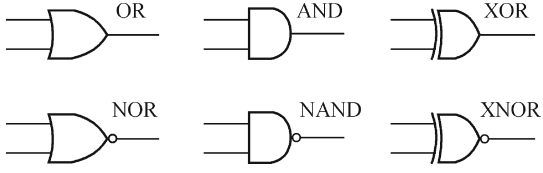

Fig. 3.2. Symbols of classic logic gates

2) Single-qubit Logic Gate

In the classic scenario, there are only two basic bits in the binary system. Correspondingly, there are only one single bit logic gate. In the quantum case, however, a qubit is a superposition state, this gives rise to many single qubit gates. In addition, transformation of qubit should be a unitary operation since the normalization requirement of qubit, i.e., quantum state. Thus any quantum gate is a unitary operation. Let U denote a quantum logic gate, it satisfies

$$U^{\dagger}U = UU^{\dagger} = I. \tag{3.3.2}$$

In addition, a quantum logic gate must be independent of physical properties of the input qubits. Thus a quantum logic gate should be a universal gate. The unitary and universal properties are basic requirements for a quantum logic gate.

There are some important gates: X gate, Y gate, Z gate, Hadamard gate, phase gate and $\pi/8$ gate. These gates are drawn in Fig.3.3. They may compose of various universal gate sets. In the following brief descriptions for these gates are presented.

The X gate is also called the Pauli-X gate, it is the Pauli x component, i.e., $X = \sigma_x = \sigma_1$. The matrix representation reads

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{3.3.3}$$

The symbol of the X gate is shown in Fig.3.3(a). The function of the X gate is to flip the qubit. Let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ be an arbitrary B-qubit, then the

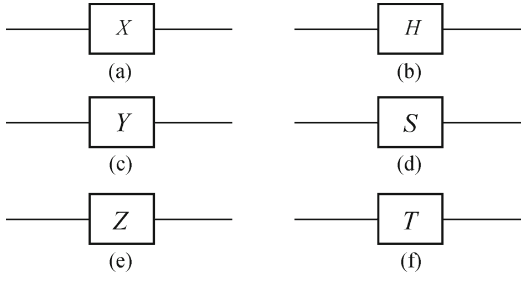

Fig. 3.3. Basic single qubit quantum logic gates

X gate on the qubit yields the following output,

$$X|\psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix} = \beta|0\rangle + \alpha|1\rangle. \tag{3.3.4}$$

The Y gate is also called the Pauli-Y gate, it is the Pauli y component, i.e., $Y = \sigma_y = \sigma_2$. The matrix representation is as follows,

$$Y = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}, \tag{3.3.5}$$

where i is the imaginary unit. The symbol of the Y gate is shown in Fig.3.3(b). The function of the Y gate is to flip the qubit, i.e., the Y gate on the qubit yields the following output,

$$Y|\psi\rangle = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \mathrm{e}^{\frac{\mathrm{i}\pi}{2}}(-\beta|0\rangle + \alpha|1\rangle). \tag{3.3.6}$$

The Z gate is the Pauli z component, i.e., $Z = \sigma_z = \sigma_3$. It is also called the Pauli-Z gate. Its matrix representation is given by

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{3.3.7}$$

The symbol of the Z gate is shown in Fig.3.3(c). The function of the Z gate is to rotate $\pi/2$ along the $|1\rangle$ axis. Mathematically, the Z gate on the qubit may be expressed as follows,

$$Z|\psi\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ -\beta \end{pmatrix} = \alpha|0\rangle - \beta|1\rangle. \tag{3.3.8}$$

The H gate is actually the Hadamard gate. The Hadamard gate and Pauli matrices have the following relations,

$$H = \sigma_1 + \sigma_3, \tag{3.3.9}$$

and have the following matrix representation,

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{3.3.10}$$

Note, comparing to its classic form the coefficient $1/\sqrt{2}$ of H is often omitted in quantum scenarios. The symbol of the H gate is shown in Fig.3.3(d). The function of the H gate may be mathematically expressed as follows,

$$H|0\rangle \to |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad H|1\rangle \to |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{3.3.11}$$

Thus, one has

$$H|\psi\rangle \to \alpha|+\rangle + \beta|-\rangle = \frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle. \tag{3.3.12}$$

Easily, one may check the following relations,

$$H^2|\psi\rangle = |\psi\rangle. \tag{3.3.13}$$

The S gate is also called the phase gate. The matrix representation of the phase gate is expressed as follows,

$$S = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{i} \end{pmatrix}. \tag{3.3.14}$$

The symbol of the S gate is shown in Fig.3.3(e). A phase gate makes the qubit have $\pi/2$ phase changes, which may be expressed as

$$S|\psi\rangle = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{i} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha|0\rangle + \mathrm{i}\beta|1\rangle. \tag{3.3.15}$$

The T gate is also called the $\pi/8$ gate. The matrix representation of the phase gate is expressed as follows,

$$T = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\frac{\pi}{4}} \end{pmatrix}. \tag{3.3.16}$$

The symbol of the T gate is shown in Fig.3.3(f). The T gate makes the qubit has $\pi/4$ phase changes, which is expressed as

$$T|\psi\rangle = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\frac{\pi}{4}} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha|0\rangle + \mathrm{e}^{\mathrm{i}\frac{\pi}{4}}\beta|1\rangle. \tag{3.3.17}$$

An arbitrary single-qubit quantum gate in the 2-dimension Hilbert space $\mathscr{H}_2$ is a 2 by 2 unitary matrix. There is a fast decomposition approach for a 2 by 2 unitary matrix which has been shown in the following theorem.

Theorem 3.3.1 Any single qubit quantum logic gate can be decomposed into the following form,

$$U = \mathrm{e}^{\mathrm{i}\alpha} \begin{pmatrix} \mathrm{e}^{-\mathrm{i}\frac{\beta}{2}} & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\frac{\beta}{2}} \end{pmatrix} \begin{pmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{pmatrix} \begin{pmatrix} \mathrm{e}^{-\mathrm{i}\frac{\delta}{2}} & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\frac{\delta}{2}} \end{pmatrix}, \tag{3.3.18}$$

where $\alpha, \beta, \gamma, \delta$ are real numbers.

A detail proof for this decomposition has been presented in Ref. [**?**].

3) Measurement Gate

The quantum measurement is an important issue in quantum mechanics and quantum information processing. It is a kind of operations on qubit, but it is not a unitary operator since it collapses the qubit. For the sake of unification, the quantum measurement is defined as a new logic gate called the measurement gate, briefly called the M gate, in this book. Since there are three measurement ways, correspondingly, there are general measurement gate M_G, projective measurement gate M_P, and POVM gate M_{POVM}. The quantum measurement gate is denoted in the book using the symbol in Fig.3.4.

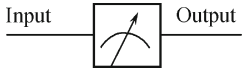

Fig. 3.4. Quantum measurement gate for qubits

As an example, consider the projective measurement gate M_P in the 2-dimension Hilbert space $\mathscr{H}_2$. Let $\{|e_1\rangle, |e_2\rangle\}$ be bases in $\mathscr{H}_2$, then any B-qubit $|\psi\rangle \in \mathscr{H}_2$ may be denoted,

$$|\psi\rangle = \alpha|e_1\rangle + \beta|e_2\rangle. \tag{3.3.19}$$

In this case, the matrix form of the projective measurement gate M_p has the following form,

$$M_P = \begin{pmatrix} \delta_{\hat{o},\,\hat{e}_1} & 0 \\ 0 & \delta_{\hat{o},\,\hat{e}_2} \end{pmatrix}, \tag{3.3.20}$$

where δ is a Delta function, and the symbols $\hat{o}$ and $\hat{e}_j$ $(j = 1, 2)$ denote directions of the quantum measurement and bases $|e_i\rangle$, respectively. For example, if the direction of the quantum measurement is along $|e_1\rangle$, i.e., $\hat{e}_1$, the measurement gate is

$$M_P^{\hat{e}_1} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \tag{3.3.21}$$

conversely the measurement gate is

$$M_P^{\hat{e}_2} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}. \tag{3.3.22}$$

Applying the quantum measurement gate M_p in Eq.(3.3.20) on qubit $|\psi\rangle$ yields

$$M_P|\psi\rangle \longrightarrow \alpha|e_1\rangle\delta_{\hat{o},\,\hat{e}_1} + \beta|e_2\rangle\delta_{\hat{o},\,\hat{e}_2}. \tag{3.3.23}$$

Clearly, this description is consistent with the definition of the quantum measurement in Section 2.3.3 for the general measurement, projective measurement, and POVM measurement.

4) Two-qubit Gate

A typical two-qubit quantum logic gate is the so-called controlled-NOT (briefly CNOT) gate, denoted C_{NOT}. This gate has two inputs, known as the control qubit and the target qubit, respectively. Its symbol is shown in Fig.3.5. The top line represents the control qubit, and the bottom line represents the target qubit. The action of this gate is described as follows. If the control qubit is 0, the target qubit is left alone; if the control qubit is 1, then the target qubit is flipped. In equations this procedure is expressed as

$$C_{NOT}|\epsilon_c\epsilon_t\rangle \rightarrow |\epsilon_c(\epsilon_c \oplus \epsilon_t)\rangle, \tag{3.3.24}$$

where $\epsilon_c, \epsilon_t \in \{0, 1\}$ and $\oplus$ denotes the addition modulo two.

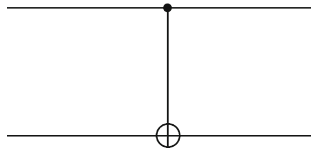

Fig. 3.5. Control-NOT gate for two qubits

To obtain the matrix form of the control-NOT gate needs a suitable basis set. Since the two-qubit system is a composite quantum system, the basis may be constructed using two single-quantum systems. Thus, the basis for the two-qubit system is $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Then the elements of the gate C_{NOT} is

$$[C_{NOT}]_{i,j} = \langle i, j|C_{NOT}|i, j\rangle, \tag{3.3.25}$$

where $i, j = 0, 1$. Employing above equation, the matrix representation of the control-NOT gate is obtained,

$$C_{NOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{3.3.26}$$

Generally, suppose that U is an arbitrary single qubit unitary operation. A controlled-U operation is a two qubit operation, again with a control and a target qubit. If the control qubit is set then U is applied to the target qubit, otherwise the target qubit is left alone; that is

$$|c\rangle|t\rangle \rightarrow |c\rangle U^c|t\rangle. \tag{3.3.27}$$

The controlled-U operation is represented by the circuit shown in Fig.3.6. In this figure, the top line is the control qubit, and the bottom line is the target qubit. If the control qubit is set the U is applied to the target qubit, otherwise it is left. The matrix representation of this operation is

$$C_U = \begin{pmatrix} I_2 & 0 \\ 0 & U \end{pmatrix}. \tag{3.3.28}$$

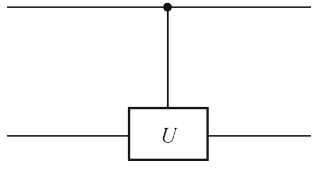

Fig. 3.6. Controlled-U gate for two qubits

Example 1 Let $U = Y$, one obtains the controlled-Y gate,

$$C_Z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -\mathrm{i} \\ 0 & 0 & \mathrm{i} & 0 \end{pmatrix} = \begin{pmatrix} I_2 & 0 \\ 0 & Y \end{pmatrix}. \tag{3.3.29}$$

The symbol is shown in Fig.3.7.

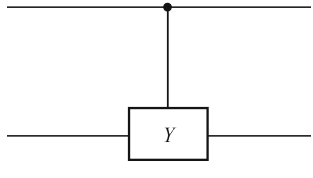

Fig. 3.7. Controlled-Y gate for two qubits

Example 2 Let $U = R$, where R is a rotation operation with the following form,

$$R = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\alpha} \end{pmatrix}, \tag{3.3.30}$$

then the matrix representation of C_R is

$$C_R = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \mathrm{e}^{\mathrm{i}\alpha} \end{pmatrix} = \begin{pmatrix} I_2 & 0 \\ 0 & R \end{pmatrix}. \tag{3.3.31}$$

The symbol is shown in Fig.3.8.

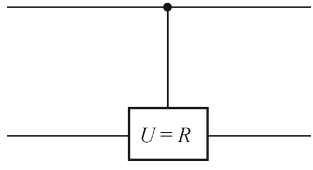

Fig. 3.8. Controlled-R gate for two qubits

5) Universal Quantum Gate

Definition 3.3.2 Let $\mathscr{G} = \{G_1, G_2, \ldots, G_n\}$ be a set of gates, if this set can be employed to compute an arbitrary function $f(x)$, the gate set $\mathscr{G}$ is called the universal gate set, and G_i with $i = 1, 2, \ldots, n$ are called universal gates.

In classic case, the gate set $\mathscr{G}_c = \{AND, OR, NOR\}$ is a universal gate set and these gates, AND, OR, NOR, are universal classic gates.

In quantum case, the universal gate set in the Hilbert space $\mathscr{H}_2^n$ is $\mathscr{G}_q = \{X, Y, Z, S, T, C_{NOT}\}$. Since any $N = 2^n$ size unitary matrix U_N can be decomposed into these matrices.

Theorem 3.3.2 Any $N = 2^n$ size unitary matrix U_N can be represented in the universal gate set $\mathscr{G}_q$.

Proof Generally, any $N = 2^n$ unitary matrix U_N can be represented in a 2 by 2 block unitary matrix $\mathcal{U}_2$,

$$U_{2^n} = \mathcal{U}_2 = \begin{pmatrix} A & B \\ C & D \end{pmatrix}, \tag{3.3.32}$$

where the block-elements A, B, C and D are 2^{n-1} size unitary matrices. In the physical case, U_{2^n} is factorable in multiplication group when $n \geq 2$. Thus, four block-elements must be kronecker products of two matrices, i.e.,

$$\begin{cases} A = \mathcal{U}_i^A \otimes U_j^1, & B = \mathcal{U}_i^B \otimes U_j^1, \\ C = \mathcal{U}_i^C \otimes U_j^1, & D = \mathcal{U}_i^D \otimes U_j^1, \end{cases} \tag{3.3.33}$$

where $i \cdot j = 2^{n-1}$. Therefore,

$$U_{2^n} = \mathcal{U}_2 = \begin{pmatrix} \mathcal{U}_i^A & \mathcal{U}_i^B \\ \mathcal{U}_i^C & \mathcal{U}_i^D \end{pmatrix} \otimes \mathcal{U}_j^1. \tag{3.3.34}$$

In such case, one has the following recursive relations [5],

$$\begin{aligned} U_{2^n} &= \prod_{i=0}^{n-1} I_{4^{n-i-1}} \otimes U_4 \otimes I_{4^i}, \\ &= \prod_{i=1}^{n} I_{4^{n-i}} \otimes U_4 \otimes I_{4^{i-1}}. \end{aligned} \tag{3.3.35}$$

If U_4 can be decomposed further, it may be written as

$$U_4 = U_2 \otimes U_2. \tag{3.3.36}$$

In addition, it has been proven that any 2 by 2 unitary matrix can be expressed in σ_x, σ_z. However, in some a case, it cannot be decomposed. For example, when $U_4 = C_{NOT}$, it cannot be represented in kronecker product. Fortunately, this kind of unitary matrix is actual a two-qubit gate. Thus the set of $\{Y, Z, C_{NOT}\}$ is a universal gate.

Corollary 1 Any single qubit gate can be decomposed as

$$U = \mathrm{e}^{\mathrm{i}\theta_0} \mathrm{e}^{-\mathrm{i}\theta_1 \frac{\sigma_z}{2}} \mathrm{e}^{-\mathrm{i}\theta_2 \frac{\sigma_y}{2}} e^{-\mathrm{i}\theta_3 \frac{\sigma_z}{2}}. \tag{3.3.37}$$

Corollary 2 Any two-qubit gate U_{AB} can be decomposed as

$$U_{AB} = \mathrm{e}^{\mathrm{i}\theta_0 I_2 \otimes I_2} (U_A \otimes U_B) U_D (V_A \otimes V_B), \tag{3.3.38}$$

where U_A, U_B, V_A, V_B are single-qubit quantum gates and U_D is a non-factorable gate responsible for the non-local characteristic of the gate, and has the following form

$$U_D = \mathrm{e}^{-\mathrm{i} \sum_{i=1}^{3} \theta_i \sigma_i \otimes \sigma_i}. \tag{3.3.39}$$

Corollary 3 Any three-qubit gate U_{ABC} can be decomposed as

$$U_{ABC} = (A_4 \otimes B_4) N_2 (A_3 \otimes B_3) M (A_2 \otimes B_2) N_1 (A_1 \otimes B_1), \tag{3.3.40}$$

where A_i, B_i are, respectively, two qubits gates and single qubit gate, N_k and M has the following form,

$$N_k = \mathrm{e}^{\mathrm{i}(a_k \sigma_x \otimes \sigma_x \otimes \sigma_z + b_k \sigma_y \otimes \sigma_y \otimes \sigma_z + c_k \sigma_z^{\otimes 3})}, \tag{3.3.41}$$

$$M = \mathrm{e}^{\mathrm{i}(a\sigma_x^{\otimes 3} + b\sigma_y \otimes \sigma_y \otimes \sigma_z + c\sigma_z \otimes \sigma_z \otimes \sigma_x + dI_2 \otimes I_2 \otimes \sigma_x)}, \tag{3.3.42}$$

where the parameters a, b, c, and d are real numbers.

3.3.2 Quantum Circuits

A quantum circuit is a flow graph which consists of "quantum wire" and "quantum logic gate", the flow direct is from left to right. The so-called wire is a logic gate which describes the flow of qubits. Compare to the electron circuit, a quantum circuit has no multiple input and multiple-out. This is because the quantum operation must be a unitary, subsequently, the wires cannot be joined together. In addition the inverse operation is not allowed since the quantum no-cloning theorem.

Example 1 Fig.3.9 is a quantum circuit which consists of two Hadamard gates H and one controlled-NOT gate C_{NOT}.

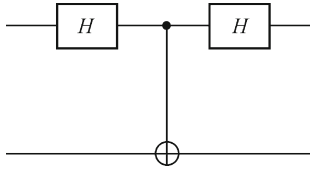

Fig. 3.9. A quantum circuit consisted of Hadamard gates and Controlled-NOT gate

Example 2 Fig.3.10 is a quantum circuit which consists of three controlled-NOT gates C_{NOT}.

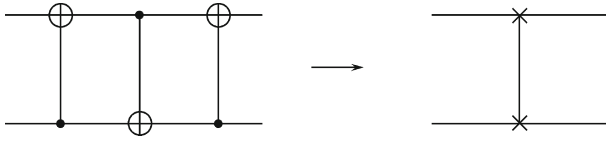

Fig. 3.10. A quantum circuit consisted of three Controlled-NOT gate

Example 3 Fig.3.11 is a quantum circuit for teleporting a qubit.

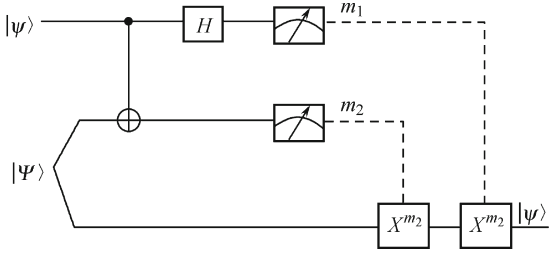

Fig. 3.11. A quantum circuit for teleporting a qubit

In the Fig.3.11, let $|\psi\rangle$ be a B-qubit in the 2 dimensional Hilbert space $\mathscr{H}_2$ which will be teleported, while the two-particle state $|\Psi\rangle$ be a EPR pair.

The corresponding particles are denoted $1, 2$, and 3. These states have the following forms,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{3.3.43}$$

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{3.3.44}$$

In this case, the total input state is

$$|\psi_0\rangle = |\psi\rangle \otimes |\Psi\rangle = \frac{1}{\sqrt{2}}\left[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)\right]. \tag{3.3.45}$$

Applying the controlled-NOT operation on particles 1 and 2 gives

$$|\psi_1\rangle = C_{NOT}|\psi_0\rangle. \tag{3.3.46}$$

Then the particle 1 is operated by a Hadamard gate,

$$|\psi_2\rangle = H|\psi_1\rangle = HC_{NOT}|\psi_0\rangle. \tag{3.3.47}$$

After these operations, the particles 1 and 2 are measured. These operations give

$$|\psi_3\rangle = M_1M_2|\psi_2\rangle. \tag{3.3.48}$$

Finally, the particle 3 is operated by two single qubit gates X and Z which are controlled under the measurement results m_1 and m_2. This operation gives

$$|\psi_4\rangle = Z^{m_1}X^{m_2}|\psi_3\rangle = |\psi\rangle. \tag{3.3.49}$$

Theorem 3.3.3 Any unitary matrix corresponds to a quantum circuit, and vice versa.

Proof If the unitary matrix U_N cannot be factorable, it may be regarded as an n-qubit quantum logic gate, which is actually a simple quantum circuit. If U_N can be decomposed, it may be denoted as 2 by 2 unitary matrices and 4 by 4 matrices. Since a 2 by 2 unitary matrix is a single-qubit quantum gate and a 4 by 4 unitary matrix is a controlled-U gate. Thus the unitary matrix U corresponds to a quantum circuit. Reversely, it is straightforward.

According to the theorem, a quantum circuit can be denoted using an N by N unitary matrix. In addition, the quantum circuit can be plotted using a given unitary matrix U.

3.4 Mathematical Property

Mathematically, a quantum state, i.e., a qubit, is a vector in a special linear space called the Hilbert space. Therefore, a qubit must have important mathematical properties which are helpful for giving an intuitive picture for the qubit. In fact, a B-qubit corresponds to a point in the Bloch sphere, this section investigates the mathematical properties of the B-qubit in the Bloch Sphere.

3.4.1 Bloch Sphere

Since $|\alpha|^2 + |\beta|^2 = 1$, the B-qubit may be rewritten as

$$|\psi\rangle = \mathrm{e}^{\mathrm{i}\gamma}\left(\cos\frac{\theta}{2}|0\rangle + \mathrm{e}^{\mathrm{i}\varphi}\sin\frac{\theta}{2}|1\rangle\right), \tag{3.4.1}$$

where θ, φ, and γ are real numbers, and $0 \le \theta \le \pi$ and $0 \le \varphi \le 2\pi$. Since the factor $\mathrm{e}^{\mathrm{i}\gamma}$ has no observable effects, the above equation may be effectively written as

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \mathrm{e}^{\mathrm{i}\varphi}\sin\frac{\theta}{2}|1\rangle. \tag{3.4.2}$$

Mathematically, the parameters θ, φ define a point on a unit 3-dimension sphere as shown in Fig.3.12. This sphere is often called the Bloch sphere. It provides a useful means of visualizing the state of a B-qubit.

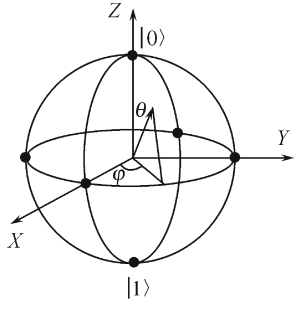

Fig. 3.12. Bloch sphere representation of a qubit

The Bloch sphere provides mathematically a visualized explanation for the B-qubit: The poles are base $|0\rangle$ and $|1\rangle$ of a B-qubit, and an arbitrary B-qubit is a point on the sphere. The φ is angle between X axis and the projection of the point in X-Y plane, and θ is an angle between the point and Z axis. If a point is determined, values of the parameters φ and θ can be obtained. According to the mathematical theory, any point on the sphere can be transformed into another point with a suitable transformation.

However, it must be kept in mind that this intuition is limited because there is no simple generalization of the Bloch sphere for P-qubit and C-qubit. Fortunately, these qubits may be expressed mathematically as

$$\rho = \frac{I + \mathbf{r}\cdot\sigma}{2}, \tag{3.4.3}$$

where I is an identity matrix, σ is a 3-dimension Pauli matrix, and the vector $\mathbf{r}$ is a parameter associated with the qubit.

Fig.3.12 demonstrates a clear mathematical construction for a B-qubit. In addition, there are infinite B-qubits in a 2-dimension Hilbert space.

3.4.2 Orthogonality of Opposite Points

Since an arbitrary point on the Bloch sphere denotes a qubit or called a quantum state, it is interesting to find out the dual qubit, i.e., the opposite point, on the Bloch sphere. In the following the orthogonality of an arbitrary point and its opposite point is presented. Consider a general B-qubit state $|\psi\rangle$,

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \mathrm{e}^{\mathrm{i}\varphi}\sin\frac{\theta}{2}|1\rangle. \tag{3.4.4}$$

Let $|\psi^d\rangle$ be a quantum state (i.e., qubit) of the corresponding opposite point, it reads

$$|\psi^d\rangle = \cos\frac{\pi-\theta}{2}|0\rangle + \mathrm{e}^{\mathrm{i}(\varphi+\pi)}\sin\frac{\pi-\theta}{2}|1\rangle \tag{3.4.5}$$

$$= \sin\frac{\theta}{2}|0\rangle - \mathrm{e}^{\mathrm{i}\varphi}\cos\frac{\theta}{2}|1\rangle. \tag{3.4.6}$$

Thus, the inner product $\langle\psi^d|\psi\rangle$ is given by

$$\langle\psi^d|\psi\rangle = \cos\frac{\theta}{2}\cos\frac{\pi-\theta}{2} - \sin\frac{\theta}{2}\sin\frac{\pi-\theta}{2} \tag{3.4.7}$$

$$= \cos\frac{\pi}{2} = 0, \tag{3.4.8}$$

which means two points are orthogonal.

3.4.3 Rotations on Bloch Sphere

The Pauli X, Y, and Z gates are so-called rotations because when they are exponentiated, they give rise to the rotation operators, which rotate the Bloch vector $(\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$ about the x, y, and z axes. Rotation operators are expressed by

$$R_x(\theta) \equiv \mathrm{e}^{-\mathrm{i}\theta X/2} = \cos\frac{\theta}{2}I - \mathrm{i}\sin\frac{\theta}{2}X, \tag{3.4.9}$$

$$R_y(\theta) \equiv \mathrm{e}^{-\mathrm{i}\theta Y/2} = \cos\frac{\theta}{2}I - \mathrm{i}\sin\frac{\theta}{2}Y, \tag{3.4.10}$$

$$R_z(\theta) \equiv \mathrm{e}^{-\mathrm{i}\theta Z/2} = \cos\frac{\theta}{2}I - \mathrm{i}\sin\frac{\theta}{2}Z, \tag{3.4.11}$$

where i is the imaginary unit. Consider $R_x(\pi) = -\mathrm{i}X$, which is equal to X up to the global phase of $-\mathrm{i}$, so one finds that the X operator is equivalent to a rotation of 180° about the X axis. Also, the rotation operators do not in general keep the coefficient of the $|0\rangle$ component of the qubit state real.

To compare rotated states to see if they correspond to the same point on the Bloch sphere, it is necessary to multiply each one by a phase to make the $|0\rangle$ component of its state real.

Since $R_z(\alpha)$ and $|\psi\rangle$ have the following matrix representations,

$$R_z(\alpha) = \begin{pmatrix} \mathrm{e}^{-\mathrm{i}\alpha/2} & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\alpha/2} \end{pmatrix}, \tag{3.4.12}$$

and

$$|\psi\rangle = \begin{pmatrix} \cos\dfrac{\theta}{2} \\ \mathrm{e}^{\mathrm{i}\varphi}\sin\dfrac{\theta}{2} \end{pmatrix}, \tag{3.4.13}$$

applying $R_z(\alpha)$ on the qubit $|\psi\rangle$ yields

$$\begin{aligned} R_z(\alpha)|\psi\rangle &= \begin{pmatrix} \mathrm{e}^{-\mathrm{i}\alpha/2} & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\alpha/2} \end{pmatrix} \begin{pmatrix} \cos\dfrac{\theta}{2} \\ \mathrm{e}^{\mathrm{i}\varphi}\sin\dfrac{\theta}{2} \end{pmatrix} \\ &= \begin{pmatrix} \mathrm{e}^{-\mathrm{i}\alpha/2}\cos\dfrac{\theta}{2} \\ \mathrm{e}^{\mathrm{i}\alpha/2}e^{i\varphi}\sin\dfrac{\theta}{2} \end{pmatrix} = \mathrm{e}^{-\mathrm{i}\alpha/2} \begin{pmatrix} \cos\dfrac{\theta}{2} \\ \mathrm{e}^{\mathrm{i}\alpha}\mathrm{e}^{\mathrm{i}\varphi}\sin\dfrac{\theta}{2} \end{pmatrix}. \end{aligned} \tag{3.4.14}$$

This result means that the net effect is to change φ to $\varphi + \alpha$ as one would expect for a rotation around the axis z.

If $\hat{n} = (n_x, n_y, n_z)$ is a real unit vector in the 3-dimension space, then it can be shown that the operator $R_{\hat{n}}(\theta)$ rotates the Bloch vector by an angle θ about the $\hat{n}$ axis, where

$$R_{\hat{n}}(\theta) = \mathrm{e}^{-\mathrm{i}\theta\hat{n}\cdot\sigma/2}, \tag{3.4.15}$$

and σ denotes three component vectors (X, Y, Z) of the Pauli matrices. Furthermore, it is not hard to show that $(\hat{n}\cdot\sigma)^2 = I$, and therefore one can use the special case operator exponential and write

$$\begin{aligned} R_{\hat{n}}(\theta) &= \cos\frac{\theta}{2}I - \mathrm{i}\sin\frac{\theta}{2}(\hat{n}\cdot\sigma) \\ &= \cos\frac{\theta}{2}I - \mathrm{i}\sin\frac{\theta}{2}(n_xX + n_yY + n_zZ). \end{aligned} \tag{3.4.16}$$

It can be shown that an arbitrary single qubit unitary operator can be written in the form,

$$U = \exp(\mathrm{i}\alpha)R_{\hat{n}}(\theta), \tag{3.4.17}$$

for some real numbers α and θ and a real 3-dimension unit vector $\hat{n}$. For example, consider $\alpha = \pi/2, \theta = \pi$, and $\hat{n} = (1/\sqrt{2}, 0, 1/\sqrt{2})$,

$$\begin{aligned} U &= \exp\frac{\mathrm{i}\pi}{2}\cos\frac{\pi}{2}I - \mathrm{i}\sin\frac{\pi}{2}\frac{1}{\sqrt{2}}(X+Z) \\ &= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \end{aligned} \tag{3.4.18}$$

which is the Hadamard gate H.

The double representation of rotations in the 3-dimension space has an interesting consequence that the rotation of 360° does not restore the phase to its initial values, and a rotation through 720° is needed. For example,

$$R_z(0) = I, \qquad R_z(2\pi) = -I, \qquad R_z(4\pi) = I. \tag{3.4.19}$$

For an isolated qubit this has no physical significance, but in relation to other qubits there is a difference, e.g., a rotation of 360° of an electron about its "spin" axis changes its state and a 720° rotation is needed to restore it. It affects the "orientation-entanglement relation" of objects in the 3-dimension real space.

3.5 Physical Property

As mentioned previously, a qubit is actually a quantum state in the Hilbert space. Consequently, a qubit holds all physical properties of the corresponding quantum state. It is impossible and not necessary to introduce all properties for a qubit since there are many physical attributes for a quantum state according to quantum mechanics. This section introduces some typical physical properties which are useful for the quantum private communication.

3.5.1 Superposition

Superposition is a basic characteristic of qubits following the quantum superposition principle. The superposition principle is the addition of the amplitudes of waves from interference. It occurs when an object simultaneously "possesses" two or more values for an observable quantity (e.g., the position or energy of a particle). For the state of quantum system in a p-dimension Hilbert space, it may be simultaneously stay in all of the basis states. Let the basis set of the Hilbert space $\mathscr{H}_p$ is $\{|0\rangle, |1\rangle, \ldots, |p-1\rangle\}$, according to the superposition principle the qubit may be denoted

$$|\psi^P\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \ldots + \alpha_{p-1}|p-1\rangle. \tag{3.5.1}$$

It is just a P-qubit. The B-qubit is a special case of the P-qubit, it can be denoted as

$$|\psi^2\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle. \tag{3.5.2}$$

For clarity, the superscript 2 is always omitted.

The superposition also exists in a C-qubit. For example, a two-particle entangled qubit (the entanglement of qubits will be defined in the following subsection) can be denoted as

$$|\psi_2^2\rangle = \alpha_{00}|00\rangle + \alpha_{11}|11\rangle. \tag{3.5.3}$$

The superposition property of qubits leads the measurement results are not determined. Let Q be operator of an observable quantity, and its eigenstate is a set of $\{|q_i\rangle|i = 1, 2, \ldots, n\}$, i.e.,

$$Q|q_i\rangle = \lambda_i|q_i\rangle. \tag{3.5.4}$$

Since the set of eigenstates may be viewed as a basis in the n-dimensional Hilbert space, any state $|\psi\rangle$ of the quantum system can be spanned by this basis, i.e.,

$$|\psi\rangle = \sum_i \alpha_i|q_i\rangle. \tag{3.5.5}$$

One may check easily,

$$Q|\psi\rangle = \sum_i \alpha_i Q|q_i\rangle \neq c|\psi\rangle. \tag{3.5.6}$$

Thus $|\psi\rangle$ is not an eigenstate of the operator Q. Now suppose that the state $|\psi\rangle$ is an eigenstate of the operator L, then the eigenequation is given by

$$L|\psi\rangle = \lambda|\psi\rangle, \tag{3.5.7}$$

where λ is the eigenvalue of the operator L. Simple calculations show that $QL \neq LQ$. Thus Q does not commute with L. Accordingly, the two observable variables corresponding to the operators Q and L cannot be determined simultaneously.

As an example, we consider a binary qubit state,

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right). \tag{3.5.8}$$

One may construct a measurement operator, e.g., projective operator P, which consists of the basis $\{|0\rangle, |1\rangle\}$. Measuring the state $|\psi\rangle$ using this projective operator yields the results $|0\rangle$ or $|1\rangle$ with probabilities $p(0) = 1/2$ and $p(1) = 1/2$, respectively. Evidently, the result is not determined before the measurement. While using the relations $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ the state $|\psi\rangle$ may be rewritten as

$$|\psi\rangle = |+\rangle. \tag{3.5.9}$$

Thus, using the measurement operator P' which consists of the basis $\{|+\rangle, |-\rangle\}$, the state $|\psi\rangle$ can be determined completely. These properties are demonstrated in Fig.3.13. Actually, this property has been employed in the BB84 protocol which will be described in the next chapter.

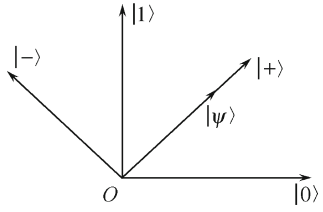

Fig. 3.13. Uncertainty of qubit for measurement

Above analysis show that the measurement of qubit depends on the chosen measuring ways. Different measurement ways lead different results. Therefore, a suitable measurement system is necessary to reach the aim in the experiment.

3.5.2 Entanglement

The entanglement is a very important physics property of qubit and plays key roles in the quantum information science and quantum mechanics. Originally, it was introduced by Einstein, Podolsky, and Rosen for formulating the EPR paradox [**?**]. Recent years, the entanglement has been investigated widely [**?**, **?**]. In the quantum cryptography and quantum private communication the entanglement of qubit is not necessary, however, it is still a very important quantum source for quantum cryptographic schemes designs and security analysis. Accordingly, this subsection introduces some basic knowledge on the entanglement of qubit.

A single-qubit has no entanglement property. To construct an entanglement system, a composite quantum system is required. Accordingly, only C-qubit might become an entangled system. Physically, a C-qubit with entanglement property is called the entanglement state. Following the definition in previous chapters, the notation C^e-qubit is employed to denote the entanglement state.

The entanglement of the continuous variable quantum system has been described briefly in Section 2.3.4. Here, the entanglement of discrete variable quantum system is introduced. In general, the N-particle entanglement states is written as

$$|\psi\rangle = \prod_{i=1}^{N} |\mu_i\rangle \pm \prod_{i=1}^{N} |\mu_i^c\rangle, \tag{3.5.10}$$

where μ_i stands for a binary variable $\mu_i \in \{|z+\rangle, |z-\rangle\}$ and $\mu_i^c = 1 - u_i$,

$|z+\rangle$ and $|z-\rangle$ denote the spin eigenstates, or equivalently the horizontal and vertical polarization eigenstates, or equivalently any two-level system. For $N = 2$ they may reduce to the Bell states, and the states with $N = 3$ and $N = 4$ represent the GHZ states, while the general N quantum states are always called the so-called "cat states".

As a special case, the state with $N = 2$ which may reduce to four Bell states is considered. These states have the following forms,

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}\left(|1_1 0_2\rangle + |0_1 1_2\rangle\right), \tag{3.5.11}$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|0_1 1_2\rangle - |1_1 0_2\rangle\right), \tag{3.5.12}$$

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|0_1 0_2\rangle + |1_1 1_2\rangle\right), \tag{3.5.13}$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}\left(|0_1 0_2\rangle - |1_1 1_2\rangle\right), \tag{3.5.14}$$

where the subscripts "1" and "2" denote the particles 1 and 2, respectively. These four states are eigenstates of Bell operators, and they consist of a basis.

There is an important characteristic for the C^e-qubit: correlation, i.e., the involved particles are correlated or anti-correlated until the part of particles are measured so that the C^e-qubit is collapsed. As an example, the correlation relationship of the particles in Eq.(3.5.12) is as follows: if particle 1 is in the state $|0\rangle$, then the particle 2 is in the state $|1\rangle$. Otherwise, if the particle 1 is in the state $|1\rangle$ then the particle 2 is in the state $|0\rangle$.

For $N = 3$ and $N = 4$ they represent the GHZ state. A GHZ state is a certain type of entangled quantum states which involves at least three subsystems (particles). It was first studied by Greenberger, Horne, and Zeilinger in 1989 [**?**]. They have noticed the extremely non-classical properties of the state. Here, we are interested in the case of $N = 3$, i.e., the GHZ triplet state. Eq.(3.5.10) reduces to eight GHZ triplet states for $N = 3$, one of these states is expressed as following form,

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|z + z + z+\rangle + |z - z - z-\rangle). \tag{3.5.15}$$

Suppose that three parties, for example, Charly, Alice, and Bob, share one particle each from a three-particle entangled GHZ state, then the GHZ state may be represented by

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|z+\rangle_c|z+\rangle_a|z+\rangle_b + |z-\rangle_c|z-\rangle_a|z-\rangle_b), \tag{3.5.16}$$

where the subscripts a, b, and c refer to Alice, Bob, and Charly, respectively.

Defining the eigenstates x and y as

$$\begin{cases} |x+\rangle = \dfrac{1}{\sqrt{2}}(|z+\rangle + |z-\rangle), \quad |x-\rangle = \dfrac{1}{\sqrt{2}}(|z+\rangle - |z-\rangle), \\ |y+\rangle = \dfrac{1}{\sqrt{2}}(|z+\rangle + \mathrm{i}|z-\rangle), \quad |y-\rangle = \dfrac{1}{\sqrt{2}}(|z+\rangle - \mathrm{i}|z-\rangle), \end{cases} \tag{3.5.17}$$

the GHZ triplet state is rewritten as one of the following forms,

$$\begin{cases} |\psi_1\rangle = \dfrac{1}{2}\left[(|x+\rangle|x+\rangle + |x-\rangle|x-\rangle)|x+\rangle + (|x+\rangle|x-\rangle + |x-\rangle|x+\rangle)|x-\rangle\right], \\ |\psi_2\rangle = \dfrac{1}{2}[(|y+\rangle|y-\rangle + |y-\rangle|y+\rangle)|x+\rangle + (|x+\rangle|x-\rangle + |x-\rangle|x+\rangle)|x-\rangle], \\ |\psi_3\rangle = \dfrac{1}{2}[(|y+\rangle|x-\rangle + |y-\rangle|x-\rangle)|y+\rangle + (|y+\rangle|x+\rangle + |y-\rangle|x-\rangle)|y-\rangle], \\ |\psi_4\rangle = \dfrac{1}{2}[(|x+\rangle|y-\rangle + |x-\rangle|y+\rangle)|y+\rangle + (|x+\rangle|y+\rangle + |x-\rangle|y-\rangle)|y-\rangle]. \end{cases} \tag{3.5.18}$$

The above decomposition demonstrates the correlation among three particles. For example, if one particle is in the state $|x+\rangle$ and the second particle in the state $|x+\rangle$ in the first expression of Eq.(3.5.18), the third particle must be in the state $|x+\rangle$ because of the correlation of the GHZ triplet states. Making use of Eq.(3.5.18), one may construct a lock-up table to summarize these properties of GHZ states.

Table 3.2 demonstrates two important properties of the GHZ triplet states. First, anyone of three participants, e.g., Alice, Bob, Charly in traditional, can determine whether the other two participators' results are the same or opposite and will gain no knowledge on what their results actually are, if he (she) knows what measurements have been made by the other two participators. Secondly, the GHZ triplet state allows two parties jointly, but only jointly, to determine which was the measurement outcome of the third party. Therefore, if the measurement directions of three participators are public, the combined result of any two participators can determine what the result of the third party's measurement is. These properties have been employed in the quantum cryptography, especially in the quantum key distribution. For example, these properties have been exploited in the multi-party quantum key distribution system [10, 11].

Table. 3.2. Correlation results of GHZ triplet states

Trent	$\|x+\rangle$	$\|x-\rangle$	$\|y+\rangle$	$\|y-\rangle$
Alice	$\|x+\rangle$	$\|x+\rangle$	$\|x+\rangle$	$\|x+\rangle$
Bob	$\|x+\rangle$	$\|x-\rangle$	$\|y-\rangle$	$\|y+\rangle$
Alice	$\|x-\rangle$	$\|x-\rangle$	$\|x-\rangle$	$\|x-\rangle$
Bob	$\|x-\rangle$	$\|x+\rangle$	$\|y+\rangle$	$\|y-\rangle$
Alice	$\|y+\rangle$	$\|y+\rangle$	$\|y+\rangle$	$\|y+\rangle$
Bob	$\|y-\rangle$	$\|y+\rangle$	$\|x-\rangle$	$\|x-\rangle$
Alice	$\|y-\rangle$	$\|y-\rangle$	$\|y-\rangle$	$\|y-\rangle$
Bob	$\|y+\rangle$	$\|y-\rangle$	$\|x+\rangle$	$\|x-\rangle$

3.5.3 Distinguishability

The quantum private communication is often associated with the comparisons of various quantum states (qubits) or quantum operations (quantum gates). Such a kind of comparisons depends on the distinguishability or indistinguishability of considered qubits or quantum gates. Accordingly, this subsection introduces the quantum distinguishability, which is a fundamental notion in quantum mechanics. Two aspects, i.e., the distinguishability of various quantum states and distinguishability of quantum operations, are involved.

1) Indistinguishability of Qubits

In quantum mechanics, the indistinguishability of the quantum states (qubits) has become a profound physical property. Especially, this property has been widely used in the quantum cryptography and subsequently the quantum private communication. Naturally, the indistinguishability of quantum states comes from the nonorthogonality of quantum states since such quantum states cannot be measured exactly according to the Heisenberg uncertainly principle. Accordingly, the distinguishability and nonorthogonality of quantum states are equal physically. Generally, the indistinguishability of qubits is defined mathematically as follows.

Definition 3.5.1 Let $|\psi\rangle, |\phi\rangle \in \mathscr{H}$ be two arbitrary qubits in the Hilbert space. If the inner product of these qubits is zero, i.e., $\langle\psi|\phi\rangle = 0$, then $|\psi\rangle$ and $|\phi\rangle$ are orthogonal, consequently, these states $|\psi\rangle$ and $|\phi\rangle$ can be exactly distinguishable. Otherwise, if the inner product of these qubits is not zero, i.e., $\langle\psi|\phi\rangle \neq 0$, these states are nonorthogonal and they are indistinguishable.

In term of the definition, if arbitrary two qubits are nonorthogonal, they must be indistinguishable. While if two qubits are orthogonal, they must be distinguishable. Thus the indistinguishability is equivalent to the nonorthogonality. The indistinguishability of qubits is described quantificationally using the so-called indistinguishable degree D, which is written as

$$D = |\langle\psi|\phi\rangle| = \cos\theta, \tag{3.5.19}$$

where θ is the angle between $|\psi\rangle$ and $|\phi\rangle$ and $0 \leq \theta \leq \pi/2$. Fig.3.14 presents an intuitive description on the indistinguishability of qubits.

To determine the difference between qubits $|\psi\rangle$ and $|\phi\rangle$, they are expressed in basis $\{|0\rangle, |1\rangle\}$,

$$|\psi\rangle = \alpha_1|0\rangle + \beta_1|1\rangle,$$

and

$$|\phi\rangle = \alpha_2|0\rangle + \beta_2|1\rangle.$$

Obviously, two qubits $|\psi\rangle$ and $|\phi\rangle$ have components $\alpha_1|0\rangle$ and $\alpha_2|0\rangle$ in the $|0\rangle$ axis, respectively, and components $\beta_1|1\rangle$ and $\beta_2|1\rangle$ in axis $|1\rangle$, respectively. Therefore, qubit $|\psi\rangle$ overlaps qubit $|\phi\rangle$, and the overlapped angle is θ. As

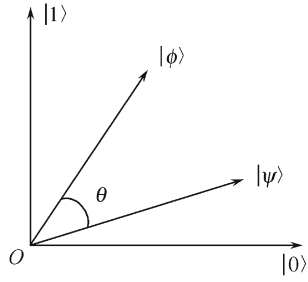

Fig. 3.14. Overlaps of two arbitrary qubits

examples, two special cases are described in the follows. When $\theta = \pi/2$, $D = 0$ means $|\psi\rangle$ and $|\phi\rangle$ are distinguishable. At this condition, $|\psi\rangle$ and $|\phi\rangle$ are orthogonal. When $\theta = 0$, $D = 1$ which means $|\psi\rangle$ and $|\phi\rangle$ is completely indistinguishable since $|\psi\rangle$ and $|\phi\rangle$ are parallel in this case. At this situation, $|\psi\rangle$ and $|\phi\rangle$ are nonorthogonal.

Clearly, to obtain available information from a qubits set which consists of nonorthogonal qubits, the involved qubits should be distinguished. But, unfortunately, there are no approach to distinguish exactly nonorthogonal qubits. Therefore, one can only reach this aim using approximate approach. Investigations show that the POVM measurement is an optimal approach for distinguishing the nonorthogonal qubits. By far, many approaches for distinguishing approximately qubits have been presented. In the following two early approaches and a new approach which uses a control-swap operation are presented.

(1) Bennett approach

In terms of qubits $|\psi\rangle$ and $|\phi\rangle$, one may construct two measurement operators,

$$\begin{cases} P_\psi = 1 - |\psi\rangle\langle\psi|, \\ Q_\phi = 1 - |\phi\rangle\langle\phi|. \end{cases} \tag{3.5.20}$$

Then measure qubits $|\psi\rangle$ and $|\phi\rangle$ using the constructed operators P_ψ and Q_ϕ. This operation gives the following results,

$$\begin{cases} p(\psi)_P = \langle\psi|P_\psi|\psi\rangle = 0, \\ p(\psi)_Q = \langle\phi|P_\psi|\phi\rangle = 1 - \cos^2\theta, \\ p(\phi)_P = \langle\psi|P_\phi|\psi\rangle = 1 - \cos^2\theta, \\ p(\phi)_Q = \langle\phi|P_\phi|\phi\rangle = 0. \end{cases} \tag{3.5.21}$$

Above equations show that if one measures the qubits set $\{|\psi\rangle, |\phi\rangle\}$ using the operator P_ψ, qubits $\{|\psi\rangle, |\phi\rangle\}$ are distinguished in the following ways: if

there is no measurement result the qubit is $|\psi\rangle$, otherwise the qubit is $|\phi\rangle$. Also if the qubit set $\{|\psi\rangle, |\phi\rangle\}$ is measured using the operator P_ϕ, one may obtains similar results. However, one may find $p(\psi)_Q \neq 1$ and $p(\phi)_P \neq 1$, which means there are inconclusive results. The corresponding probability is

$$p^e = 1 - p(\psi)_Q = 1 - p(\phi)_P = \cos^2\theta, \tag{3.5.22}$$

which means the qubits $\{|\psi\rangle, |\phi\rangle\}$ cannot be distinguished completely.

(2) Ekert approach

Ekert has constructed the following measurement operators,

$$\begin{cases} A_\psi = \dfrac{1 - |\psi\rangle\langle\psi|}{1 - |\psi\rangle\langle\phi|}, \\ A_\phi = \dfrac{1 - |\phi\rangle\langle\phi|}{1 - |\psi\rangle\langle\phi|}, \\ A_? = 1 - A_\psi - A_\phi. \end{cases} \tag{3.5.23}$$

Easily, above measurement operators are positive operators and $A_\psi + A_\phi + A_? = I$. These operators construct a POVM measurement. Of course, the qubit set $\{|\psi\rangle, |\phi\rangle\}$ cannot be distinguished exactly yet. There is still an inconclusive result with probability,

$$p_? = |\psi\rangle\langle\phi| = \cos\theta. \tag{3.5.24}$$

(3) Controlled-swap approach

For the aim of comparisons of qubits, above approaches will destruct the qubits although some comparison results may be obtained. In some cases, however, one has to distinguish various qubits but not destruct them. To solve this problem, a useful approach was proposed in Ref.[**?**] may be employed. In this approach, a machine for comparison of two arbitrary quantum states $|\Phi\rangle$ and $|\Phi'\rangle$ by using the controlled-swap operation is employed. The machine denoted U completes the following operations on the states $|\Phi\rangle$, $|\Phi'\rangle$, and $|0\rangle$ and generates a composite qubit,

$$\begin{aligned} U|0\rangle|\Phi\rangle|\Phi'\rangle &= (H \otimes I)(U_{SWAP})(H \otimes I)|0\rangle|\Phi\rangle|\Phi'\rangle \\ &= \frac{1}{\sqrt{2}}(H \otimes I)(U_{SWAP})(|0\rangle|\Phi\rangle|\Phi'\rangle + |1\rangle)|\Phi\rangle|\Phi'\rangle) \\ &= \frac{1}{\sqrt{2}}(H \otimes I)(|0\rangle|\Phi\rangle|\Phi'\rangle + |1\rangle)|\Phi'\rangle|\Phi\rangle) \\ &= \frac{1}{2}(|0\rangle(|\Phi\rangle|\Phi'\rangle + |\Phi'\rangle|\Phi\rangle) + |1\rangle(|\Phi\rangle|\Phi'\rangle - |\Phi'\rangle|\Phi\rangle)), \end{aligned} \tag{3.5.25}$$

where H is the Hadamard transform, i.e., the Hadamard gate, and U_{SWAP} is the controlled-SWAP gate (controlled by the first qubit) defined by

$$\begin{cases} U_{SWAP}|0\rangle|\Phi\rangle|\Phi'\rangle = |0\rangle|\Phi\rangle|\Phi'\rangle, \\ U_{SWAP}|1\rangle|\Phi\rangle|\Phi'\rangle = |1\rangle|\Phi'\rangle|\Phi\rangle. \end{cases} \tag{3.5.26}$$

The operation presented in Eq.(3.5.25) may be sketched using Fig.3.15. If the measurement result is "1", a determined result is obtained, i.e., $|\Phi\rangle \neq |\Phi'\rangle$. However, if the measurement result is "0", one can judge $|\Phi\rangle = |\Phi'\rangle$ with an error probability,

$$p_e = \frac{1+\epsilon^2}{2}, \tag{3.5.27}$$

where $\epsilon = |\langle\Phi|\Phi'\rangle|$.

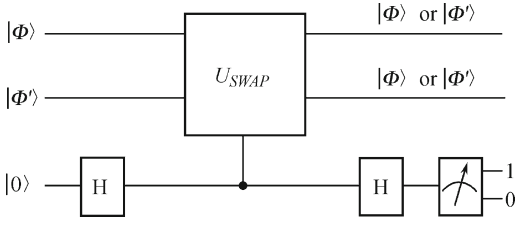

Fig. 3.15. Comparatione between $|\Phi\rangle$ and $|\Phi'\rangle$ for one time

To give more accurate comparisons between $|\Phi\rangle$ and $|\Phi'\rangle$, one may proceed with n identical copies of these states. Then comparison operation will be performed τ times. Finally, one may obtain an error probability,

$$p_e^{\tau} = \left[\frac{1+\epsilon^2}{2}\right]^{\tau}, \tag{3.5.28}$$

after repeating τ times. Apparently, one may find $p^{\tau} \to 0$ for $\tau \to +\infty$.

The indistinguishability of qubits has been broadly applied in the quantum private communication. It is mainly exploited in guaranteing the security of the quantum cryptographic schemes such as the quantum key distribution scheme and quantum cryptosystem. The details will be described in Chapters 4 and 5.

2) Distinguishability of Quantum Operations

Unlike the discrimination of nonorthogonal states which is impossible to achieve given arbitrarily large but finite number of copies, it has been proven that one can always discriminate any finite set of quantum operations with certainty using a suitable quantum network consisted of quantum operations [13 – 16] with the assistance of a suitable input state. The involved quantum operations may be unitary operation or quantum measurement. Usually, the involved input state is a multiparticle entangled state, but in some special cases the non-entangled state is also possible. For example, a multiparticle state with a local operation and classic communication (LOCC) can be employed for exactly discrimination of unitary operations [16].

Suppose that one has an unknown unitary operation U, which is secretly chosen from a set of pre-specified unitary operations $\{U_1, U_2, \ldots, U_N\}$. To

distinguish these unitary operations, one should firstly design a suitable quantum network consisting of quantum operations according to the employed input state. In documentary, a special quantum network which is reduced to the form of $U^{\otimes t}$ has been widely employed [16]. This quantum network is also called the parallel scheme. For clearly, a special situation for comparing two arbitrary quantum operations, e.g., U_1 and U_2, is exemplified here. Since a quantum network may be denoted using a matrix, the quantum network consisting of U_1 and U_2 may be denoted $\mathcal{N}_{U_1}$ and $\mathcal{N}_{U_2}$, respectively. To distinguish U_1 and U_2 one needs to distinguish the outputs $|y_1\rangle$ and $|y_2\rangle$ of $\mathcal{N}_{U_1}$ and $\mathcal{N}_{U_2}$, respectively. Thus $|y_1\rangle$ and $|y_2\rangle$ must be orthogonal, i.e., $|\langle y_1|y_2\rangle| = 0$. Let $|x\rangle$ be the input state (entangled state or non-entangled state). Consider $|y_i\rangle = \mathcal{N}_{U_i}|x\rangle$ with $i = 1, 2$, one obtains

$$\langle x|\mathcal{N}_{U_2}^{\dagger}\mathcal{N}_{U_1}|x\rangle = 0. \tag{3.5.29}$$

The above equation denotes that the operators U_1 and U_2 may be discriminated with a suitable structure for the quantum network $\mathcal{N}$ and the input state $|x\rangle$. In documentary, it has been proven that such quantum network and input state may always be found.

The distinguishable characteristics of quantum operations may be applied in many scenarios, such as the quantum computation, quantum signature scheme, quantum measurement, etc. Especially, the application of this property in quantum signature scheme will be discussed in Chapter 6.

3.5.4 Quantum No-cloning

The no-cloning theorem is a result of quantum mechanics which forbids the creation of identical copies of an arbitrary unknown quantum state. It was stated by Wootters, Zurek, and Dieks in 1982 [**?**, **?**], and has profound implications in the quantum computing and related fields. The property of quantum no-cloning is a vital ingredient in the quantum cryptography, as it forbids eavesdroppers from creating copies of a transmitted quantum cryptographic key. However, the quantum no-cloning is passive in some situations, especially in the quantum computation. For example, this property leads the exact quantum-copy which is very easy in the classic computation to be impossible. In addition, the no-cloning property prevents us from using classical error correction techniques on quantum states. For example, one cannot create backup copies of a state in the middle of a quantum computation, and use them to correct subsequent errors. Error correction is vital for practical quantum computing, and for some time this was thought to be a fatal limitation. In 1995, Shor and Steane revived the prospects of quantum computing by independently devising the first quantum error correcting codes, which circumvent the no-cloning theorem.

1) Quantum No-cloning Theorem

The quantum cloning is a process that takes an arbitrary, unknown quantum state and makes an exact copy without altering the original state in any way. In Dirac notation, the process of quantum cloning is described by

$$U|\psi\rangle_A|e\rangle_B = |\psi\rangle_A|\psi\rangle_B \tag{3.5.30}$$

where U is an actual cloning operation, $|\psi\rangle_A$ is a state to be cloned, $|e\rangle_B$ is an initial state of the copy and $|\psi\rangle_B$ represents the final copy state which is exact same as the state $|\psi\rangle_A$. In most scenarios, however, the quantum cloning is forbidden by the laws of quantum mechanics as shown by the no-cloning theorem, which proves that there is no such operation U that can perform the cloning operation for any arbitrary qubit. The quantum non-cloning theorem is presented in follows.

Theorem 3.5.4 An arbitrary, unknown quantum state cannot be copied exactly without altering the original state in any way.

Proof Suppose that the state of a quantum system, which needs to be cloned, is $|\psi\rangle_q$. In order to make a copy, a system with the same state space and initial state $|e\rangle_B$ is chosen. The initial, or blank state must be independent of $|\psi\rangle_q$, of which one has no prior knowledge. The composite system is then described by the tensor product, and its state is $|\psi\rangle_q|e\rangle_B$.

There are only two ways to manipulate the composite system. One could perform an observation, which irreversibly collapses the system into some eigenstates of the observable, corrupting the information contained in the qubit. This is not obviously what one wants. Alternatively, one could control the Hamiltonian of the system, and thus the time evolution operator U up to some fixed time interval, which is a unitary operator. Then U acts as a copier provided that

$$U|\psi\rangle_q|e\rangle_B = |\psi\rangle_q|\psi\rangle_B, \tag{3.5.31}$$

and

$$U|\phi\rangle_q|e\rangle_B = |\phi\rangle_q|\phi\rangle_B, \tag{3.5.32}$$

for all $|\phi\rangle$ and $|\psi\rangle$. By definition of the unitary operator, U preserves the inner product,

$$\langle e|_B\langle\psi|_q U^* U|\phi\rangle_q|e\rangle_B = |\phi\rangle_q|\phi\rangle_B, \tag{3.5.33}$$

i.e.,

$$\langle\phi|\psi\rangle = \langle\phi|\psi\rangle^2. \tag{3.5.34}$$

This is clearly not true in general. Therefore no such an operation U exists. This proves the no-cloning theorem.

Alternatively, one can argue using just linearity of U: if the cloning succeeds in general, one must have

$$U(2\psi) \otimes e = (2\psi) \otimes (2\psi). \tag{3.5.35}$$

By linearity, the left side equals

$$2U(\psi \otimes e) = 2(\psi \otimes \psi), \tag{3.5.36}$$

while the right hand side is

$$4(\psi \otimes \psi). \tag{3.5.37}$$

This is a contradiction, therefore no-cloning holds.

Following this theorem, a corollary for nonorthogonal qubits is derived as follows by some researchers.

Corollary Any qubit from a set of nonorthogonal qubits cannot be cloned without destroying the original qubits.

Note that the state of a quantum system can be entangled with the state of another quantum system. For instance, one can use the controlled-NOT gate and the Walsh-Hadamard gate to entangle two qubits. However, this is not the cloning procedure. No well-defined state can be attributed to a subsystem of an entangled state. The term cloning refers to a process whose end result is a separable state with identical factors.

2) Quantum Copying

Above arguments shows any unknown qubit is non-cloning. Actually, this result may be extended: any nonorthogonal qubits are non-cloning. Subsequently, the exactly copy, which is very common in the classic information, is impossible in the quantum case. Of course, the given orthogonal qubits can be copied exactly, which has been shown in the above.

The quantum copy procedure is expressed as follows,

$$U_c : |\psi\rangle|0\rangle \longmapsto |\psi\rangle|\psi'\rangle, \tag{3.5.38}$$

where $|\psi'\rangle$ is a copied qubit and U_c denotes a general quantum copy operation. Apparently, in the quantum copying procedure the output qubit can be very similar to the original unknown qubit $|\psi\rangle$ but it cannot never reach the original qubit due to the no-cloning theorem. The distance between the original qubit and the copied qubit may be described in two ways. The first way is using the so-called trace distance which is defined as

$$D(\rho_{in}, \rho_{out}) \equiv \frac{1}{2} Tr|\rho_{in} - \rho_{out}|, \tag{3.5.39}$$

where as per usual we define $|A| \equiv \sqrt{A^\dagger A}$. Since the density can be denoted as

$$\rho = \frac{I + \mathbf{r} \cdot \sigma}{2}, \tag{3.5.40}$$

one has

$$D(\rho_{in}, \rho_{out}) = \frac{1}{2} Tr|\mathbf{r}_{in} - \mathbf{r}_{out}|, \tag{3.5.41}$$

where $\mathbf{r}_{in}$ and $\mathbf{r}_{out}$ are parameters associated with the input state ρ_{in} and output state ρ_{out}, respectively.

Another way is using the fidelity to describe approximately the copy procedure. Generally, the fidelity is defined as

$$F_m = Tr\sqrt{\rho_{out}^{\frac{1}{2}}\rho_{in}\rho_{out}^{\frac{1}{2}}}. \tag{3.5.42}$$

where ρ_{in} and ρ_{out} denote the input and output states of the system, respectively. If the input and output states are pure states, then in this case the fidelity may be written as follows,

$$F_p = \langle\psi|\psi'\rangle, \tag{3.5.43}$$

where $|\psi'\rangle$ is the copied qubit.

3.6 Information Property

To describe quantificationally the information of a qubit, two notions, i.e., the carried information of qubit and accessible information of qubit transmitted in a quantum channel, are defined in the quantum information. The carried information of qubits specifies the maximal information carried by a qubit, which is actually the quantum information. While the accessible information means the information may be obtained by the communicators. Obviously, the information of qubits is different from that of classic bits. In the classic case, the carried information is the same as the accessible information, which is actually the Shannon information. In the quantum case, to obtain the information the communicator should measure the qubit. Since novel properties of the quantum measurement, after having been measured the qubit is destructed. In addition, due to the superposition of qubit the communicator can only obtained part information.

3.6.1 Single Qubit Information

Give a qubit $|\psi\rangle = c_1|e_1\rangle + c_2|e_2\rangle$, the quantum information of the given qubit is described using the von Neumann entropy,

$$S(\rho) = Tr(\rho \ln \rho). \tag{3.6.1}$$

where Tr denotes the trace, and ρ is a density matrix. To solve the above equation, one may firstly diagonalize the density matrix, then obtain $\ln \rho$ using the operator function. After that the Von Neumann entropy is given easily.

The accessible information, i.e., the Shannon information, may be calculated using the Shannon entropy formula,

$$H(p) = \sum_j p_j \log \frac{1}{p_j}, \tag{3.6.2}$$

where $j = 1, 2, \ldots, n$, and p_j is a probability of the output jth result with a measurement E_j. If the communicator measures the qubit $|\psi\rangle$ using the projective measurement, probabilities are given as follow,

$$p_j = |\langle e_j|\psi\rangle|^2 = |c_j|^2. \tag{3.6.3}$$

Thus

$$H(p) = \sum_{j=1}^{2} |\langle e_j|\psi\rangle|^2 \log |\langle e_j|\psi\rangle|^2. \tag{3.6.4}$$

3.6.2 Nonorthogonal Qubits Information

Suppose that there is a set of nonorthogonal qubits $\{|\psi\rangle, |\varphi\rangle\}$, where $\langle\psi|\varphi\rangle \neq 0$. In this case, since the total density operator ρ is direct product of ρ_ψ and ρ_φ, i.e.,

$$\rho = \rho_\psi \otimes \rho_\varphi, \tag{3.6.5}$$

the quantum information, i.e., the von Neumann entropy, may be calculated as follows,

$$S(\rho) = Tr[(\rho_\psi \otimes \rho_\varphi) \ln(\rho_\psi \otimes \rho_\varphi)]. \tag{3.6.6}$$

Since $\langle\psi|\varphi\rangle \neq 0$ the accessible information cannot be obtained exactly. Generally, the accessible information follows the Holevo bound presented initially in Ref.[19] demonstrated in the theorem 2.4.1 in Section 2.4.2. The Holevo bound is an exceedingly useful upper bound on the accessible information that plays an important role in many applications of the quantum information theory [20].

References

[1] Shannon C E (1948) A mathematical theory of Communication. Bell System Technical Journal, 27(4): 397 – 423

[2] Cleve R, Gottesman D, Lo H K (1999) How to share a quantum secret. Physical Review Letters, 83: 648 – 651

[3] Zeng G H (2006) Quantum cryptology. Science Press, Beijing

[4] Nielsen M A, Chuang I L (2000) Quantum computation and quantum information. Cambridge University, London

[5] Zeng G H, Lee M H (2008) A generalized reverse block jacket transform. IEEE Transactions on Circuit and System I, 55(6): 1589 – 1600

[6] Einstein A, Podolsky B, Rosen N (1935) Can quantum mechanical description of physical reality be considered complete? Physical Review, 47: 777 – 780

[7] Bengtsson I, Zyczkowski K (2006) Geometry of quantum states. An introduction to quantum entanglement. Cambridge University Press, London

[8] Steward E G (2008) Quantum mechanics: Its early development and the road to entanglement. World Scientific Publishing, Singapore

[9] Greenberger D M, Horne M A, Zeilinger A (1989) Going beyond Bell's theorem. Bell's theorem, quantum theory, and conceptions of the universe edited by Kafatos M, Kluwer, Dordrecht, 69 – 72

[10] Hillery M, Buzek V, Berthiaume A (1999) Quantum secret sharing. Physical Review A, 59: 1829 – 1834

[11] Tittel W, Zbinden H, Gisin N (2001) Experimental demonstration of quantum secret sharing. Physical Review A, 63: 1 – 9

[12] Buhrman H, Cleve R, Watrous J, et al (2001) Quantum Fingerprinting. Physical Review Letters, 87: 1 – 4

[13] Acín A (2001) Statistical distinguishability between unitary operations. Physical Review Letters, 87: 1 – 4

[14] Mauro G, D'Ariano, Presti P L, et al (2001) Using entanglement improves the precision of quantum measurements. Physical Review Letters, 87: 1 – 4

[15] Sacchi M F (2005) Optimal discrimination of quantum operations. Physical Review A, 71: 1 – 4

[16] Duan R, Feng Y, Ying M (2008) Local distinguishability of multipartite unitary operations. Physical Review Letters, 100: 1 – 4

[17] Wootters W K, Zurek W H (1982) A single quantum cannot be cloned. Nature (London), 299: 802 – 803

[18] Dieks D (1982) Communication by EPR devices. Physics Letters A, 92(6): 271 – 272

[19] Holevo A S (1973) Information-theoretic aspects of quantum measurement. Problems of Information Transmission, 9(2): 31 – 42

[20] Nielsen M A, Chuang I L (2000) Quantum computation and quantum information. Cambridge University Press, London

4 Quantum Key Distribution

The key management which is associated with the key generation, key distribution, key storage, and key updating has become an important issue in the private communication. This chapter introduces a novel approach of generating and distributing key-pair via quantum ways. The aim is to illustrate how to obtain secure keys via quantum key distribution (QKD) techniques. Four modules, i.e., the quantum coding, quantum transmission, eavesdropping detection and key distillation, of a QKD procedure are described. In addition, a security model for the QKD is established.

Chapters 1 – 3 consist of the first part which describes the basic theory for the quantum private communication. In this part, a communication model and a quantum security theory for the quantum private communication have been constructed. In addition, characteristics of qubit has been described. As mentioned in previous, the aim of the quantum private communication is to protect the confidentiality and authentication of communication systems in quantum ways. To illustrates how to reach this aim one should move on to the second part composed of Chapter 4 – 6. Generally, the protection ways of the confidentiality and authentication are associated with a suitable key management system and cryptographic schemes. This chapter introduces how to implement the secure key management in quantum ways. While the cryptographic algorithms are addressed in the following two chapters.

4.1 Intuition on QKD

To ensure the confidentiality and authentication of communication systems, the cryptosystem which will be introduced in Chapter 5 is always employed. As mentioned in Chapter 1, a cryptosystem consists of the encryption algorithm, decryption algorithm, and key management system. Since the encryption algorithm and decryption algorithm are always public in the modern secure communication, the privacy of a cryptosystem depends completely on the key management system. Unfortunately, it is difficult to generate keys with unconditional security in the classic cryptology as well as classic private communication. This gives rise to the problem of how to implement a secure key management system. For example, difficulties of the key management

leads the classic Vernam cipher to be impractical in commerce applications although it has been proven to be unconditional security.

The mentioned problems for the key management have been partly solved using QKD techniques, which were originated by Bennett and Brassard in 1984 [1]. Making use of QKD techniques one may generate and distribute secure keys between two communicators who share no initial information. Currently, QKD has become the most important part in the quantum cryptography as well as the quantum private communication. Also, QKD is the most mature part in theory and technology since it has been presented. By far, various QKD schemes have been presented and some have been implemented practically [2 – 9]. A summarization on QKD was firstly presented in 2002 in Ref.[10].

The so-called QKD is a technique that allows two parties, conventionally called Alice and Bob, to share a common secret key for cryptographic purposes. If an eavesdropper, conventionally called Eve, tries to eavesdrop the key, she will be detected by the communicators using suitable quantum laws, e.g., the well-known Heisenberg uncertainty principle. This section presents an intuitive description on the definition of QKD and its kernel techniques involved. The details regarding QKD will be described in subsequent sections. Generally, a QKD scheme involves four stages: quantum coding, quantum transmission, eavesdropping detection, and key distillation. These involved modules are diagramed in Fig.4.1.

Fig. 4.1. Diagram of four basic stages of quantum key distribution

In the quantum coding stage, the sender called usually Alice chooses qubits from a quantum source to encode a random-bit string which is no meaningful. The quantum source is defined similar to the classic resource. Thus a quantum source is also expressed using quantum symbol set $\mathcal{S} = \{s_i | i = 1, 2, \ldots, n\}$ where s_i denote the ith quantum symbol or quantum letter. For example, $\mathcal{S}_1 = \{|0\rangle, |1\rangle\}, \mathcal{S}_2 = \{|0\rangle, |+\rangle\}$, and $\mathcal{S}_3 = \{|x\rangle, |p\rangle\}$ are all quantum symbol sets, where x and p denote the position and momentum. Generally, there are two kinds of quantum symbol sets, i.e., discrete symbol set and continuous symbol set. Clearly, $\mathcal{S}_1$ and $\mathcal{S}_2$ are discrete symbol sets and $\mathcal{S}_3$ is a continuous symbol set. At the first stage of the QKD procedure, Alice randomly chooses symbols from a chosen quantum source to encode a random-bit string with a probabilistic distribution function, e.g., an equivalently probabilistic distribution or a Gaussian-distribution. For the sake of security, the random-bit string should be a truly random number but not the pseudo-randomly generated bits.

As an example, the quantum source consists of $\mathcal{S}_{BB84} = \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ in the well-known BB84 protocol [1] which will be described in next section.

To carry the meaningless random binary bit string, Alice encodes each element in the string using qubits choosing from the source $\mathcal{S}_{BB84}$ according to the following code rule: $0 \rightarrow |0\rangle$ or $0 \rightarrow |+\rangle$ and $1 \rightarrow |1\rangle$ or $1 \rightarrow |-\rangle$. Then a random qubit-string consists of quantum symbols from $\mathcal{S}_{BB84}$ is obtained. This string will be sent to Bob in the second stage. Clearly, the coding procedure is actually a quantum source coding which is apparently different from the quantum error correction code (QECC).

After having finished the first stage, communicators enter the quantum transmission stage. In this stage, the encoded qubits are sent physically from one communicator to another communicator, i.e., from Alice to Bob, through a communication channel. Obviously, a QKD scheme requires, in this stage, a transmission channel so that the quantum carriers taken the encoding qubits are transmitted from Alice to Bob. Theoretically, any particle obeying laws of quantum physics can be employed. In practices, however, the quantum carriers are usually the photons (an elementary particle of light), or light wave with quantum effect due to the excellent transmission characteristics of light. The optical fiber (e.g., for telecommunication networks) or open air (e.g., for satellite communications) are often adopted as the transmission channel.

Generally, there are two kinds of transmission ways for the qubits, i.e., the direct transmission and entanglement transmission. In the direct transmission way, the encoded qubits (information qubits) are directly transmitted from Alice to Bob carried by a suitable qubit signal. This way is the same as that in the classic communication. Both BB84 protocol and B92 protocol [2] are implemented in this way. While the encoded qubits (information qubits) are instantaneously transmitted from Alice to Bob using the entanglement correlation which has been described in Section 3.5.2 in the entanglement transmission way. Here, the entanglement transmission is used to set up an entangled quantum channel. The encoded qubits are not transmitted in the established channel like the direct transmission way although entangled qubits have been transmitted for one communicator to others. The entanglement transmission way is always adopted in the QKD scheme based entangled qubit, e.g., EPR protocol [3].

During the transmission between Alice and Bob, Eve might eavesdrop the quantum channel so that she may spy on potential secret key bits. Unfortunately, Eve's operation on the quantum channel may be detected in principle using appropriate quantum laws. However, how to detect Eve is a technical problem which actually associates with the security of the adopted QKD scheme. In addition, the employed detection approaches are different in various QKD schemes. Therefore, the eavesdropping detection stage is very important. This leads an important stage: eavesdropping detection. This is actually a quantum channel authentication procedure. In practices, the eavesdropping is judged using the so-called quantum bit error rate which is defined with the ratio of errors and transmitted qubits. To design a secure QKD scheme two important properties, i.e., the nonorthogonality and

entanglement correlation, are often employed. These properties provide useful ways for the eavesdropping detection.

The final stage is the key distillation. After having finished the quantum coding stage, quantum transmission stage, and eavesdropping detection stage, the legitimate communicators Alice and Bob obtain a raw key. However, there are some error bits generated by Eve's operation and communicators' apparatus in the generated raw key. In addition, Eve might possess some available key bits via her eavesdropping operations on the quantum channel. These will influence the availability and security of the generated key strings. Accordingly, one has to correct errors and enhance the privacy of the key-string. To correct errors an approach called reconciliation is adopted [11 – 14]. This approach depends on the classic error-correction techniques. By far, the utilized approach is mainly associated with the Hamming code or low density parity code (LDPC). To enhance the privacy of the final key, the obtained raw key is distilled to be a shorter key so that Eve's information on the final key becomes arbitrary less. This procedure is usually called the privacy amplification [15, 16]. Both the reconciliation and privacy amplification are indispensable techniques in the QKD scheme. They will be introduced in detail in subsequent sections.

To perform the error-correction and privacy amplification procedures, a public classical channel with authentication function is necessary in the final stage. This channel has two important characteristics, namely, publicness and authentication. As an important consequence, any message exchange by legitimate communicators on this channel there will be known inevitably by Eve. Since the authentication characteristic has been involved in these stages, communicators should pre-share a short authentication key. The authentication key may be pre-generated, or generated instantaneously with QKD procedures. The details on the authentication will be introduced in Chapter 6.

In principle, a secure key can be obtained in a QKD scheme after having finished the above stages. However, one should note that a necessary condition has been adopted actually. That is, the information eavesdropped by Eve is less than Bob's information. Accordingly, to guarantee the obtained final key to be secure, one has to calculate the security condition for a designed QKD scheme using a suitable security model. This security model relies on the quantum security theory described in Chapter 2. By far, many security theories for QKD schemes have been presented [17 – 19]. The details will be described in Section 4.6.1.

4.2 Standard QKD Schemes

By far, many QKD schemes have been presented. These schemes may be divided into three kinds, i.e., standard QKD schemes, improved QKD schemes,

and ping-pong schemes. The standard QKD schemes mean those schemes which can be described in cryptographic primitives. According to this requirement, only the BB84 protocol and B92 protocol are regarded as the standard QKD schemes in this book. Although the EPR protocol is the first QKD scheme using entanglement property of qubits, it would rather be treated as a kind of technical implementation of the BB84 protocol than a standard cryptographic scheme since it has been proven that the EPR protocol is equivalent to the BB84 protocol [20]. The improved QKD schemes mean those schemes similar to standard schemes but with improvement on these schemes, such as the orthogonal state schemes [**?**, **?**], 3-state protocol [**?**], and 6-state scheme [**?**]. The ping-pong QKD scheme can be regarded as technical improvement scheme of the standard QKD scheme or improved QKD scheme. This kind of schemes adopts a novel physical technique of sending a quantum signal and then returning it in a quantum channel like playing ping-pong game between two participants [21, 22] so that the key rate is improved. Although the ping-pong scheme was claimed to be employed for QKD as well as quantum encryption, enough proofs show that this application on quantum encryption is insecure or even impossible since the privacy amplification used in the ping-pong scheme damages the transmitted secret data and there exists available information leakage [**?**, **?**]. Thus, the ping-pong schemes are only regarded as a kind of QKD schemes in this book.

The standard schemes, improved schemes, and ping-pong schemes are all four-stage protocols which are described in Fig.4.1. Except for these schemes, there is a novel QKD scheme which is similar to the classic public key generation scheme. This kind of QKD schemes is called as the asymmetrical quantum key scheme, which will be introduced in next chapter with the cryptosystem since it is associated closely with the encryption algorithm and decryption algorithm. This section introduces two standard QKD schemes, i.e., the BB84 protocol and B92 protocol.

4.2.1 BB84 Protocol

The BB84 protocol is the first QKD scheme published in 1984 in a computer conference [1]. The main ideas of this scheme were proposed initially in 1979 by Bennett, a scientist in IBM, and Brassard, a cryptanalyst in Montreal University in Canada, and then improved by both authors in 1989 which was finally published in the Journal of Cryptology in 1992 [2].

To generate and distribute a secure key, the legitimate communicator Alice prepares a quantum source expressed $\mathcal{S}_{BB84} = \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and a random string $R_c = \{r_i^c | i = 1, 2, \ldots, n\}$ with $r_i^c \in \{0, 1\}$. In the quantum source $\mathcal{S}_{BB84}$, the probability $p_i (i = 1, 2, 3, 4)$ of each quantum letter is the same, i.e., $p_i = 1/4$. According to the elements in the random string R_c Alice encodes the random bits using quantum letters from the quantum source.

Then a random qubit string, i.e., $R_q = \{r_i^q | i = 1, 2, \ldots, n\}$, is generated, where $r_i^q \in \mathcal{S}_{BB84}$. Note, Alice does not reveal which encoding rule she used. Thus anybody including Bob does not know detail information on each quantum bit in the generated random qubit string R_q. This is the first stage, i.e., the quantum coding stage.

After having finished the encoding procedure, Alice sends the random qubit string to Bob via a chosen quantum channel, e.g., an optical fiber or a free-space channel. In practices, each symbol in the generated qubit string is sent to Bob with a proper time interval $\Delta\tau$. After receiving the qubit from Alice, Bob measures randomly it using one of measurement bases $M = \{M_1, M_2\}$, where the measurement bases $M_1 \in \{|0\rangle, |1\rangle\}$, $M_2 \in \{|+\rangle, |-\rangle\}$, and $[M_1, M_2] \neq 0$, i.e., M_1 and M_2 are not commutation. At the same time, Bob keeps secretly his measurement results. Since Bob does not know exactly the received qubits, he can measure correctly only part of the qubits Alice sent him. This finished the second stage, i.e., the quantum transmission stage.

Now Alice and Bob move on to the eavesdropping detection stage. After finishing the measurement on all the transmitted qubits in the random qubit string R_q, Alice tells Bob which encoding rule she chosen for each key element, i.e., the adopted measurement basis for each qubit. Physically, this corresponds to comparison of the measurement bases between Alice and Bob. Through this procedure, Bob is then able to sift the correct results by discarding all the wrong measurements. To detect Eve the well-known Heisenberg uncertainty principle and quantum no-cloning theorem begin to play a pivotal role. To retrieve available information, Eve should operate the qubits transmitted in the quantum channel from Alice to Bob. However, since quantum symbols in the chosen quantum source are nonorthogonal, Eve cannot distinguish correctly the transmitted qubits $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Thus, according to the quantum no-cloning theorem Eve cannot copy the transmitted qubit with a fidelity of $F = 1$, i.e., the exact copying is impossible since the restriction of the quantum no-cloning theorem. Therefore, the eavesdropper cannot attack the qubits in offline ways like that often used in the classic scheme. This limitation leads that Eve can only attack the qubits in online ways. In this scenario Eve may intercept the quantum channel. However, Heisenberg uncertainty principle helps legitimate communicators to detect eavesdropping operations.

Intuitively, when Alice sends a qubit $|0\rangle$ or $|1\rangle$, Eve might measure it using the basis M_2 which outputs the result $|+\rangle$ or $|-\rangle$ since she has no any knowledge on the transmitted qubit. Then in the whole procedure Eve's interception will disturb the quantum channel and generate a wrong result with probability 1/2. After Bob has finished measurement on all received qubits, there is an error probability threshold 1/4 resulted by Eve's interception according to the Heisenberg uncertainty principle, i.e., $p_0^e = 25\%$. With this parameter Alice and Bob may detect eavesdropping: if the error probability p^e is more than the threshold p_0, i.e., $p^e \geq p_0^e$, the legitimate communicators abandon this communication since Eve has obtained much

more useful information on the transmitted random qubit string; otherwise Alice and Bob obtain a raw key and enter the following stage, i.e, the key distillation stage.

Before describing the key distillation stage, a simple example is presented. The above procedure is associated with the quantum coding, quantum transmission and eavesdropping detection stages. For clarity, these steps are shown in Table 4.1 with a simple example. In this example, Alice chooses a random string in Step 1 and then encodes each binary bit in the string into a qubit one by one in Step 2. This encoding procedure corresponds to choose a string of measurement bases. The encoded qubit is then sent to Bob through a quantum channel, e.g., a fiber or air channel. When Bob receives the qubit, he measures it in Step 3 by randomly choosing a measurement basis from a 2-tuple $\{\oplus, \otimes\}$, where the bases $\oplus$ and $\otimes$ can measure exactly the states $\{\updownarrow, \leftrightarrow\}$ and $\{\curvearrowleft, \curvearrowright\}$, respectively. These measurements give possible measurement results in Step 4. Clearly, these results are different from Alice's original qubit string, which implicates that errors have been generated during communication procedures. These errors are caused by Eve's operations and a noise environment, especially the Eve's operations. Accordingly, detecting eavesdropping becomes necessary. This is achieved by comparing Alice's and Bob's measurement bases in Step 5. If the error rate is low than the threshold, the protocol runs continually by throwing away the error qubits. After this operation, the corrected qubits are kept in Step 6. Then a raw key is obtained in Step 7.

Table 4.1. A simple example for BB84 protocol

Step 1	1	1	0	0	1	0	1	1	0	1
Step 2	$\updownarrow$	$\curvearrowleft$	$\leftrightarrow$	$\curvearrowright$	$\updownarrow$	$\leftrightarrow$	$\updownarrow$	$\updownarrow$	$\leftrightarrow$	$\updownarrow$
Step 3	$\oplus$	$\otimes$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$
Step 4	$\updownarrow$	$\curvearrowleft$	$\curvearrowleft$	$\curvearrowright$	$\updownarrow$	$\leftrightarrow$	$\curvearrowleft$	$\updownarrow$	$\leftrightarrow$	$\curvearrowleft$
Step 5	✓	✓		✓	✓	✓		✓	✓	
Step 6	$\updownarrow$	$\curvearrowleft$		$\curvearrowright$	$\updownarrow$	$\leftrightarrow$		$\updownarrow$	$\leftrightarrow$	
Step 7	1	1		0	1	0		1	0	

In the obtained raw key there still exist some errors which were given rise to by environment, eavesdropper, and legitimate communicators' apparatus. As consequences, there are slight differences between Alice's and Bob's raw key strings. In addition, Eve might obtain small valid information on the raw key string which may influence security of the final key. Accordingly, communicators have to enter the final stage, i.e., the key distillation stage. This stage is independent of the quantum laws since the involved techniques in this stage is completely classic. Its aim is to correct the errors and enhance the privacy of the obtain raw key. To perform this stage, an assistant classic channel is necessary. This channel is a publicly classical authenticated channel. Alice and Bob can still try to make a fully secret key. This procedure is called the secret key distillation. Usually, the secret-key distillation comprises a step called reconciliation, whose purpose is to correct the transmission errors, and

a step called privacy amplification, which wipes out Eve's information at the cost of reduced key length by using universal hash function.

To correct the errors in the raw key string the classic error-correcting techniques are always used in the reconciliation phase. By far two kinds of error-correction approaches, i.e., Hamming code and LDPC, are often adopted. Investigations show that the later is more effective. To wipe out Eve's information the universal hash function is always used. This technique reduces the length of raw key to be a short secret random string, which is the final key.

4.2.2 B92 Protocol

This protocol was proposed independently by Bennett in 1992, consequently, it is usually called B92 protocol. Since the B92 protocol works using the indistinguishability properties of two nonorthogonal qubits, it is also called a two-state protocol. Cryptographically, the B92 protocol is a revised version of the BB84 protocol although the physical natures are different in both protocols.

The B92 protocol is designed based on nonorthogonality of arbitrary two qubits in Hilbert space. The detail physical property of the indistinguishability was described in Section 3.5.3. Let $|\phi\rangle, |\psi\rangle$ be two arbitrarily nonorthogonal qubits in Hilbert space, i.e., $|\phi\rangle, |\psi\rangle \in \mathscr{H}$ and $|\langle\psi|\phi\rangle| \neq 0$. The nonorthogonality leads these states are indistinguishable, subsequently, exactly copying becomes impossible in this scenario. This characteristic is employed to guarantee the security of the B92 protocol.

The B92 protocol is executed following the route as shown in Fig.4.1. Since the key distillation stage is the same as the BB84 protocol does, and it will be addressed in detail in the Sections 4.4 and 4.5, this subsection mainly focuses on how to generate the raw key.

At the quantum coding stage, to distribute a secure key k between legitimate communicators, Alice prepares a quantum source $\mathcal{S}_{B92} = \{|\phi\rangle, |\psi\rangle|\}$ and a truly random string $R_c = \{r_i^c | i = 1, 2, \ldots, n\}$ with $r_i^c \in \{0, 1\}$, where $|\phi\rangle, |\psi\rangle \in \mathscr{H}$ and $|\langle\psi|\phi\rangle| \neq 0$. In the quantum source, the probability $p_i (i = 1, 2)$ of each quantum letter is the same, i.e., $p_i = 1/2$. According to the value of each element in the random string R_c, Alice encodes each random bit using quantum letter from the quantum source. The mapping between the random string and quantum source may be $0 \rightarrow |\phi\rangle, 1 \rightarrow |\psi\rangle$, or vice versa. Here the former mapping is adopted. Then a random qubit sequence is generated, i.e., $R_q = \{r_i^q | i = 1, 2, \ldots, n\}$ where $x_i^q \in \mathcal{S}_{B92}$. Note, Alice does not reveal which encoding rule she used. Thus anybody including Bob does not know detail information on each quantum bit in the generated random qubit string R_q.

At the second stage, Alice sends each qubit in the generated sequence

R_q one-by-one with a time interval $\Delta\tau$ to Bob. After receiving the qubit Bob measures it using the positive operator value measurement (POVM) technique which has been introduced in Section 2.3.3. The employed measurement bases denote $P(\psi)$ and $P(\phi)$. According to the theory presented in Section 2.3.3 there are two measurement results, i.e., vanishing or conclusive value. Note, the summarization of probabilities of these results is not unit since there exist inconclusive results. After having finished measurement on all qubits Bob tells Alice his measurement results, but his choice on the measurement bases $P(\psi)$ and $P(\phi)$ are kept secretly.

The aim of the eavesdropping detection stage is to detect any eavesdropping strategies on the transmitted qubits. Similar to the BB84 protocol, Heisenberg uncertainty principle and quantum no-cloning theorem work now in this stage. To reach this aim, Alice compares Bob's results with her random qubit string R_q. If Bob's result is conclusive, Alice keeps the corresponding bits in R_c; otherwise, Alice aborts the corresponding bits. In detail, to retrieve available information, Eve should operate the qubits transmitted in the quantum channel from Alice to Bob. However, since $P(\psi)$ and $P(\phi)$ are not commutation, Eve cannot distinguish correctly the transmitted qubits $\{|\psi\rangle, |\phi\rangle\}$. According to the quantum no-cloning theorem Eve cannot copy exactly the transmitted qubits with a fidelity of $F = 1$. Therefore, the eavesdropper cannot attack the protocol like that in the classic scheme. In this scenario Eve may intercept the quantum channel. However, Heisenberg uncertainty principle prevents her from obtaining exact results. Essentially, the eavesdropping detections in the BB84 protocol and B92protocol are all based on the indistinguishability of qubits although the involved quantum sources are different. Therefore, the indistinguishability of qubits is one of important properties in guaranteing the security of QKD schemes.

The detection threshold depends on the employed approach. For example, in the Bennett's approach presented in Section 3.5.3, when Alice sends a qubit $|\psi\rangle$ or $|\phi\rangle$ to Bob through a quantum channel, Eve measures it using the basis $P(\psi)$. If the output vanishes, Bob judges the sent qubit to be $|\phi\rangle$, otherwise the transmitted qubit is $|\psi\rangle$. However, this measurement gives inevitably rise to a mistake probability

$$p_f = \{1 - \sin^2(2\theta)\}/2,$$

where θ is the overlapping angle between qubits $|\psi\rangle$ and $|\phi\rangle$. Apparently, the error probability $p_f > 50\%$. Consequently, in the whole procedure Eve's interception disturbs the quantum channel and generates a wrong result with probability 1/2. After Bob's measurement the final error probability resulted by Eve's interception is 1/2, i.e., $p_0^e = 50\%$. With this parameter Alice and Bob may detect eavesdropping: if the error probability p_f is more than the threshold p_0, i.e., $p_f \geq p_0^e$, legitimate communicators abandon this communication since Eve has obtained much more useful information on the transmitted qubits; otherwise Alice and Bob enter the following stage, i.e., the key distillation stage. At this point, the obtained key is usually called a raw key.

The remained stage is the so-called key distillation. Since this stage is the same as that in the BB84 protocol, it doesn't repeat here again.

4.3 Quantum Communication Model for QKD

In the previous section, the standard QKD schemes including the BB84 protocol and B92 protocol are described briefly. These schemes have revealed a common structure for the QKD procedure. That is, all proposed QKD schemes have a four-stage structure shown in Fig.4.1. One may find that the four-stage structure of the QKD procedure reveals clearly communication characteristics. Therefore, a QKD scheme can be regarded as a quantum communication system. This section describes characteristics of the QKD procedure from the viewpoint of communication.

By analogy with the Shannon communication model, a quantum communication model should involve a quantum source, quantum channel, and quantum sink. Of course, there are some differences between the quantum model and classic model due to the quantum nature. This leads the quantum information theory is different from the Shannon information theory. Fig.4.2 illustrates a special quantum communication model which is employed in QKD schemes. Different from the Shannon communication model, there is a quantum measurement channel and a classic assistant channel. What are the quantum measurement channel and assistant channel will be defined in the later in this section. Referring to the four-stage protocol shown in Fig.4.1, the quantum coding, quantum transmission, and eavesdropping detection are associated with the quantum source, quantum channel, and sink. In the following, dependence of QKD schemes on the quantum communication model as shown in Fig.4.2 is described.

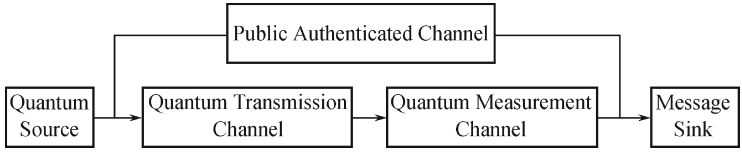

Fig. 4.2. Communication model for QKD

4.3.1 Quantum Source

A QKD scheme must associate with a certain quantum source in the quantum coding stage. For example, the involved quantum sources in the BB84 protocol and B92 protocol are $\mathcal{S}_{BB84} = \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and $\mathcal{S}_{B92} = \{|\psi\rangle, |\phi\rangle | \langle\psi|\phi\rangle \neq 0\}$, respectively. Since quantum symbols in these sources take

identical probabilities, they are expressed in simple ways as formulated in above. In general, however, the probability of each symbol is various. Hence, the quantum source used in the BB84 protocol may be precisely denoted as

$$\mathcal{S}_{BB84} = \begin{cases} |0\rangle, |1\rangle, |+\rangle, |-\rangle, \\ p_1,\ p_2,\ p_3,\ \ p_4, \end{cases} \tag{4.3.1}$$

where $p_j = 1/4$ with $j = 1, 2, 3, 4$.

Generally, a quantum source with discrete symbols is denoted

$$\mathcal{S}_d = \begin{cases} |\phi_1\rangle, |\phi_2\rangle, \ldots, |\phi_r\rangle, \ldots, |\phi_n\rangle, \\ p_1, \quad p_2, \ \ \ldots, \quad p_r, \ldots, p_n, \end{cases} \tag{4.3.2}$$

where $|\phi_r\rangle$ and p_r denote the rth quantum letter (or quantum symbol) and its probabilistic distribution, respectively, and $\sum_{j=1}^{n} p_j = 1$.

If the quantum source consists of continuous variables, it is expressed as,

$$\mathcal{S}_c = \begin{cases} |\omega\rangle, \\ p(\omega), \end{cases} \tag{4.3.3}$$

where $|\omega\rangle$ and $p(\omega)$ denote the quantum symbol and its probabilistic density, respectively, and $\int_{\infty} p(\omega)\mathrm{d}\omega = 1$.

In addition, if the quantum symbol in a quantum source is a mixed state, such a quantum source is denoted

$$\mathcal{S}_\rho = \begin{cases} \rho_1, \rho_2, \ldots, \rho_n, \\ p_1, p_2, \ldots, p_n, \end{cases} \tag{4.3.4}$$

where $\sum_{i=1}^{n} p_i = 1$ and ρ_i is the density matrix.

To design a secure QKD scheme is impossible without a suitable quantum source. Actually, main properties of a QKD scheme depend on the chosen quantum source. For instance, the B92 protocol depends on the nonorthogonality of quantum symbols in the quantum source. In addition, the quantum source partly influences the efficiency of a QKD scheme, e.g., the difference of quantum sources in BB84 protocol and B92 protocol leads different efficiency.

Next is to encode a secret random string using the chosen quantum source. This is called as the quantum source coding which is one of important components in the QKD procedure. Suppose that Alice chooses a secret random string,

$$\mathbf{s}_c = \{s_1, s_2, \ldots, s_n\}, \tag{4.3.5}$$

where s_i is the element of the random string. In principle, the random string may be any secret message denoted by an arbitrary P-ary number string. For convenience, however, the binary random string is always employed. In this case, $s_i \in \{0, 1\}$. According to the secret random string, Alice encodes each

bit into a qubit denoted using the quantum symbol from the chosen quantum source. Consequently, a random qubit-string is generated. Denote it using

$$\mathbf{s}_q = \{q_1, q_2, \ldots, q_n\}, \tag{4.3.6}$$

where q_i is a quantum symbol from the quantum source.

Usually, each qubit in the sequence $\mathbf{s}_q$ is regarded as an independent unit called qubit-unit, and each qubit-unit has no relationship since the sequence $\mathbf{s}_q$ is a truly random string. Of course, one may also divide the sequence $\mathbf{s}_q$ into m units or called blocks. Each unit or block in the generated sequence is transmitted from one communicator to others with a fix time-interval $\Delta\tau$ in the next stage.

4.3.2 Quantum Channel

The quantum transmission stage is associated with several channels including quantum channels and classic channels. Especially, the employed channels impact apparently efficiency and security of the QKD scheme. In the private communication, two kinds of channels, i.e., the perfect channel and imperfect channel, are always involved.

Definition 4.3.1 If there is no any information leakage to Eve, the channel is called a perfect channel. A perfect channel is also called a privacy channel.

Definition 4.3.2 In the message transmission, there are part information leak to Eve via the channel (classic channel or quantum channel), and Eve may change the transmitted message. However, Eve's information less than the total information. Such the kind of channels is called the imperfect channel.

In the classic private communication, only the one-time pad may be regarded as a perfect channel. Note, an imperfect channel does not mean an insecure channel. With some assistant tools, an imperfect channel may become a secure channel.

For a QKD scheme, Fig.4.2 illustrates that three kinds of channels have been involved, including the quantum transmission channel, quantum measurement channel and publicly authenticated channel. These channels have different characteristics so that they are used for various aims in the QKD procedure.

1) Quantum Transmission Channel

The so-called quantum transmission channel is a physical channel used for transmitting quantum signal from one communicator Alice to another communicator Bob. In a QKD system, the quantum transmission is an imperfect channel since the eavesdropper, i.e., Eve might obtain some useful information, and she may change the qubits transmitted in the channel.

To describe the quantum transmission channel one has to know the input random variables, output random variables and channel characteristics which are often expressed using a so-called channel matrix. Let ρ_{in} and ρ_{out} be the input and output qubits, respectively. In addition, let $\mathcal{E} = \{E_i | i = 1, 2, \ldots, n\}$ be a super-operator which expresses all possible operations from the transmission channel, including channel noise and environment influence. Then, one obtains

$$\mathcal{E}(\rho_{in}) \rightarrow \rho_{out}. \tag{4.3.7}$$

Consequently, the conditional probability of obtaining output ρ_{out}^j given input ρ_{in}^i reads

$$p(j|i) = Tr(\rho_{in}^i \mathbf{E}_j). \tag{4.3.8}$$

All conditional probabilities yield the channel matrix P,

$$P = \begin{pmatrix} p(1|1) & p(2|1) & \ldots & p(n|1) \\ p(1|2) & p(2|2) & \ldots & p(n|2) \\ \vdots & \vdots & & \vdots \\ p(1|n) & p(2|n) & \ldots & p(n|n) \end{pmatrix}. \tag{4.3.9}$$

Clearly, the channel matrix of the quantum transmission channel is similar to that of the Shannon channel. Accordingly, the mutual information and channel capability may be calculated using the Shannon information theory. Of course, the involved evolution of the qubit depends on the super-operator $\mathcal{E}$ which is different from the classic case.

2) Quantum Measurement Channel

A quantum measurement is associated with the input random variable, output random variable, and some measurement operations on the input random variable. Clearly, this procedure is the same as the transmission channel. Thus, an additional channel called quantum measurement channel is defined. That is, the quantum measurement procedure is regarded as a quantum channel. Consequently, the information theory may be used to solve the problems on quantum measurement operations.

Generally, the quantum measurement operation plays significant roles in quantum mechanics as well as quantum information science. For example, the quantum measurement is always employed to obtain available information by legitimate communicators. Also, it may be used for eavesdropping detection for the QKD scheme. Since a quantum measurement operation is equivalent to a quantum channels, i.e., the quantum measurement channel, one may solve the quantum measurement problems using information theory. To reach this aim, one has to build a channel model for the quantum measurement channel. Suppose that the qubit to be measured is ρ and the measurement operator is $\mathcal{M} = \{M_i | i = 1, 2, \ldots, n\}$. According to the measurement theory introduced in Chapter 3, one obtains the output probabilities,

$$p_m(j|i) = Tr(\rho_{out}^j M_i). \tag{4.3.10}$$

Then, the channel matrix for the quantum measurement channel reads

$$P_m = \begin{pmatrix} p_m(1|1) & p_m(2|1) & \dots & p_m(n|1) \\ p_m(1|2) & p_m(2|2) & \dots & p_m(n|2) \\ \vdots & \vdots & & \vdots \\ p_m(1|n) & p_m(2|n) & \dots & p_m(n|n) \end{pmatrix}. \tag{4.3.11}$$

As an example, the eavesdropping operation in B92 protocol may be regarded as a quantum measurement channel. In this case, Eve's operation gives rise to an error probability $p_e = 1 - \frac{\sin^2 2\theta}{2}$. This gives the channel matrix,

$$P_{B92} = \begin{pmatrix} p_e & 0 \\ 0 & 1 - p_e \end{pmatrix}. \tag{4.3.12}$$

It is similar to the binary symmetrical channel (BSC) in classic communication. In this case the mutual information is given by

$$I(A, E) = 1 - h(p_e), \tag{4.3.13}$$

where $h(p) = -p \log_2 p - (1-p) \log_2 (1-p)$.

Generally, let the input of the quantum measurement channel be ρ_s^i with a probability p_i and the measurement operator is $\mathcal{M} = \{M_i | i = 1, 2, \dots, n\}$, then the mutual information of the measurement channel is

$$I(\rho, \mathcal{M}) = \sum_{i=1}^{N} \sum_{j=1}^{N} p_i Tr \rho_s^i \mathbf{M}_j \log_2 \frac{Tr \rho_s^i \mathbf{M}_j}{\sum_{k=1}^{N} p_k Tr \rho_s^k \mathbf{M}_j}. \tag{4.3.14}$$

3) Public Classic Authenticated Channel

Making use of a quantum transmission channel, qubits might be transmitted from one communicator to another communicator. While using a quantum measurement channel the legitimate communicators may obtain available classic information and detect the eavesdropping operations which results in errors. However, one cannot obtain a perfectly secure key with only these channels. To reach a secure key one needs an assistant channel. Usually, this channel is a classic channel. Exactly, it is a publicly classic channel with authentication function. Clearly, this classic channel has two characteristics: publicness and authentication. The "publicness" means any participants in the communication system may access this communication channel, while the "authentication" specifies that any forger operations may be detected using authentication techniques which will be introduced in Chapter 6. Consequently, although Eve is allowed to access this channel but she cannot change the transmitted message.

There are many authentication approaches, but one has to note here the employed authentication scheme for the assistant channel should be unconditionally secure. This aim can be reached in both classic ways [25] and in quantum ways. The quantum authentication is described in Chapter 6.

4.3.3 Quantum Sink

A quantum sink is actually a receiver. It is similar to the classic sink. Since there is no quantum features we will not present detail discussion here.

4.4 Reconciliation

After having finished the quantum source coding stage, quantum transmission stage, and eavesdropping detection stage, a raw key is generated between Alice and Bob. However, the obtained raw key is imperfect since there are still error bits in the raw key string and information leakage to the eavesdropper called Eve. To correct these errors a so-called reconciliation technique is adopted. While to remove the influence of the information leakage on the security of the obtained key, Alice and Bob should use the privacy amplification technique. This section introduces the key reconciliation.

4.4.1 Reconciliation Model

Once the quantum transmission has been completed, the first task for Alice and Bob is to exchange their public messages enabling them to reconcile differences between their data. Suppose throughout that Eve listens to all of the public messages exchanged between Bob and Alice. This exchange must be performed in a way that reveals as little information as possible on these data. On the other hand, Eve cannot corrupt contents of these public messages.

The reconciliation is a technique needed to ensure both legitimate communicators' key elements are completely equal. The reconciliation may be either one-way or interactive. If the information is sent only from one legitimate communicator to another, the involved process is called an one-way reconciliation. Otherwise, if both legitimate communicators can exchange their information interactively, this process is called an interactive reconciliation. In the reconciliation procedure, there are some information should be disclosed. The criterion to optimize is the number of disclosed bits needed

to obtain the same string. In principle, only the one-way reconciliation is needed, but interactivity helps in quickly narrowing down errors to correct.

Mathematically, suppose that both legitimate communicators, i.e., Alice and Bob, hold random variables X and Y, respectively, the aim of the reconciliation is to obtain a common string Z via exchanging proper information. In practice, the random variables X, Y, Z may be discrete or continuous. For example, the obtained raw keys in the discrete-variable QKD and continuous-variable QKD [**?**, **?**] are discrete random variable and continuous random variable, respectively. Correspondingly, the discrete random variables are treated with binary reconciliation techniques, while the continuous random variables have to be deal with non-binary reconciliation techniques.

Generally, variables X and Y are independent, i.e., the communicators do not know their random variables each other. Without lost the generality, it usually assumes that the probability distribution of these variables, i.e., $P_{XY}(x, y)$, are known to all communicators. To prevent discovery of the most elements of the variable X, the random variable X should be transmitted in a secret way in the channel. Consequently, the coding techniques are always employed. For example, encoding X to be a code $\alpha(X)$, and sending it to the receiver, who knows the variable Y. Combing the received code $\alpha(X)$ and Y the receiver generates a new code $f(\alpha(X), Y)$ so that Alice and Bob may decode the new code and yield a common string Z with no error or an arbitrary smaller error probability. Clearly, this procedure is similar to some classic key-agreement protocols implemented with public key algorithms, such as the well-known RSA key-agreement protocol. Thus, one may also use a suitable classic public key cryptosystem (PKC) to implement the reconciliation. However, since all presented classic PKCs are not strictly proven to be secure, making use of the classic public key algorithms influences possibly the security of the considered QKD scheme.

In the QKD procedure, two kinds of reconciliation ways are possibly involved, they are the direct reconciliation and reverse reconciliation. In the former only Bob corrects the errors in his string and there are no changes in Alice's string, while the later uses a reverse way. Denote the information rates ΔI_{dr} and ΔI_{rr} for the direct reconciliation and reverse reconciliation, respectively, they are obtained respectively by

$$\Delta I_{dr} = I(A, B) - I(A, E), \tag{4.4.1}$$

and

$$\Delta I_{rr} = I(B, A) - I(B, E), \tag{4.4.2}$$

where $I(A, B) = I(B, A)$ denotes the mutual information between Alice and Bob, $I(A, E)$ is the mutual information between Alice and Eve, and $I(B, E)$ represents the information between Bob and Eve. Intuitively, the differences

between these two reconciliation ways are depicted in Fig.4.3. In this figure, the dashed arrows associated with $I(B, A)$ and $I(B, E)$ are refereed to the reverse reconciliation and the others correspond to the direct reconciliation.

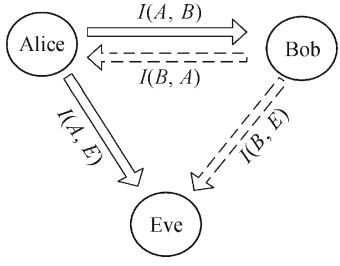

Fig. 4.3. Two Reconciliation ways for QKD scheme

4.4.2 Binary Reconciliation Protocol

To reconcile the key string, a novel protocol was proposed in 1992 by Bennett, Bessette, Brassard, Salvail, and Smolin [4]. Naturally, this protocol is called BBBSS scheme. With this protocol, Alice and Bob reconcile their data through public discussions, revealing to Eve no more information than she may have already discovered during the quantum transmission stage. The follows illustrate how to use the BBBSS protocol to perform the reconciliation for a binary string. This protocol executes the following steps.

Step 1: Alice and Bob agree on a randomly-chosen permutation operator P. Using this operator, Alice and Bob perform random permutations of the bit positions in their strings. This operation randomizes the locations of errors. The aim is to redistribute the locations of the errors.

Step 2: Alice and Bob partition the permuted strings into blocks of size k such that single blocks are believed to be unlikely to contain more than one error. Note, the optimal block size, which should be a function of the expected error rate, has not yet been determined theoretically. Consequently, it is always employed empirically in practices.

Step 3: For each block, Alice and Bob compare the block's parity. Blocks with matching parity are tentatively accepted as correct, while those of discordant parity are subject to a bisective search, disclosing $\log k$ further parities of sub-blocks, until the error is found and corrected. The operation is as follows.

Step 3.1: Alice and Bob exchange the parity of half of the block to generate two sub-blocks. If the parity is wrong, they go on with the bisective search in that half of the sub-block; otherwise, at least one error is present in the other half of the sub-block and the bisection focuses on that other half.

Step 3.2: The bisective search ends when an erroneous bit is enclosed.

Step 3.3: Knowing the position of this bit is enough for communicators to correct it, e.g., simply flipping it.

In the above procedure, in order to avoid leaking information to Eve, during the reconciliation process, Alice and Bob agree to discard the last bit of each block or sub-block whose parity they have disclosed. This reduces the efficiency but improves the security. Generally, with k iterations, the error probability becomes $p_e = 2^{-k}$. Clearly, when k becomes enough larger the error probability approaches zero.

Note, if the initial block size was much too large or too small, due to a bad priori guess of the error rate that fact will become apparent, and the procedure can be repeated with a more suitable block size. Alternatively, a small random sample of the bits could be compared initially in order to estimate the error rate, much like the quality control mechanism in the basic QKD protocol. Of course, these bits would then have to be sacrificed.

Based on the BBBSS algorithm, some improved algorithms for the binary reconciliation have been proposed, such as the Furukawa-Yamazaki algorithm [**?**], the Cascade algorithm [**?**], and the Winnow algorithm [**?**]. In addition, to correct the errors in Alice's and Bob's strings the error-correction code techniques are employed recently. The favor error-correction codes are Hamming code and LDPC. Details on these improved approaches with classic error-correction codes may be referred to Ref.[**?**].

4.4.3 Non-Binary Reconciliation Protocol

In the QKD scheme with continuous variables, the generated raw key strings consist of non-binary elements, and elements of these strings are not in a uniform distribution but instead of a Gaussian distribution. Mathematically, let Alice's raw key be a Gaussian variable $X \sim N(0, \Sigma^2)$ and Bob's raw key be $Y = X + \epsilon, \epsilon \sim N(0, \sigma^2)$, where the expression $\lambda \sim N(\mu, \sigma^2)$ denotes that the random variable λ follows a Gaussian probability distribution with average value μ and variance σ^2, respectively. Obviously, there are small differences between Alice and Bob's raw keys. This difference is produced by the noise distribution ϵ. To generate a common key, a reconciliation algorithm is also needed in this case. Since the variables X and Y are continuous variables, the reconciliation algorithms for binary bits are apparently not suitable. Thus, new approaches are necessary.

Generally, the non-binary reconciliation involves a two-step protocol. The first step is for the so-called interval partition. In this step, since X and Y are continuously Gaussian variables, they must be discretized to be n interval partition for the reconciliation process. After that, Alice encodes the interval, and tells Bob the rule of encoding. The second step is for the slice estimation. According to the reconciliation information received from Alice, Bob distills some information. After these two steps, Alice and Bob share

two long bit sequences. The errors in these two sequences can be corrected through the algorithm used in the binary reconciliation algorithm. Obviously, the key problems are how to partition the interval and how to perform the slice estimation. After these procedures, the remained parts are the same as that for the binary reconciliation.

1) Principle of Non-binary Reconciliation

Before presenting the interval partition and slice estimation approaches, we describe briefly the principle of the non-binary reconciliation. Suppose that Alice sends L copies of x to Bob, then the average information carried by x is

$$H(K(X)) - I(K(X), E) - (|C|/L),$$

where $I(K(X), E)$ represents the information eavesdropped by Eve. It will be wiped out using the privacy amplification technique, which will be described in next section. In the non-binary reconciliation algorithm, the objective is to minimize $I(K(X), E) + (|C|/L)$ so that a single symbol may carry more information. Since the minimum of $|C|$ is $LH(K(X)|Y)$ [**?**], the maximum of $H(K(X)) - (|C|/L)$ is $I(K(X), Y)$.

In the information reconciliation process of the continuous QKD, one should find a good way to partition the interval so that $I(K(X), Y)$ can approach the maximum $I(X, Y)$. It has been shown that the sufficient and necessary condition [**?**] is

$$\alpha(x) = \arg \min_{z=1}^{N} D(p(Y|X = x) \| (p(Y|Z = z), \tag{4.4.3}$$

where $D(q(x)\|(t(x))$ denotes the relative entropy of $q(x)$ and $t(x)$ which describes the similarity of them. The relative entropy for continuous variable x is defined as

$$D(q(x)\|(t(x)) = \int_{-\infty}^{+\infty} p(x) \log \frac{q(x)}{t(x)} \mathrm{d}x. \tag{4.4.4}$$

Above equation shows that computing the relative entropy is very difficult, but there is a special case, i.e., computation of the relative entropy of a Gaussian Function with respect to another Gaussian Function is very easy. As an example, let A and B be two random variables $A \sim N(\mu_1, \sigma_1^2)$ and $B \sim N(\mu_2, \sigma_2^2)$ and their probability density functions be $p_a(x)$ and $q_b(x)$, respectively. Since $p_a(x)$ and $q_b(x)$ are Gaussian distributions, Eq.(4.4.4) gives the relative entropy among them,

$$D(p_a(x)\|q_b(x)) = \ln \frac{\sigma_2}{\sigma_1} - \frac{1}{2} + \frac{\sigma_1^2 + (\mu_1 - \mu_2)^2}{2\sigma_2^2}. \tag{4.4.5}$$

2) Interval Partition

Generally, one cannot retrieve the optimal interval partition through single computation. Consequently, an iterative computation is necessary so that the maximum $I(X,Y)$ can be reached. An iterative algorithm has been investigated theoretically in Ref.[**?**], it executes as follows,

Step 1: Random choose N intervals $Q_k(1 \leq k \leq N)$.

Step 2: Compute the average conditional probability density of each interval using $f_k = E(p(x'|X)|X \in Q_k)$ with $k = 1, 2, \ldots, N$.

Step 3: If x satisfies the following condition: $D(p(x'|X = x)\|f_j) > D(p(x'|X = x)\|f_k)$ with $j \neq k$ and $k, j = 1, 2, \ldots, N$, then one has $x \in Q_k$.

Step 4: Continue the steps above until the iterations reach a convergence.

In the above algorithm one has to compute a multiple integral for each iterations calculation. This costs many computational resources for computing the relative entropy in engineering application, consequently, leads a very lower efficiency for the secret key rate of QKD scheme. In order to simplify the computation of the relative entropy, one may construct a Gaussian distribution with the same numerical character to replace the non-Gaussian distribution, and use properties of the relative entropy of the Gaussian distribution to compute the separation of the adjoining interval.

Consider a random variable V with the Gaussian distribution, then the conditional probability distribution is given by

$$p_v(x) = p(x'|X = x) = \frac{1}{\sqrt{2\pi}\sigma} \exp\left(\frac{(x' - x)^2}{2\sigma^2}\right). \tag{4.4.6}$$

The average conditional probability density function in the interval $Q_k = \{x|a \leq x \leq b\}$ is obtained by

$$q_v(x) = p(x'|Z = z) = \int_b^a p(X = x)p(x'|X = x)\mathrm{d}x, \tag{4.4.7}$$

where $z \in [a, b]$. Clearly, the average conditional probability density function $q_v(x)$ is a non-Gaussian distribution. Consequently the relative entropy of $p_v(x)$ respect to $q_v(x)$ is difficult to compute. To simplify the computation procedure, a random variable W with a Gaussian distribution $q_w(x) \sim N(E(q_v(x)), Var(q_v(x))$ which has the same numerical characters with $q_v(x)$ is constructed, where $E(\cdot)$ and $Var(\cdot)$ denote the mathematical expectation and variance of $q_v(x)$, respectively, they are given by

$$E(q_v(x)) = \int_{-\infty}^{+\infty} x' q_v(x')\mathrm{d}x',$$

and

$$Var(q_v(x)) = \int_{-\infty}^{+\infty} [x' - E(q_v(x'))]^2 q_v(x')\mathrm{d}x'.$$

Then one obtains

$$D(p_v(x)\|q_v(x)) \approx D(p_v(x)\|q_w(x)). \tag{4.4.8}$$

Suppose that b is the boundary of adjoining intervals $[a, b]$ and $[b, c]$. After the iteration computation reaches a convergence, one obtains

$$\begin{aligned} & D(p_v(x)\|q_w(x), x \in K = [a, b]) \\ & \quad = D(p_v(x)\|q_w(x), x \in K + 1 = [b, c]) \\ & \quad = \frac{1}{2}\ln\frac{\xi^2}{\sigma^2} + \frac{\sigma^2 + [b - \int_b^c xp(X = x)\mathrm{d}x]^2}{2\xi}. \end{aligned} \tag{4.4.9}$$

where $\xi = \{\sigma^2 + [\int_b^c xp(X = x)\mathrm{d}x]^2\}\int_b^c p(X = x)\mathrm{d}x + 2[\int_b^c xp(X = x)\mathrm{d}x]^2 + \int_b^c x^2 p(X = x)\mathrm{d}x$. Clearly, the computation has been simplified according to Eq.(4.4.9) since there is no multiple integrals again. The improved algorithm executes the following steps.

Partitioning the interval $(-\infty, \infty)$ into 2^m parts. Since the random variable X follows a Gaussian distribution, its values reach 99.7% in the interval $(-3\Sigma \le x \le +3\Sigma)$. Accordingly, only this interval needs to be considered mainly. Choose $Q_1 = \{x| - \infty < x < -3\Sigma\}$ and $Q_N = \{x| + 3\Sigma < x < +\infty\}$. The iteration algorithm executes the following steps.

Step 1: Suppose $j = 1$, $a_1 = -3\Sigma, a_{N-1} = 3\Sigma$ and from a_2 to a_{N-2} evenly partition the interval.

Step 2: If $j < N_1$, take a_j, a_{j+2} into Eq.(4.4.9) and calculate the boundary a_{j+1}.

Step 3: Let $j = j + 1$.

Step 4: After one circulation, reset $j = 1$ and return to Step 2.

3) Bit Estimation

After finishing the interval partition, one may use a so-called bit estimation function to achieve a discrete bit sequence. The details of the bit estimation function are as follows.

Step 1: Suppose that the considered interval $[a, b]$ is divided into 2^m subintervals. Then, encode these subintervals making use of 2^m binary-bit strings arranged from $00\ldots0$ to $11\ldots1$. Accordingly, when Alice sends $x \in [a, b]$ to Bob, it can be decoded into a bit sequence $[(S_m(x), S_{m-1}(x), \ldots, S_1(x)]$.

Step 2: Bob estimates which interval does the x belong to according to the x' he received and the information reconciliation exchanged through the authenticated channel. The information exchanged is the lower j bits of the sequence $[(S_m(x), S(m-1(x), \ldots, S_1(x)]$. Bob uses the following process to guess the higher $m - j$ bits. S2.1: $i = j$; S2.2: $b = S_{i,i-1,\ldots,1}(x)$; S2.3: $S'_{i+1}(x) = S(x', b)$; S2.4: $S_{i+1}(x) = S'_{i+1}(x)$; S2.5: $i = i + 1$; S2.6: If $i \le m-1$ return to S2, otherwise, go to S2.7; S2.7: Bob gets the higher $m-j$ bits $[(S'_m(x), S'_{m-1}(x), \ldots, S'_{j+1}(x)]$.

Step 3: After Alice and Bob process n realizations of the continuous variable, they obtain $(m - j)n$ bits. These bits form the discrete random variable X and Y for Alice and Bob, respectively. Then one can implement the error correction like that in the scenario for binary bits.

In the above algorithm, the ith bit's estimator is as follows,

$$S_i'(x', b) = \arg\max_s Pr[S_i(X) = s | S_{i-1,\ldots,1}(X) = b, X' = x'], \tag{4.4.10}$$

where $s \in \{0, 1\}$. In Eq.(4.4.10) the inputs $s = 0$ and $s = 1$ yield two different output probabilities. Here we are interested in the larger one. For example, if the input $s = 0$ yields the larger probability, the ith bit is encoded into 0, otherwise the ith bit is bit 1. Since

$$\begin{aligned} &Pr[S_i(X) = s | S_{i-1,\ldots,1}(X) = b, X' = x'] \\ &\quad = \frac{Pr[S_i(X) = s, S_{i-1,\ldots,1}(X) = b, X' = x']}{Pr[S_{i-1,\ldots,1}(X) = b, X' = x']}, \end{aligned} \tag{4.4.11}$$

Bob can guess the ith bit through the lower $i-1$ bits $S_{i-1,\ldots,1}(X) = b$. Subsequently, Bob can guess all the bits.

As an example, suppose there are m bits. Alice partitions the interval into 2^m parts. If one knows the lower $i-1$ bits, there are 2^{m-i+1} subintervals meet the requirement. Using $Pr[S_{i-1,\ldots,1}(X) = b, X' = x']$ to represent the sum of the probabilities from these subintervals to $X' = x'$, then,

1) If $s = 0$, 2^{m-i} subintervals from all 2^{m-i} subintervals are obtained. Substituting $s = 0$ into Eq.(4.4.11) one obtains the probability $p(0)$. If substituting $s = 1$ into Eq.(4.4.11), one may obtain $p(1)$. When $p(1) < p(0)$, the ith bit is regarded as bit 0; otherwise, the ith bit is regarded as bit 1.

2) All computations can be modeled as the probability calculation from one interval to a point. The denominator in Eq.(4.4.11) is the sum of these probabilities. One may easily know that this probability is 0. Thus, the formula in Eq.(4.4.11) obeys the Law of L'Hospital, consequently, this formula can be simplified and an estimation function is obtained. If the estimation function can be used instead of the Law of L'Hospital, the efficiency could be increased.

3) The difficulty of Eq.(4.4.11) is finding an estimation function to replace for the complex computation of the planar Gaussian distribution.

If one uses margin probability density function $p(x)$ and $p(x')$ to compute the joint probability density function $p(x, x')$ and then use it to compute the probability of the model, the condition is complex. Followings are two easier ways to compute the probability from the interval to the point.

Since $p(x, x')$ is very complex, one may compute the joint probability density function $p(x, n)$ as an alternative. Suppose the random variable $X \sim N(0, \Sigma^2)$, the interesting interval is $[a, b]$. Since X and N are individual, $X' = X + N \sim N(0, \Sigma^2 + \sigma^2)$. Suppose the interval of X' is $\left[x' - \frac{dx'}{2}, x' + \frac{dx'}{2}\right]$, then the interval of $N = X' - X$ is $\left[x' - \frac{dx'}{2} - x, x' + \frac{dx'}{2} - x\right]$. Combining these gives

$$p(x, n) = p(x)p(n) = \frac{1}{\sqrt{2\pi}\Sigma} \exp\left(-\frac{x^2}{2\Sigma^2}\right) \times \frac{1}{\sqrt{2\pi}\sigma} \exp\left(-\frac{x^2}{2\sigma^2}\right) \tag{4.4.12}$$

Thus, the joint probability density function of X and X' is

$$p(X,X') = \int_a^b \int_{x'-dx'/2}^{x'+dx'/2} p(x,x')\mathrm{d}x\mathrm{d}x' = \int_a^b \int_{x'-dx'/2-x}^{x'+dx'/2-x} p(x,n)\mathrm{d}x\mathrm{d}n. \tag{4.4.13}$$

Substituting Eq.(4.4.12) into Eq.(4.4.13) yields,

$$p(X,X') = \int_a^b p(x) \int_{x'-dx'/2-x}^{x'+dx'/2-x} p(n)\mathrm{d}x\mathrm{d}n. \tag{4.4.14}$$

Then a bit of complex computation yields finally the probability from the interval $[a,b]$ to the point x' as follows,

$$\begin{aligned} p(a \le X \le b, x') &= p(a \le X \le b, x')/dx' \\ &= \frac{1}{2\pi\sigma\Sigma} \int_a^b \exp\left(-\frac{x^2}{2\Sigma^2} - \frac{(x'-x)^2}{2\sigma^2}\right)\mathrm{d}x. \end{aligned} \tag{4.4.15}$$

Now consider an alternative ways. Since the source is a Gaussian distribution and the channel is AWGN. When $X = x$, the probability of X and the conditional probability density function of random variable X' given X are respectively,

$$p(X = x) = \frac{1}{\sqrt{2\pi}\Sigma} \exp(-\frac{x^2}{2\Sigma^2}), \tag{4.4.16}$$

and

$$p(x'|X = x) = \frac{1}{\sqrt{2\pi}\sigma} \exp\left(-\frac{(x'-x)^2}{2\sigma^2}\right). \tag{4.4.17}$$

With condition $X \sim N(0,\Sigma^2)$, the average conditional probability is

$$\begin{aligned} \int_a^b p(X = x)p(x'|X = x)\mathrm{d}x &= \frac{1}{2\pi\sigma\Sigma} \int_a^b \exp\left(-\frac{x^2}{2\Sigma^2} - \frac{(x'-x)^2}{2\sigma^2}\right)\mathrm{d}x \\ &= p(a \le X \le b, x'). \end{aligned} \tag{4.4.18}$$

Therefore, the physical meaning of the estimation function is the average probability density from the interval $[a,b]$ to the point x'.

4.5 Privacy Amplification

Through k iterations computation in the reconciliation process, Alice and Bob's raw keys are identical or at least to be equivalent with an arbitrary smaller error probability $p_e = 2^{-k}$ which depends on the parameter k. However, the common key between Alice and Bob is still partly secret since Eve knows some bits. This, obviously, influences the security of the final key. To

create a key with unconditionally secure the privacy amplification technique is adopted in the QKD scheme for amplifying the security of the key. The so-called privacy amplification is actually a kind of distillation techniques. In Section 4.1 an intuition on this technique is presented, here a further description on the privacy amplification is presented.

4.5.1 Privacy Amplification Principle

Definition 4.5.1 If there is a few information leakages to the illegitimate participant in a private communication system, the exchange string must be partly secret. Consequently, the privacy of the exchanged string is debased. The technique of enhancing the privacy of the random string is called privacy amplification. Exactly, the privacy amplification is a distillation technique which compresses a long random number string to a shorter one so that the privacy of random string is amplified.

The privacy amplification is a necessary part for the QKD scheme to obtain secure keys. This notation was proposed in 1995 by Bennett and his coworkers [**?**]. Let Alice and Bob share a common key $\tilde{K}$ which is obtained from the raw key using reconciliation technique. After the privacy amplification process Eve's information is reduced exponentially. This conclusion is exactly illustrated in the following theorem.

Theorem 4.5.1 Let $S \in \{0,1\}^n$ and $Z \in \{0,1\}^r$ be two random variables, where S has a probability distribution $p(s)$, and Z is jointly distributed with S according to $p(s,z)$, n and r denote the length of the variables S and Z, respectively. Let G be the random variable corresponding to the random choice (with uniform distribution) of a member of the universal class $\mathscr{G}_h(S)$ of hash functions from S to $K \in \{0,1\}^{n-r}$, where $K = G(S)$. If Eve's collision entropy on S satisfies $H_c(S|Z=z) \leq c$, then

$$H(K|G,Z=z) \geq s - \log_2(1+2^{s-c}) \geq \frac{s-2^{s-c}}{\ln 2}, \tag{4.5.1}$$

where $s = n - r$.

From the above theorem, one may calculate the information of what Eve obtains on the final key K,

$$H(K) - H(K|G,Z=z) \leq \frac{2^{s-c}}{\ln 2}. \tag{4.5.2}$$

Clearly, when s is arbitrary shorter, Eve's information on the final key K tends to be vanished.

There is a key notation—universal hash function, which is different from hash functions usually employed in the classic cryptographic scheme. Actually, the privacy amplification mainly depends on the universal hash function. In theoretical, one has the following result for the universal hash function.

Theorem 4.5.2 Let S be a random variable on an alphabet $\mathcal{S}$ with the probability distribution $p(s)$ and collision entropy $H_c(S)$, and let G be a random variable corresponding to the random choice (with uniform distribution) of a member of the universal class $\mathscr{G}_h(S)$ of hash functions from S to $\{0,1\}^m$. Then

$$H(G(S)|G) \geq H_c(G(x)|G) \geq m - 2^{m-H_c(S)}. \tag{4.5.3}$$

This theorem illustrates the uncertainty of choosing hash functions.

4.5.2 Privacy Amplification Techniques

As mentioned in above the key technique for the privacy amplification relies on choice of universal hash function. In the follows several examples for the universal class of hash functions are illustrated [**?**].

Example 1 An intuition way has been proposed in the original scheme, i.e., the BB84 protocol. In this case, Alice randomly chooses pair of bits and computes their XOR value. But, in contrast to error correction, she does not announce this XOR value. She only announces which bits she chose (e.g., bits number 103 and 537). Alice and Bob then replace two bits by their XOR value. In this way, they shorten their key while keeping it error free, but if Eve has only partial information on the two bits, her information on the XOR value is even less. Assume, for example, that Eve knows only the value of the first bit and nothing about the second one. Then she has no information at all about the XOR value. Also, if Eve knows the value of both bits with 60% probability, then the probability that she correctly guesses the XOR value is only $0.6^2 + 0.4^2 = 52\%$. This process would have to be repeated several times.

Example 2 Let $\mathscr{A} = GF(2)^l$ and $\mathscr{B} = GF(2)^k$. For M, a $k \times l$ binary matrix, let $h_M(x) = Mx$ be the product of M with the column vector x. Then $\mathscr{H}_3 = \{h_M : M \in GF(2)^{k\times l}\}$ is universal.

In this example, there are kl bits in the employed matrix M which is actually the universal class of hash functions. If the element bits of the matrix M need to be transmitted, this example is not acceptable since the cost of transmitting element bits is too much. Thus a special matrix, e.g., Toeplitz matrix which has characteristics of $M_{i,j} = M_{i+\delta,j+\delta}$ for any $i, j, \delta \in \mathbb{N}$ such that $1 \leq i, i+\delta \leq k$ and $1 \leq j, j+\delta \leq l$, should be chosen. However, if Alice and Bob have pre-chosen the universal hash function class $\mathscr{H}_3$ through the public classic authenticated channel, they do not need to transmit the element bits. For instance, Alice and Bob choose a permutation P_h like that in the BBBSS algorithm for reconciliation, and permute randomly positions of each matrix in $\mathscr{H}_3$. Then Alice tells Bob the location of the chosen hash function. Using the corresponding matrix Alice and Bob may perform the privacy amplification process.

Example 3 Let $\mathscr{A} = GF(2^l)$ and $\mathscr{B} = \{0,1\}^k$. Let $h_c(x)$ be defined as the first k bits of the product cx in a polynomial representation of $GF(2^l)$. The set $\mathscr{H}_{\mathscr{A}\to\mathscr{B}} = \{h_c : c \in GF(2^l)\}$ is a universal class of hash functions.

4.6 Security Model for QKD

The security is an important issue in the classic private communication as well as quantum private communication. A security model for quantum private communication has been presented in Chapter 2. This section further describes the security issues focused on the QKD. As mentioned previously, the quantum coding, quantum transmission, eavesdropping detection, reconciliation, and privacy amplification are necessary techniques for obtaining secure key via quantum ways, but only these core techniques cannot guarantee the security of the generated key since a suitable condition for yielding secure key is required. In this section, some security conditions for QKD are presented. Firstly, a general proof for proving unconditional security of QKD which was presented by Mayer in Ref.[19] is introduced. Following this security proof a criterion for the security judgement of the QKD schemes is presented. Then, some typical attack strategies are introduced.

4.6.1 Security Theory

Since the BB84 protocol was presented, the security of the QKD scheme has attracted much attention. Here three kinds of security proofs are described. They are often employed to judge the security condition for the QKD scheme.

1) Security Criteria

In theory, the goal of an ideal QKD scheme is to allow two participants, Alice and Bob, who share no information initially to share a secret key (a string of bits) at the end. A third participant, usually called Eve, should not be able to obtain any information about the key. Also, whatever Eve does, Alice's and Bob's key should be identical. It is assumed that all quantum communications between Alice and Bob passes through Eve, and similarly for the classical communication.

In reality, however, one cannot realize this ideal task. There are few subtle points to consider. First, no QKD protocol can succeed if Eve has the power to impersonate Alice while communicating with Bob and to impersonate Bob while communicating with Alice unless the authentication techniques is employed. Cryptographically, this kind of attacks is called the Man-in-the-middle attack. To prevent such attack strategy, an initial authenticated key is necessary. Subsequently, the protocol implements essentially the key expansion rather than the key distribution. In a scenario where Alice and

Bob have never exchanged a secret key before, one must assume that Alice and Bob have access to a faithful (classical) public channel so that a third party cannot accomplish the impersonation attack without being detected. Another related point is that a secret key is not always shared between Alice and Bob because it is always possible for a third party to jam the quantum channel. This involves the so-called Man-in-the-middle attack.

Consequently, Mayer believed that the QKD scheme is theoretical impossibilities in the key distribution [19]. Its security is based on the assumption of above two points. According to these restrictions Mayer gave a *security Criterium* for the QKD scheme. In the QKD schemes, and ideally in other applications of the quantum cryptography, a security result is expected to hold against all attacks allowed by quantum mechanics. This is what is called an unconditional security, and this is what all authors have proven.

2) Proofs for Unconditionally Secure QKD Schemes

By defining a ϵ-private, a proof of guaranteeing the unconditional security of any QKD scheme was presented. Mayer believed if a QKD protocol is ϵ-private then it is unconditionally secure. The ϵ-private is defined as follows.

Definition 4.6.1 Let K, M, and V be random variables of a key, key length, and Eve's any strategy on a QKD scheme, respectively. Consider any number $\epsilon > 0$, a QKD protocol $\mathfrak{P}$ is ϵ-private if, for every strategy adopted by Eve,

$$\sum_m p(m)(m - H_m(K|V)) \leq \epsilon, \tag{4.6.1}$$

where $p(m)$ is the probability of $M = m$ and

$$H_m(K|V) = -\sum_v \sum_{k \in \{0,1\}^m} p(k, v|m) \log_2 p(k|v).$$

The equality in Eq.(4.6.1) exists when the number $\epsilon = \epsilon_0$, where ϵ_0 is the upper bound of ϵ.

Using the ϵ-private definition, a judgement for unconditionally secure QKD protocol has been presented. It is demonstrated in the following theorem.

Theorem 4.6.1 Let $\delta > 0$ be the tolerated error rate and $p_T > 0$ be the probability that any given position $i \in \Omega$ is tested, that is, δ and p_T are the parameters satisfied $d_T \geq \delta p_T n_\Omega$. Let $p_E = 1 - p_T$. Let $\varepsilon > 0$ and $\tau > 0$ be the fixed parameters satisfied $H^{-1}(1 - (r + m)/n_E - \tau)n_E \geq 2d_+(\varepsilon)$, where $\varepsilon > 0$ and $\tau > 0$ are any positive values fixed in the protocol and $H(x)$ is the entropy. Let $n_E^{min}, n_\Omega^{min}$ be the lower bounds and m^{max} be the upper bound, i.e., $n_E \geq n_E^{min}, n_\Omega \geq n_\Omega^{min}$ and $m \leq m^{max}$. Let μ be the following function of these parameters

$$\mu = \exp\left(\frac{-\varepsilon^2 \min\{p_T^2, p_E^2\}}{2\delta + \varepsilon} n_\Omega^{min} + \frac{2\varepsilon^2 p_E^2}{(2\delta + \varepsilon)^2}\right) \tag{4.6.2}$$

Let $\gamma = \sqrt{\mu}, \eta = 2\sqrt{\gamma}+\gamma, \lambda = 2^{-\tau n_E^{min}}, \xi = \gamma+\lambda+\eta+2\sqrt{2\eta}$ and $\sigma = \eta+\sqrt{2\eta}$. The protocol is ϵ-private where $\epsilon = \sigma/\ln 2 + m^{max}\xi$.

The used symbols in the above theorem are defined in same way as that in Ref.[**?**]. This privacy result provides a bound on the amount of information that Eve can obtain about the final key. This bound holds as long as the length of the key is set by Alice and Bob in accordance with the validation constraints.

In a simple way, a proof for an unconditional security QKD scheme has been presented in Ref.[**?**]. In this case, both the mutual information between Alice and Bob and mutual information between one of communicators and the eavesdropper are involved. According to the above security theory, the necessary condition for obtaining a secure QKD scheme is given. Define a useful notation, i.e., the private degree $\mathcal{P}$ of a QKD scheme. Mathematically, the private degree is defined as follows,

$$\mathcal{P}_d = \sup\left[\frac{I(\alpha,\beta) - I(\alpha,\epsilon)}{I(\alpha,\beta)}\right] \tag{4.6.3}$$

for direct reconciliation, or

$$\mathcal{P}_r = \sup\left[\frac{I(\beta,\alpha) - I(\beta,\epsilon)}{I(\beta,\alpha)}\right] \tag{4.6.4}$$

for the reverse reconciliation, where $I(\alpha,\beta)$, $I(\alpha,\epsilon)$, and $I(\beta,\epsilon)$ denote the average mutual information between Alice and Bob, Alice and Eve, and Bob and Eve, respectively. Note here, $I(\alpha,\beta) = I(\beta,\alpha)$.

Clearly, $|\mathcal{P}| \leq 1$. If $\mathcal{P} = 1$ the protocol is perfect privacy since in this case Eve cannot obtain any information, i.e., $I(A,E) = 0$. If $\mathcal{P} > 0$ the protocol may reach perfect privacy with the reconciliation and privacy amplification techniques. For the other cases, i.e., $\mathcal{P} < 0$, the protocol is insecure even if with the reconciliation and privacy amplification technique. There is a special case with $\mathcal{P} = 0$, in this situation one cannot judge whether the protocol is secure or not.

More precisely, the above results may be described using the Csiszar-Körner Theorem [**?**], which was first migrated to quantum cryptography by Maurer in 1993 [**?**]. This theorem has become an important security judgement criterion for finding the security condition of a given QKD scheme.

Theorem 4.6.2 Given a QKD scheme $\mathfrak{P}$, with the reconciliation and privacy amplification technique, the necessary condition of $\mathfrak{P}$ being secure is

$$max\{I(\alpha,\beta) - I(\alpha,\epsilon), I(\beta,\alpha) - I(\beta,\epsilon)\} > 0, \tag{4.6.5}$$

where the first expression corresponds to the direct reconciliation, and the second corresponds to the reverse Reconciliation.

4.6.2 Typical Attack Strategies

Under quantum attacks the QKD has been proven to be unconditionally secure. In reality, however, a QKD system should be against not only quantum attacks but also classic attacks since any drawback regarding security will impair the communicators' benefits. Thus, from the viewpoint of application, all attack strategies for key generation and distribution in classic cryptography is suitable for the QKD scheme. Here some typical attack strategies on QKD scheme are introduced.

Commonly, the quantum attack include the individual attack, joint attack, and collective attack. The individual attack is an incoherent attack strategy, while the joint attack and the collective attack are coherent attack strategies. In detail, if the attacker attaches independent probes to each qubit and measures him probes one after the other. This class of attacks is called the *individual attack*, or incoherent attack. Individual attacks have the nice feature that the problem can be entirely translated into a classical one: Alice, Bob, and Eve all have classical information in the form of random variables A, B, and E, respectively, and the laws of quantum mechanics impose constraints on the joint probability distribution $P(a, b, e)$. The classical scenarios have been widely studied by the classical cryptology community, and many of their results can thus be directly applied.

Two other classes of eavesdropping strategies let Eve process several qubits coherently, hence the name coherent attacks. The most general coherent attacks are called *joint attacks*, while an intermediate class assumes that Eve attaches one probe per qubit, as in individual attacks, but can measure several probes coherently, as in coherent attacks. This intermediate class is called the *collective attack*. It is not known whether this class is less efficient than the most general class, that of joint attacks. It is also not known whether it is more efficient than the simpler individual attacks. Actually, it is not even known whether joint attacks are more efficient than individual ones. For joint and collective attacks, the usual assumption is that Eve measures her probe only after Alice and Bob have completed all public discussion about basis reconciliation, error correction, and privacy amplification. For the more realistic individual attacks, one assumes that Eve waits only until the basis reconciliation phase of the public discussion. The motivation for this assumption is that one hardly sees what Eve could gain by waiting until after the public discussion on error correction and privacy amplification before measuring her probes, since she is going to measure them independently anyway.

Except for the quantum attack, there are many strategies come from the classic attack on a practical QKD system. Typically, two strategies are introduced in the follows. These strategies are the Man-in-the-middle attack strategy and Trojan horse attack strategy. Since the Trojan horse attack strategy has been introduced in Chapter 2, only the Man-in-the-middle attack strategy is focused here. In cryptography, the Man-in-the-middle attack or called bucket-brigade attack, sometimes Janus attack, is a form of active

eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all messages going between the two victims and inject new ones, which is straightforward in many circumstances. A Man-in-the-middle attack can only be successful when the attacker can impersonate each endpoint to the satisfaction of the other. Most cryptographic protocols include some form of endpoint authentication specifically to prevent Man-in-the-middle attacks. For example, the secure sockets layer (SSL) authenticates the server using a mutually trusted certification authority. To prevent such attack, the authentication technique should be employed. It has been demonstrated that unconditionally secure authentication is possible in classic cryptography [25].

Except for the quantum attacks and classic attacks, there is a special kind of attacks which is arisen from drawback of technique implementation. This attack is called as photon-number splitting (PNS) attack, it is occurred in the discrete-variable QKD system. Generally, a discrete-variable QKD scheme requires the transmitter Alice sends quantum states to Bob using single photon signals. In practices, however, many implementations use laser pulses attenuated to a very low level to send the quantum states (refer to Chapter 7). These laser pulses contain a very small number of photons, for example 0.2 photons per pulse for average, which are distributed according to a Poissonian distribution. This means most pulses actually contain no photons (empty pulse), some pulses contain 1 photon (which is desired) and a few pulses contain 2 or more photons. If the pulse contains more than one photon, then Eve can split off the extra photons and transmit the remaining photons to Bob. This is the basis of the PNS attack [**?**], where Eve stores these extra photons in a quantum memory until Bob detects the remaining single photon and Alice reveals the encoding basis. Eve can then measure her photons in the correct basis and obtain information on the key without introducing detectable errors.

To prevent this attack, a straightforward strategy is to create a true single photon source instead of an attenuated laser. Although this technique is not matured for practical application, but it has quickly made progress. Another solution is to modify the original protocol into a new one which can be against this attack. For example, the SARG04 protocol is such a scheme based on the BB84 protocol [**?**], in which the secure key rate scales as $r^{3/2}$. The most promising solution is the decoy state approach [**?**, **?**], in which Alice randomly sends some of laser pulses with a lower average photon number. These decoy states can be used to detect a PNS attack, as Eve has no way to tell which pulses are signal and which decoy. Using this approach the secure key rate scales as r, the same as for a single photon source. This approach has been implemented successfully in several QKD experiments, allowing for high key rates secure against all known attacks [**?**].

References

[1] Bennett C H, Brassard G (1984) An update on quantum cryptography. Advances in Cryptology-Proceedings of Crypto 84, Barbara, Springer, pp 475 – 480

[2] Bennett C H (1992) Quantum cryptography using any two non-orthogonal states. Physical Review Letters, 68: 3121 – 3124

[3] Ekert A K (1991) Quantum cryptography bases on Bell's theorem. Physical Review Letters, 67: 661 – 664

[4] Bennett C H, Bessette F, Brassard G, el al (1992) Experimental quantum cryptography. Journal of Cryptology, 5: 3 – 28

[5] Goldenberg L, Vaidman L (1995) Quantum cryptography based on orthogonal states. Physical Review Letters, 75: 1239 – 1243

[6] Koashi M, Imoto N (1997) Quantum cryptography based on split transmission of one-bit information in two steps. Physical Review Letters, 79: 2383 – 2386

[7] Bechmann-Pasquinucci H, Peres A (2000) Quantum cryptography with 3-state systems. Physical Review Letters, 85: 3313 – 3316

[8] Bruß D (1998) Optimal eavesdropping in quantum cryptography with six states. Physical Review Letters, 87: 3018 – 3021

[9] Zeng G H, Wang Z Y, Zhu H W (2000) Quantum key distribution scheme with 100% efficiency. The 5th interaction conference on quantum communication, measurement and computing, Capri, 3 – 8 July 2000, pp 2 – 8

[10] Gisin N, Ribordy G, Tittel W, et al (2002) Quantum cryptography. Reviews of Modern Physics, 74: 145 – 195

[11] Brassard G, Salvail L (1994) Secret-key reconciliation by public discussion. Advances in Cryptology: Eurocrypt 93, Lofthus, Norway, May 23 – 27, 1993. Helleseth T (ed) Lecture Notes in Computer Science (LNCS). Springer, Heidelberg, pp 441 – 423

[12] Yamazaki K, Sugimoto T (2000) On secret key reconciliation protocol. Proceedings IEEE International Symposium on Information Theory and its Applications, Honolulu. 2000

[13] Sugimoto T, Yamazaki K (2000) A study on secret key reconciliation protocol cascade. IEICE Transactions on Fundamentals, E83-A(10): 1987 – 1991

[14] Assche G V, Cardinal J, Cerf N J (2004) Reconciliation of a quantum distributed gaussian key. IEEE Transactions on Information Theory, 50(2): 394 – 400

[15] Bennett C H, Brassard G, Crepeau C, et al (1995) Generalized privacy amplification. IEEE Transactions on Information Theory, 41: 1915 – 1938

[16] Deutsch D, Ekert A, Jozsa R, et al (1996) Quantum privacy amplification and the security of quantum cryptography over noisy channels. Physical Review Letters, 77: 2818 – 2821

[17] Lütkenhaus N (1996) Security against eavesdropping in quantum cryptography. Physical Review A, 54: 97 – 112

[18] Lo H K, Chau H F (1999) Unconditional security of quantum key distribution over arbitrarily long distances. Science, 283: 2050 – 2057

[19] Mayers D (2001) Unconditional security in quantum cryptography. Journal of the ACM, 48: 351 – 406

[20] Bennett C H, Brassard G, Mermin N D (1992) Quantum cryptography without Bell's theorem. Physical Review Letters, 68: 557 – 559

[21] Boström K, Felbinger T (2004) Deterministic secure direct communication using entanglement. Physical Review Letters, 89: 1 – 4

[22] Wójcik A (2004) Eavesdropping on the "Ping-pong" quantum communication protocol. Physical Review Letters, 90: 1 – 4

[23] Hoffmann H, Bostroem K, Felbinger T (2005) Comment on "Secure direct communication with a quantum one-time pad". Physical Review A, 72: 016301

[24] Cai Q Y (2006) Eavesdropping on the two-way quantum communication protocols with invisible photons. Physics Letters A, 351: 23 – 25

[25] Wegman M N, Carter J L (1981) New hash function and their use in authentication and set equality. Journal of Computer and System science, 22: 265 – 287

[26] Cerf N J, Lévy M, Assche G V (2001) Quantum distribution of gaussian keys using squeezed states. Physical Review A, 63: 052311

[27] Grosshans F, Grangier P (2002) Continuous variable quantum cryptography using coherent states. Physical Review Letters, 88: 1 – 4

[28] Buttler W T, Lamoreaux S K, Torgerson J R, et al (2003) Fast, efficient error reconciliation for quantum cryptography. Physical Review A, 67(5): 052303

[29] Cardinal J, Assche G V (2003) Construction of a shared secret key using continuous variables. Proceedings of IEEE Information Theory Workshop (ITW), Paris, 2003

[30] Assche G V (2006) Quantum cryptography and secret-key distillation using quantum cryptography. Cambridge University Press, London

[31] Zeng G H (2006) Quantum cryptology. Science Press, Beijing

[32] Csiszar I, Körner J (1978) Broadcast channels with confidential messages. IEEE Transactions on Information Theory, 24(3): 339 – 348

[33] Maurer U M (1993) Secret key agreement by public discussion from common information. IEEE Transactions on Information Theory, 39(3): 733 – 742

[34] Brassard G, Lütkenhaus N, Mor T, et al (2000) Limitations on practical quantum cryptography. Physical Review Letters, 85(6): 1330 – 1333

[35] Scarani V, Acín A, Ribordy G, et al (2004) Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. Physical Review Letters, 92: 1 – 4

[36] Hwang W Y (2003) Quantum key distribution with high Loss: toward global secure communication. Physical Review Letters, 91: 1 – 4

[37] Wang X B (2005) Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography. Physical Review Letters, 94: 1 – 4

[38] Yuan Z L, Sharpe A W, Shields A J (2007) Unconditionally secure one-way quantum key distribution using decoy pulses. Applied Physics Letters, 90: 011118

5 Quantum Cryptosystem

This chapter investigates how to protect the confidentiality of the quantum private communication. By analogy with the classic cryptosystem, a notion called quantum cryptosystem is presented. Three kinds of quantum cryptosystems are described. One is the well known quantum Vernam cipher, the second is the quantum block cryptosystem, and the last is the quantum public-key cryptosystem. These cryptosystems are employed to protect the private message so that the attacker cannot obtain available information.

As described in Chapter 1, the confidentiality is a basic requirement for the private communication. To protect the confidentiality of private message transmitted in a communication system, an effective approach is to disturb the private message to be an unintelligible form by making use of the so-called cryptographic algorithm which is controlled under the "key". This gives rise to the so-called cryptosystem. The classic cryptosystem has been investigated and broadly applied in practices. By analogy with the classic cryptosystem, a new notion called the quantum cryptosystem, which is different from the quantum key distribution (QKD), is described in this chapter. By far, several typical quantum cryptosystems, such as the QKD-based cryptosystem, quantum Vernam cipher, quantum block cryptosystem, and quantum public-key cryptosystem, have been investigated, and some available algorithms have been proposed. Some of these algorithms have been exploited in practices.

Comparing to the classic cryptosystem, a distinct characteristic of the quantum cryptosystem is that its ciphertext could be indistinguishable when the generated ciphertext states are nonorthogonal, or even if it is possible that both the ciphertext and plaintext are entangled. In these situations, only obtaining the ciphertext is not available for eavesdropping the encrypted message due to the restriction of the quantum no-cloning theorem or entanglement properties. Apparently, the quantum cryptosystem is more suitable for the private communication than the classic cryptosystem.

This chapter focuses on the principle, algorithm design and security analysis of the quantum cryptosystem. Except for these issues, both the technical implementation and practical application of the quantum cryptosystem are also important topics in the quantum private communication. The technical implementation will be described in Chapters 7 and 8, and the application in practical communication systems will be addressed in Chapter 9.

5.1 Introduction

The key problem for the private communication is to solve the confidentiality and authentication of the communication systems, so that the attacker cannot obtain available information on the transmitted message. This chapter focuses on how to protect the confidentiality using quantum private communication techniques.

The secure transmission of classical information via cryptosystems is a well studied topic. For instance, suppose that Alice wants to send n bits private message M to Bob over an insecure (i.e., spied-on) channel. To prevent the attacker from obtaining any information about M with tapping the channel, an appropriate cryptosystem is always adopted in classic private communication. By this end many useful algorithms in classic cryptography have been proposed [**?**]. These algorithms are categorized as symmetrical-key cryptosystem and public-key cryptosystem. Of all presented classic algorithms, only the Vernam algorithm (also called one-time pad or Vernam cipher), which belongs to the framework of the symmetrical-key cryptosystem, has been proven with unconditional security. However, it cannot be used efficiently in practical application especially in the commercial application because of the intractable difficulties in the key management, such as the key distribution and the key storage. Fortunately, this situation has been changed partly by the QKD techniques, which have been propelled into the mainstream of computer science, secure communication, and physic in the past three decades. This result in the so-called quantum private communication which builds the secure communication in quantum ways.

To implement the quantum private communication in a practical communication system a quantum cryptosystem is necessary. Generally, there are two ways for the quantum encryption and decryption processes. The first is a combination of the QKD techniques with classic cryptosystems. In this case, the key point is to substitute the classic key generation and distribution module using the QKD techniques, while the encryption and decryption procedures are the same as that in the classic private communication. To protect the private communication, one of the classic cryptographic algorithms such as the well known one-time pad, advanced encryption standard (AES), and RSA algorithm is employed. This kind of cryptosystem is called the QKD-based cryptosystem in this book. Like the well known classic cryptology, the QKD-based cryptosystems can be applied for the data encryption, identification verification, signature, etc. The second way is a new design which uses pure quantum techniques. In this scenario, like the classic cryptosystem there are also two kinds of algorithms, i.e., quantum symmetrical-key algorithms and quantum public-key algorithms. In the range of the quantum symmetrical-key algorithms, the quantum Vernam algorithm and quantum block algorithm have been widely investigated in both theoretical and experimental. However, there are few investigations on the quantum public-key algorithm.

Making use of the cryptographic language, a quantum cryptosystem is defined mathematically as follows.

Definition 5.1.1 A quantum cryptosystem is a 5-tuple $\{\mathscr{M}, \mathscr{C}, \mathscr{K}, \mathscr{E}_k, \mathscr{D}_{k'}\}$, where the canonical notions and notations are plaintext space $\mathscr{M}$, ciphertext space $\mathscr{C}$, key space $\mathscr{K}$, family of the encrypting transformations $\mathscr{E}_k$, and family of the decrypting transformation $\mathscr{D}_{k'}$. The involved keys k and k' may be the same or different. If $k = k'$ or both keys are symmetrical, the corresponding cryptosystem is called a symmetrical-key algorithm. Otherwise it is called an asymmetrical-key algorithm.

Some other canonical notions and notations are the plaintext $M \in \mathscr{M}$, ciphertext $C \in \mathscr{C}$, key $K \in \mathscr{K}$, encrypting operation $E_k \in \mathcal{E}_k$ and decrypting operation $D'_k \in \mathscr{D}_{k'}$. The spaces $\mathscr{M}, \mathscr{C}, \mathscr{K}$ may be real spaces or Hilbert spaces. E_k and $D_{k'}$ mean the encrypting and decrypting transformations under the control of keys k and k', respectively. If the encryption and decryption procedures are the quantum transformation, they should be unitary operations and may be denoted using proper quantum logic gates.

In the quantum private communication, the plaintext and ciphertext are associated with qubits. Exactly, the plaintext means the message or the encoded codewords, which consists of qubits or/and classic bits. The particle which carry the plaintext is called as the plaintext particle, and the quantum state of the plaintext particles are called as the plaintext state. While the ciphertext means the encoded message, which consists of qubits or/and classic bits. The ciphertext particles indicate particles carried the ciphertext, and the ciphertext state means the quantum state of the ciphertext particles. It is noted that plaintext particles and ciphertext particles may be the same, but the plaintext state and ciphertext state must be different. As mentioned in above, the ciphertext particles and plaintext particles may be entangled in a suitable algorithm.

It is noted that the qubits in the ciphertext are usually indistinguishable so that the attacker is difficult to obtain available information. Even if the qubits in the ciphertext is entangled the qubits in the plaintext so that only obtaining the ciphertext qubit is not useful. These aims can be achieved by choosing suitable quantum operations in the quantum encryption algorithm controlled under the key. Clearly, the quantum ciphertext is unknown to the attacker but the ciphertext in the classic case is exactly known.

5.2 QKD-based Cryptosystem

In the classical cryptology, cryptosystems are categorized as the symmetrical key cryptosystem (SKC) and asymmetrical key cryptosystem, i.e., public key cryptosystem (PKC) [**?**, **?**]. The basic characteristic of SKC is that the encryption and decryption use same keys (or a pair symmetrical keys), which are kept secretly by communicators. While the main feature of PKC is that

the public key associated with a private key can be published publicly so that the public key may be announced like a telephone number. With only the public key one cannot, in principle, obtain any information about the private key. Since the holder may publicly announce the public key, everyone who wants to communicate with the holder can easily find the public key and can use it. The classic cryptographic algorithms have been widely used in both private information protection and private communication. However, the key management, including the key generation, key distribution, and key storage, has become an intractable problem. This makes for employment of the QKD technique in the classical cryptosystem, which may be called the QKD-based cryptosystem.

A QKD-based cryptosystem involves keys generated using quantum ways and a classical cryptosystem, which are both well understood and implemented experimentally [**?**, **?**]. In detail, a QKD-based algorithm consists of two parts, i.e., a classic cryptographic algorithm and a key generated using QKD techniques. Generally, two steps should be involved in such a kind of algorithms in practical applications. The first step is to generate a secure key using the QKD technique, and the second step is to combine the generated key and an appropriate cryptographic algorithm to perform the encryption and decryption processes. Since only symmetrical key is generated using the QKD scheme which has been investigated in Chapter 4, involved classic cryptographic algorithms are always symmetrical key algorithms, such as the Vernam algorithm, AES, and tri-DES, etc. Let the transmitted private message be m, the private communication model for the QKD-based cryptosystem is described in Fig.5.1. It is similar to the Shannon private communication model except for the key distribution channel.

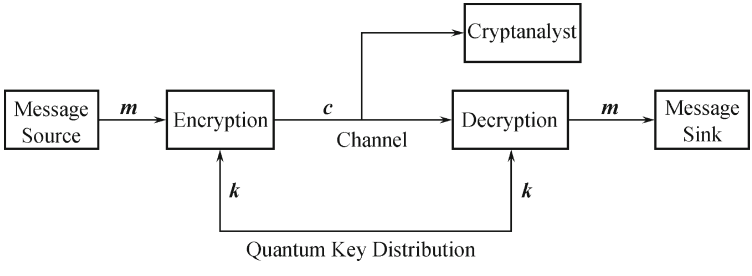

Fig. 5.1. Private communication model for QKD-based algorithm

A more interesting algorithm in such a scenario is the combination of the QKD technique and classic Vernam algorithm. Actually, the original motivation of the quantum cryptography is to generate a secure key for the Vernam cipher so that the obstacle of applying the Vernam cipher in practices is circumvented. One may call this kind of algorithms as the QKD-based Vernam cipher. The fundamental principle of the QKD-based Vernam cipher is very simple. First, communicators called as Alice and Bob distribute a shared

secret n-bit key k via the QKD technique. Then, Alice encrypts the plaintext m by carrying an exclusive-or with the secret key k, and sends the result (ciphertext) $c = m \oplus k$ over an imperfect channel to Bob. After that, Bob decodes the ciphertext using XOR operations on the ciphertext again with k and obtains the plaintext, i.e., $c \oplus k = m$. Eve may see the ciphertext c but this gives her no information about the plaintext since for any m' there is a key k' giving rise to the same encoding c. The QKD-based Vernam cipher has been implemented in experiment in different technique ways. In practices, however, there are still some technique problems to be solved. The main problem is that the key rate in the current QKD system is too lower (currently, it is about several kbit/s or even several bit/s) so that the practical application is impossible. Thus, to protect the private communication using the QKD-based Vernam algorithm, high-rate QKD systems are needed to be developed.

In the above the QKD-based cryptosystem which involves symmetrical-key algorithms are mainly discussed. Now we move on to the application of the QKD technique in PKC. Clearly, there are not direct correlation between the QKD technique and PKC since the later uses key-pair with the public key. However, because many public-key algorithms including encryption algorithms and digital signature algorithms (see Chapter 6) are associated with the random number sequence and hash function, while the QKD technique may be employed to generate true random numbers and construct hash functions in principle. Accordingly, it is possible that the QKD technique is applied in PKC in a suitable way. For example, one may employ the random number generated using the QKD technique to construct a random string s applied in the ElGamal algorithm so that it may work in a more secure way.

It has to stress that the security of the QKD-based algorithm depends on not only the employed QKD scheme but also involved classical algorithm. Therefore, if one employs a cryptographic algorithm with computational security, e.g., AES, then the QKD-based algorithm is still computationally secure but not unconditional security although the key is generated using the QKD scheme with unconditional security. Since in this scenario, only the part of the key generation and distribution have the same security as the employed QKD scheme. Generally, a combined cryptosystem, which consists of several independent parts, may reach at most the security level of those parts with lowest secure-level.

5.3 Quantum Vernam Cipher

Shannon has proven mathematically that the classic Vernam cipher may reach the informational security. However, there are drawbacks in the key management (especially in the key distribution and storage) when the Vernam cipher is employed in practices. This motivates investigation on the

QKD-based algorithm, which is a combined system of the QKD scheme and classic cryptographic algorithm. The security of such cryptosystem depends on the employed classic algorithm. If the employed cryptographic algorithm is the well known Vernam cipher, then a practically cryptographic algorithm with informational security is possible in principle. However, the security of the QKD-based Vernam cipher cannot yet reach the perfectness since the employed QKD system and Vernam algorithm are separated in currently technical operations. In addition, both the classic Vernam cipher and the QKD-based Vernam cipher cannot be used for quantum data, i.e., quantum bits. This prompts investigation on the so-called quantum Vernam cipher.

The quantum Vernam cipher may also call quantum Vernam algorithm, and it is similar to the classic Vernam algorithm. But it is not limited by the so-called "one-time" characteristic which is necessary in the classic Vernam algorithm for its security. Actually, in some quantum Vernam algorithms the shared key between communicators might be employed repeatedly since its quantum nature. Clearly, this characteristic is very useful in practical applications.

The quantum Vernam algorithm has been investigated widely. For example, making use of properties of quantum private channels a quantum Vernam algorithm in a special case was proposed in Ref.[**?**] and then a general model was proposed in Ref.[**?**]. These algorithms use classic bits as keys, and the message is encrypted by using quantum operations, i.e., unitary transformations, which are controlled under classic keys. In addition, quantum Vernam algorithms based on EPR pairs have also been investigated. These algorithms employ EPR pair(s) as keys. In Ref.[**?**] the message is encrypted by means of a quantum controlled-NOT with employment of a symmetrical key which consists of a EPR pair and a bilateral rotation. In Ref.[**?**] the message is encrypted with a key which consists of two EPR pairs. A common feature of the above quantum Vernam algorithms is that two qubits (bits) are necessary to encrypt one qubit message. In Ref.[**?**] a quantum Vernam algorithm employed an entanglement state as key with unsymmetrical operations was proposed. This algorithm is theoretically secure which is guaranteed by the no-cloning property of the key, but the implementation of the proposed algorithm is simple by exploiting entanglement photon pairs. In addition, some experiment schemes for the quantum Vernam algorithm have also been proposed in Refs.[**?**, **?**] with employing photon sequences.

This section introduces firstly the classic Vernam algorithm. Then gives a precise definition for the quantum Vernam cipher by analogy with the classic Vernam algorithm. Since the classic as well as quantum Vernam cipher are the private channel, a description for the quantum private channel is presented. Finally, a security theory model by analogy with the classic Vernam cipher is established.

5.3.1 Classic Vernam Algorithm

Before describing the quantum Vernam algorithm, it is useful to recall briefly the classic Vernam cipher. As stated in the previous section, implementation of the classic Vernam algorithm is very simple. If Alice and Bob share a secret n-bit key K, Alice encrypts the plaintext M by carrying an exclusive-ors with the secret key K, and then send Bob the result (ciphertext) $C = M \oplus K$ over an insecure channel. Bob then decodes the ciphertext by xoring the ciphertext again with K and obtains the plaintext, i.e., $C \oplus K = M$. Eve may see the ciphertext C but this gives her no information about the plaintext since for any M' there is a key K' giving rise to the same encoding C.

The aim of the Vernam algorithm is to reach the perfect secrecy. Thus, a classic Vernam algorithm is defined cryptographically as follows.

Definition 5.3.1 A 5-tuple $\{\mathscr{M}, \mathscr{C}, \mathscr{K}, \mathscr{E}, \mathscr{D}\}$ is called as a classic Vernam algorithm if and only if the following conditions are satisfied. (1) $\mathscr{M}$, $\mathscr{C}$, and $\mathscr{K}$ are space spanned by binary bits 0 and 1. (2) $\mathscr{E}$ and $\mathscr{D}$ are families of exclusive-ors transformations, and $\mathscr{E} = \mathscr{D}^{-1}$, i.e., $C = K \oplus M$ and $M = K \oplus C$, where $\oplus$ denotes addition modulus 2, $M \in \mathscr{M}, C \in \mathscr{C}$ and $K \in \mathscr{K}$. (3) The optimal length of the key is long as the plaintext. (4) The key can be used only one times.

Shannon's investigation shown that the classic Vernam algorithm is theoretically secure, and the optimal length of the key is long as the plaintext [**?**]. To warrant the unconditional security, conditions (3) and (4) in the above definition are necessary. It needs to stress that the unconditional security of the classic Vernam algorithm proven by Shannon only means that the ciphertext-only attack is impossible. However, in practical application, other factors should be concerned, such as the known-plaintext attack and key management. Because of difficulty of the key management, conditions (3) and (4) lead a huge cost or even if are impossible in the classic cryptology. Thus, unfortunately, these conditions decrease the availability of the classic Vernam algorithm in practical communication systems.

5.3.2 Quantum Vernam Cipher

By analogy with the classic Vernam algorithm, a quantum Vernam algorithm is defined as follows.

Definition 5.3.2 A 5-tuple $\{\mathscr{M}, \mathscr{C}, \mathscr{K}, \mathscr{E}_q, \mathscr{D}_q\}$ is called a quantum Vernam algorithm if and only if the following conditions are satisfied. (1) At least one of the 5-tuple is a Hilbert space or a quantum transformation. (2) $\mathscr{E}_q$ and $\mathscr{D}_q$ are families of quantum exclusive-ors transformations and $\mathscr{E}_q = {\mathscr{D}_q}^{-1}$, i.e., $|\psi^c\rangle = |K\rangle\hat{\oplus}|\phi^M\rangle$ and $|\psi^m\rangle = |K\rangle\hat{\oplus}|\phi^c\rangle$, where $\hat{\oplus}$ denotes a quantum exclusive-ors operation in which $|K\rangle$ is the target state, $|\psi^m\rangle \in \mathscr{M}$, $|\psi^c\rangle \in \mathscr{C}$, and $|K\rangle \in \mathscr{K}$.

Let us give a more detail explanations on the above definition. First, the definition shows that if at least one of the 5-tuple has quantum characteristic, then the algorithm is called as the quantum Vernam algorithm. Accordingly, if all of the five tuples are classic, it becomes a classic Vernam algorithm with the conditions (3) and (4) described in Definition 5.3.1. Secondly, from the viewpoint of information theory, the 5-tuple $\{\mathscr{M}, \mathscr{C}, \mathscr{K}, \mathscr{E}_q, \mathscr{D}_q\}$ constructs a channel. For example, when all of five tuples are classic, this channel is called as the classic private channel. When the plaintext and ciphertext spaces are Hilbert spaces, the key space is classic space, and the encrypting and decrypting transformations are unitary operations, the channel $\{\mathscr{M}, \mathscr{C}, \mathscr{K}, \mathscr{E}_q, \mathscr{D}_q\}$ is called as a quantum private channel which will be described in later. Naturally, when all of five tuples have quantum characteristics, i.e., the plaintext space, key space, and ciphertext space are Hilbert spaces and the encrypting and decrypting transformations are quantum operations (unitary operations), it could be called as a fully private quantum channel.

It is noted that Definition 5.3.2 is simpler than Definition 5.3.1. The main differences between the classic Vernam algorithm and quantum Vernam algorithm are two folds. First, the quantum Vernam algorithm demands at least one of the 5-tuple holding quantum characteristic, i.e., the quantum space or quantum operation. However, in the classic Vernam algorithm all of the 5-tuple are classic, e.g., binary spaces or exclusive-ors transformations. Second, the condition (4) in Definition 5.3.1 is not necessary in the definition 5.3.2, which means the key employed in the quantum Vernam algorithm may be used many times. This is because of the following reasons. In the classic Vernam algorithm, the use of a same key leads a redundant property, i.e., $M_1 \oplus M_2 = C_1 \oplus C_2$ with $M_1, M_2 \in \mathscr{M}$ and $C_1, C_2 \in \mathscr{M}$, which can be applied to break easily the cipher system. While in the quantum Vernam algorithm, the ciphers which are created by the same key with different plaintexts, give no redundant information on the plaintext and secret key, since the different ciphers are not distinguishable.

The advantage of the quantum Vernam algorithm is apparent because the difficulty of the key management in the quantum Vernam algorithm goes away. In addition, the quantum Vernam algorithm can encode quantum messages as well as classic messages, and the optimal length of the key may be the same as the plaintext, the details will be analyzed in later. However, the cost will be less than the classic Vernam algorithm when the technology for the quantum cryptography becomes practices.

Making use of the cryptographic language, the encryption and decryption procedures of the quantum Vernam algorithm are denoted formally by the following expressions,

$$Q_E^K(\rho_m) \to \rho_c, \tag{5.3.1}$$

and

$$Q_D^K(\rho_c) \to \rho_m, \tag{5.3.2}$$

where ρ_m and ρ_c denote the plaintext and ciphertext, i.e., message states

and ciphertext states, respectively. They may be pure states, mix states, or even classic states (this case means the classic bits). The symbols $Q_E^K \in \mathscr{E}_q$ and $Q_D^K \in \mathscr{D}_q$ denote respectively the quantum encryption algorithm and quantum decryption algorithm which are controlled under the key shared by legitimated communicators. Eqs.(5.3.1) and (5.3.2) show that the quantum Vernam algorithm is actually to encode the plaintext state to the ciphertext state under the control of encrypting key, and then decode the ciphertext state into plaintext state under the decrypting key. Since the Vernam algorithm is belong to the family of the symmetrical key cryptosystem, in the quantum Vernam algorithm as well as the classic Vernam algorithm, the encrypting key and decrypting key are same or symmetrical. This is a basic feature of the symmetrical key cryptosystem.

5.3.3 Private Quantum Channel

Let us sketch the following scenario. There are N possible keys identified with the numbers $1, 2, \ldots, N$. The probability of the ith key is p_i. Accordingly, the key has entropy $H(p_1, p_2, \ldots, p_N)$ when viewed as a random variable. Suppose that the legitimate communicator Alice wants to send a message $M \in \mathscr{M}$ to the legitimate communicator Bob. Then Alice encrypts the message M with the ith key. Bob, who shares the key with Alice, decrypts the cipher and obtains the message. If the attacker Eve can get no information at all about the send message M, i.e., the ciphertext is independent of the message M. Then this kind of channels is called as the private channel. The private channel has become a very useful tool in the classic communication. Obviously, the Vernam cipher is a private classic channel.

The private quantum channel (PQC) is defined in similar way. Let the quantum states $\rho_m \in \mathscr{M}$, suppose that each key i corresponds to a unitary transformation U_i, and let ρ_a be some fixed ancilla quantum states. Then the PQC is defined as follows [**?**].

Definition 5.3.3 Let $\mathscr{M} \subseteq \mathscr{H}^{2^n}$ be a set of quantum states, $\mathcal{E} = \{\sqrt{p_i}U_i | 1 \leq i \leq N\}$ be a superoperator where each U_i is a unitary mapping on $\mathscr{H}^{2^l}$, $\sum_{i=1}^N p_i = 1$, ρ_a be an $(l-n)$ density matrix, and ρ_0 be an l density matrix. Then $[\mathscr{M}, \mathcal{E}, \rho_a, \rho_0]$ is called a PQC if and only if for all $\rho_m \in \mathscr{M}$ one has

$$\mathcal{E}(\rho_m \otimes \rho_a) = \sum_{i=1}^{N} p_i U_i(\rho_m \otimes \rho_a)U_i^\dagger = \rho_0. \tag{5.3.3}$$

If $l = n$ (i.e., no ancilla), ρ_a is always omitted.

Like the private classic channel, a secure PQC requires that if Eve does not know i then the density matrix ρ_0 that she gets from monitoring the channel is independent of ρ_m. This implies that Eve gets no information at all about the message state ρ_m. Of course, Eve's measurement on the channel might destroy

the encoded message, but this is like classically jamming the channel and cannot be avoided. It is not hard to see that this is the most general quantum mechanical scenario which allows Bob to recover the message perfectly and at the same time gives Eve zero information.

From definitions 5.3.2 and 5.3.3, one may find that the quantum Vernam algorithm is a special case of the PQC.

5.3.4 Security Model

In the QKD scheme, the unconditional security of the final key depends not only on the quantum transmission procedure but also the key distillation procedure. However, the key reconciliation and privacy amplification are pure classic tools. These tools change inevitably contents of the obtained raw key. Actually, these compression techniques ensure just the unconditional security of the QKD scheme.

Apparently, the security model for QKD is not suitable for the quantum Vernam cipher. According to the general security model presented in Chapter 2, a security model is built here by analogy with the classic Vernam cipher. In the Vernam cipher Shannon proven that the perfect privacy of the cryptographic algorithm should satisfy

$$I(M, C) = 0, \tag{5.3.4}$$

or

$$I(K, C) = 0. \tag{5.3.5}$$

Similarly, a quantum Vernam cipher should satisfy

$$I(\rho^m, \rho^c) = 0, \tag{5.3.6}$$

or

$$I(K, \rho^c) = 0. \tag{5.3.7}$$

This leads

$$\rho^c \propto I, \tag{5.3.8}$$

which indicates that the ciphertext state cannot reveal any information on the key and plaintext state.

5.4 Typical Quantum Vernam Ciphers

In terms of the employed key, the quantum Vernam algorithm is divided into two categories: classic-key-based quantum Vernam algorithm and quantum-key-based quantum Vernam algorithm. The former uses classic key, e.g.,

binary string, which may be generated using classic way or the QKD technique. The later employs qubit-string, especially entanglement pairs as key. The quantum privacy amplification [**?**], i.e., the entanglement purification technique, gives rise to the possibility of share many entanglement-pair between communicators. As examples, this section introduces one classic-key-based quantum Vernam algorithm and three quantum-key-based quantum Vernam algorithms.

5.4.1 Classic-key-based Quantum Vernam Cipher

Suppose that the legitimate communicators Alice and Bob share a classic key, e.g., a binary key $K = \{k_1, k_2, \ldots, k_N\}$, where $k_i \in \{0, 1\}$ are elements of the key K. Now we show how to design a quantum Vernam algorithm using the binary key K.

Let $\rho = \{\rho_1, \rho_2, \ldots, \rho_n\}$ be plaintext, i.e., message, to be encrypted, U_i be a transform operator which is associated with the secret key k_i, and $p(k_i)$ is the probability of the key. The sender Alice encrypts a quantum state ρ_j by a pre-distributed secret key k and its related unitary operator U_k as $U_{k_i}\rho_j U_k^\dagger$. It is important to fix the ensemble $\{U_k\}$ so that $\sum_k p(k)U_k\rho_j U_k^\dagger$ is independent of j. The encryption procedure is denoted as

$$\rho_c = \sum_{i=1}^{N} p(k_i)U_i\rho U_i^\dagger, \tag{5.4.1}$$

where ρ_c denotes the whole ciphertext. Knowing the secret key K, the receiver can decrypt the quantum state with operating $U_K^\dagger$ on it. Obviously, the encryption and decryption procedures may be a quantum transform operation and its reverse transform operation of the plaintext and ciphertext, respectively.

As an example, the operator U_i is defined as $U_i = \otimes_{i=1}^{m}(X^{k_{2i}}Z^{k_{2i-1}})$ and $p(k) = 1/2^{2n}$ in Ref.[**?**], where k_{2i-1}, k_{2i} are elements in the secret key k with $i = 1, 2, \ldots, m$ and $k_{2i-1}, k_{2i} \in \{0, 1\}$. In this case, the length of the key for quantum Vernam algorithm is $2n$, where n is the length of the message. The encryption procedure reads

$$\rho_c = \sum_{\alpha,\beta} \frac{1}{2^{2n}} X^\alpha Z^\beta \rho_i (X^\alpha Z^\beta)^\dagger. \tag{5.4.2}$$

Expanding any message state ρ_i in the $X^\alpha Z^\beta$ basis gives

$$\rho_i = \sum_{\alpha,\beta} a_{\alpha,\beta} X^\alpha Z^\beta, \tag{5.4.3}$$

where $a_{\alpha,\beta} = Tr(\rho_i Z^\beta X^\alpha)/2^n$. Using this formalism, it is clear that the given

choice of $p(k_i)$ and $U(k_i)$ guarantee the following result,

$$\sum_i p_i U_i \rho_i U_i^\dagger = \frac{1}{2^{2n}} \sum_{\gamma,\delta} X^\gamma Z^\delta \rho_i Z^\delta X^\gamma = \frac{I}{2^n}. \tag{5.4.4}$$

This illustrates the ciphertext state distributes in a uniform way so that no information on plaintext state and the key might be leaked to the eavesdropper. Consequently, the above algorithm is secure.

5.4.2 Bell-key-based Quantum Vernam Cipher

Using one of four Bell states $\{|\Phi^\pm\rangle, \Psi^\pm\rangle\}$ as key the quantum Vernam algorithm is possible. For convenience, it is called as the Bell-key-based quantum Vernam algorithm. Commonly, the Bell states are typical two-particle entanglement states. These states have been widely used in many scenarios because of their novel characteristics. Interestingly, the shared entanglement states between two legitimate communicators may be regarded as a quantum key. This is different apparently from the QKD system where the final key is actually a binary string. Investigations on such a case have been presented in Ref.[**?**, **?**]. Here we conclude a general algorithm for the Bell-key-based quantum Vernam algorithm using entanglement states as keys.

Suppose that Alice and Bob share N identical EPR pairs as the key K, i.e.,

$$K = (|k_1\rangle, |k_2\rangle, \ldots, |k_i\rangle, \ldots, |k_N\rangle), \tag{5.4.5}$$

each element in the key corresponds to a EPR pair,

$$|k_i\rangle = |\Phi_i^+\rangle = \frac{1}{\sqrt{2}}(0_a 0_b\rangle + |1_a 1_n\rangle), \tag{5.4.6}$$

where the subscripts a, b denote the particles p_a and p_b hold by Alice and Bob, respectively.

Denote the plaintext state,

$$|\psi^m\rangle = \alpha|0\rangle + \beta|1\rangle), \tag{5.4.7}$$

which is carried by the particle p_m. Using the controlled-NOT gate on her particle and the message particle p_m, Alice encrypts the message state according to the following way,

$$|\phi^c\rangle = C_{am}^n\{|k_n\rangle C_{am}^{n-1}[|k_{n-1}\rangle \ldots C_{am}^1(k_1\rangle|\psi^m\rangle)]\}, \tag{5.4.8}$$

where C_{am}^i denotes the ith C_{NOT} gate applied on p_a and p_m.

After having finished the encryption operation, p_m is sent to Bob, who shares the key with Alice. Then Bob may obtain the message state using the following operation,

$$|\phi^m\rangle = C_{mb}^n\{|k_1\rangle C_{mb}^{n-1}[|k_2\rangle \ldots C_{mb}^1(k_n\rangle|\psi^c\rangle)]\}, \tag{5.4.9}$$

where C_{mb}^{i} denotes the ith control-NOT gate applied on the p_m and p_b.

Operationally, communicators Alice and Bob should share a Bell state sequence when they want to establish a private communication. One may imagine the following communication model. Suppose that Alice and Bob share initially no information except for knowledge for authentication. When Alice wants to send a private message to Bob, she firstly builds a quantum key channel which consists of Bell states. To reach this aim the entanglement purification technique or call quantum privacy technique is employed. Then, the message is encrypted by Alice and then decrypted by Bob using the shared Bell-key. Clearly, distribution of the employed quantum-key, i.e., Bell states, and the message encryption and decryption procedures may be executed simultaneously. Consequently, the quantum memory is not necessary.

Example 1 Consider a special case of $N = 1$ in Eq.(5.4.5). In this case, the communicators only share one EPR pair. Thus the key state satisfies $|k\rangle = |\Phi^+\rangle$. The encryption procedure is simplified as

$$|\phi^c\rangle = C_{am}(|k\rangle|\psi^m\rangle) = C_{am}(|\Phi^+\rangle|\psi^m\rangle), \tag{5.4.10}$$

and the decryption procedure reads

$$|\phi^m\rangle = C_{mb}(|\psi^m\rangle|k\rangle) = C_{mb}(|\psi^m\rangle|\Phi^+\rangle). \tag{5.4.11}$$

Example 2 Consider a special case of $N = 2$ in Eq.(5.4.5). This situation has been investigated in Ref.[**?**] in 2001. The key may be expressed as $K = (|k_1\rangle, k_2\rangle)$, where the key elements are given by

$$|k_1\rangle = \frac{1}{\sqrt{2}}(0_a^1 0_b^1\rangle + |1_a^1 1_n^1\rangle), \tag{5.4.12}$$

and

$$|k_2\rangle = \frac{1}{\sqrt{2}}(0_a^2 0_b^2\rangle + |1_a^2 1_n^2\rangle). \tag{5.4.13}$$

The encryption procedure yields the following ciphertext state,

$$|\phi^c\rangle = C_{a_2m}^{Z}(C_{a_1m}^{X}|k_1\rangle|\psi^m\rangle|k_2\rangle), \tag{5.4.14}$$

where $C_{a_2m}^{Z}, C_{a_1m}^{X}$ are control-Z and control-X gates, respectively. When Bob gets the ciphertext state, he may decrypt easily it using the following way,

$$|\phi^m\rangle = C_{b_1m}^{X}(C_{b_2m}^{Z}|\psi^c\rangle). \tag{5.4.15}$$

In the above examples 1 and 2, the presented quantum Vernam algorithms have been proven to be secure in Refs.[**?**, **?**]. However, they are fragile against the Trojan horse attack. This may be circumvented using the following improvement [**?**]. Suppose that the legitimate communicators Alice and Bob share an EPR pair $|\Phi^+\rangle$ as the key, i.e., $|k\rangle = |\Phi^+\rangle$. Bob presents

a quantum controlled-NOT gate set $\mathscr{G}$ which consists of C_{12} and U_{12}, i.e., $\mathscr{G} = \{C_{12}, U_{12}\}$, where the controlled-NOT gates C_{12}, U_{12} are defined respectively as

$$C_{12}|\epsilon_1\rangle|\epsilon_2\rangle = |\epsilon_1\rangle|\epsilon_1 \oplus \epsilon_2\rangle, \tag{5.4.16}$$

and

$$\begin{cases} U_{12}(|+\rangle|\epsilon\rangle) \to |+\rangle|(\epsilon \oplus 1)\rangle, \\ U_{12}(|-\rangle|\epsilon\rangle) \to |-\rangle|\epsilon\rangle, \end{cases} \tag{5.4.17}$$

where $\epsilon_{1,2}, \epsilon \in \{0, 1\}$. In matrix form C_{12} and U_{12} are denoted respectively,

$$C_{12} = \begin{pmatrix} I & \mathbf{0} \\ \mathbf{0} & \sigma_x \end{pmatrix}, \tag{5.4.18}$$

and

$$U_{12} = \begin{pmatrix} \sigma_x & \mathbf{0} \\ \mathbf{0} & I \end{pmatrix}, \tag{5.4.19}$$

where $\mathbf{0}$ denotes a 2×2 matrix with 0 elements. It is very easy to prove that $U_{12}^\dagger = U_{12}$ and $U_{12}^\dagger U_{12} = U_{12} U_{12}^\dagger = I$. So U_{12} is physically implementable, which means that U_{12} is a quantum control gate.

Before Alice sends the private message, Bob randomly operates his EPR particle using the gate $G \in \{I, H\}$, where I and H are the identity matrix and Hadamard matrix, respectively. The operation I or H change the key state to be a Bell state $|k\rangle = |\Phi^+\rangle$ or the state $|k'\rangle = H|\Phi^+\rangle = |\psi^+\rangle = \frac{1}{\sqrt{2}}(|1_a{+}_b\rangle + |0_a{-}_b\rangle)$, respectively. Then Alice encrypts her message use the key. Denote the plaintext state, i.e., the message state,

$$|\psi^m\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha'|+\rangle + \beta'|-\rangle, \tag{5.4.20}$$

where $\alpha' = 1/\sqrt{2}(\alpha+\beta), \beta' = 1/\sqrt{2}(\alpha-\beta)$, and $|\alpha|^2+|\beta|^2 = |\alpha'|^2+|\beta'|^2 = 1$. To send the plaintext $|\psi^m\rangle$ to Bob, Alice applies a controlled-NOT gate C_{am} on the entangled particle p_a and the plaintext particle p_m. This operation (encryption process) yields the ciphertext state. Clearly, the ciphertext state is associated with states of the particles p_a, p_b and p_m, and it is a three-particle entanglement state. When the key element is the Bell state $|k\rangle = |\Phi^+\rangle$, the three-particle entanglement state is

$$\begin{aligned} |\psi^{c_1}\rangle &= C_{am}|\Phi^+\rangle|\psi^m\rangle \\ &= \sum_{i=0,1} \gamma_i(|0_a 0_b i_m\rangle + |1_a 1_b (i \oplus 1)_m\rangle) \\ &= \frac{1}{\sqrt{2}} \sum_{i=0}^{1} |i_a i_b\rangle \otimes (\mathbf{I}\delta_{i,0} + X_m \delta_{i,1}) |\psi^m\rangle, \end{aligned} \tag{5.4.21}$$

where $\gamma_i = (\alpha\delta_{i0} + \beta\delta_{i1})/\sqrt{2}$, δ_{ij} is the Kronecker delta, the subscript m specifies the particle p_m, and X_m is an X gate to the particle p_m. When the key element has been changed by the Hadamard gate, i.e., $|k'\rangle = |\psi^+\rangle$, the three-particle entanglement state has the following form,

$$\begin{aligned}|\psi^{c_2}\rangle &= C_{am}|\psi^+\rangle|\psi^m\rangle \\ &= \sum_{i=0,1} \gamma_i(|1_a +_b (i \oplus 1)_m\rangle + |0_a -_b i_m\rangle) \\ &= \frac{1}{\sqrt{2}} \sum_{i=0}^{1} |i_a \lambda_b^i\rangle \otimes (\mathbf{I}\delta_{i,0} + X_m\delta_{i,1})\,|\psi^m\rangle, \end{aligned} \tag{5.4.22}$$

where $\lambda_b^0 = |-_b\rangle$, $\lambda_b^1 = |+_b\rangle$.

It is easy to verify that $|\langle\psi^{c_1}|\psi^{c_2}\rangle|^2 \neq 0$ which means these ciphertext states are nonorthogonal states. According to Eqs.(5.4.21) and (5.4.22), Alice's encryption generates the output state $|\psi^{c_1}\rangle$ or $|\psi^{c_2}\rangle$ relying on the employed operation I or H on the key element, respectively. Because Bob knows the key he can exactly recognize these states. However, any attacker cannot distinguish these states without the key because $|\psi^{c_1}\rangle$ and $|\psi^{c_2}\rangle$ are nonorthogonal. Suppose that Bob chooses randomly the gate from $\mathscr{G}$ with identical probability, i.e., the probabilities p_1 and p_2 for choosing the gate I and H are the same, respectively. Then the ciphertext is a mixed state from Eve's viewpoint. Thus, the ciphertext can be written as

$$\rho^c = p_1\rho^{c_1} + p_2\rho^{c_2} = \frac{1}{2}\left(|\psi^{c_1}\rangle\langle\psi^{c_1}| + |\psi^{c_2}\rangle\langle\psi^{c_2}|\right). \tag{5.4.23}$$

Simple calculation gives $\rho^c \propto I$. Consequently, the algorithm is unconditional security.

After having finished the encrypting transformation, Alice obtains the ciphertext. Then Alice sends the particle p_m to Bob, which means to send the ciphertext state to Bob. In the next step, Bob decrypts the received ciphertext states. Because Bob knows the key K, the decrypting transformation can be performed very easily by choosing a proper control operation from C_{12} and U_{12}. When the key element is the Bell state $|\Phi^+\rangle$, Bob applies the gate C_{bm} on the particles p_b and p_m. After this operation, Bob obtains the plaintext because

$$C_{bm}|\psi^{c_1}\rangle = |\Phi^+\rangle \otimes |\psi^m\rangle. \tag{5.4.24}$$

When key element is the superposition state $|\psi^+\rangle$, Bob uses the gate U_{bm} on the particles p_b and p_m. This operation gives

$$U_{bm}|\psi^{c_2}\rangle = |\psi^+\rangle \otimes |\psi^m\rangle. \tag{5.4.25}$$

Obviously, Bob also obtains the plaintext $|\psi^m\rangle$.

It is noted that Eqs.(5.4.24) and (5.4.25) show the encrypting and decrypting transformations do not disentangle the key's entanglement. In addition,

the secrecy of the key is not decreased by the encryption and decryption operation. Therefore, the key might be utilized many times. This is different from the classic Vernam algorithm and presented quantum Vernam algorithms in Refs.[5 – 8]. This property is very useful in the practical application.

In the above, how to encrypt the general qubit (quantum message) denoted in Eq.(5.4.20) has been demonstrated. It is noted that Bob's decryption can only get a unknown state because α and β cannot be determined by the decrypting transformation. To make Bob know completely the qubit Alice should send again a public parameter, e.g., the phase information on the message, to Bob. However, this procedure has nothing to do with the cryptographic algorithm. In addition, this kind of treatments will not influence the security of the employed algorithms.

In practical application, the message (e.g., images, text, etc) is firstly encoded using simple and effective codewords before Alice's encryption. A codeword consists of alphabets. In the quantum case, the simplest alphabets may be $|0\rangle$ and $|1\rangle$. Therefore from the aspect of practical communication, one only needs to consider the encryption and decryption of quantum states $|0\rangle$ and $|1\rangle$. When the qubit in plaintext is $|0_m\rangle$, Eqs.(5.4.21) and (5.4.22) become

$$|\psi_0^{c_1}\rangle = C_{am}|\Phi^+\rangle|0_m\rangle = \frac{1}{\sqrt{2}}\left(|0_a 0_b 0_m\rangle + |1_a 1_b 1_m\rangle\right), \tag{5.4.26}$$

and

$$|\psi_0^{c_2}\rangle = C_{am}|\psi^+\rangle|0_m\rangle = \frac{1}{\sqrt{2}}\left(|1_a +_b 1_m\rangle + |0_a -_b 0_m\rangle\right). \tag{5.4.27}$$

When the qubit in plaintext is $|1_m\rangle$, Eqs.(5.4.21) and (5.4.22) become

$$|\psi_1^{c_1}\rangle = C_{am}|\Phi^+\rangle|1_m\rangle = \frac{1}{\sqrt{2}}\left(|0_a 0_b 1_m\rangle + |1_a 1_b 0_m\rangle\right), \tag{5.4.28}$$

and

$$|\psi_1^{c_2}\rangle = C_{am}|\psi^+\rangle|1_m\rangle = \frac{1}{\sqrt{2}}\left(|1_a +_b 0_m\rangle + |0_a -_b 1_m\rangle\right). \tag{5.4.29}$$

Eqs.(5.4.26) and (5.4.27), and Eqs.(5.4.28) and (5.4.29) show that it is possible to encrypt the message which is encoded by using quantum alphabets $|0\rangle$ and $|1\rangle$. These equations also show the proposed algorithm can encrypt the classic plaintext. Because Eve does not know the key, the ciphertext state what the Eve can "see" takes the following form,

$$\rho^c = \frac{1}{4}\left(|\psi_0^{c_1}\rangle\langle\psi_0^{c_1}| + |\psi_0^{c_2}\rangle\langle\psi_0^{c_2}| + |\psi_1^{c_1}\rangle\langle\psi_1^{c_1}| + |\psi_1^{c_2}\rangle\langle\psi_1^{c_2}|\right). \tag{5.4.30}$$

Obviously, the attacker cannot break the cipher because he cannot recognize correctly the four ciphertext states, i.e., $|\psi_0^{c_1}\rangle, |\psi_0^{c_2}\rangle, |\psi_1^{c_1}\rangle$ and $|\psi_1^{c_2}\rangle$. In addition, each of these state is a three-particle entanglement state. However, Bob

has not such problem because of his knowledge on the key. By choosing a proper quantum gate like that in the above decryption, Bob can completely decrypt the ciphertext state in the Eq.(5.4.30). Then measuring the particle p_m by making use of the base for $\{|0\rangle, |1\rangle\}$ Bob finally obtains the message. It is noted that Bob does not need any of Alice's public parameter in this case. This algorithm also shows that the classic message can be encrypted and decrypted using quantum cryptosystem.

5.4.3 Teleportation as Quantum Vernam Cipher

The teleportation is a well-known quantum communication mode, it has been suggested as a quantum vernam algorithm in Ref.[**?**]. According to the teleportation scheme, a pre-shared EPR pair is required. Regarding it as a quantum Vernam algorithm, the pre-shared EPR pair is actually the shared key between legitimate communicators. In addition, the teleportation scheme needs a classic channel to transmit the Bell states information (classic information), without this channel the plaintext cannot be decrypted by the receivers.

Now we show how to implement the encryption and decryption procedures using the quantum teleportation. Suppose that Alice and Bob has shared a EPR pair as the key, i.e.,

$$|K\rangle = |\Phi^+\rangle. \tag{5.4.31}$$

Let the plaintext be the following state

$$|\psi^m\rangle = \alpha^m|0\rangle + \beta^m|1\rangle, \tag{5.4.32}$$

where the supscript m implies the message. To encrypt the message state, Alice combines the shared EPR pair, i.e., the key state $|K\rangle$ and message state $|\psi^m\rangle$ to generate a product state $|\psi^c\rangle = |K\rangle \otimes |\psi^m\rangle$. This operation gives

$$\begin{aligned} |\psi^c\rangle = \frac{1}{\sqrt{2}} \big[&|\Phi^+\rangle(\alpha^m|1\rangle - \beta^m|0\rangle) + |\Phi^-\rangle(\alpha^m|1\rangle + \beta^m|0\rangle) \ + \\ &|\Psi^+\rangle(-\alpha^m|0\rangle + \beta^m|1\rangle) + |\Psi^-\rangle(-\alpha^m|0\rangle - \beta^m|1\rangle)\big], \end{aligned} \tag{5.4.33}$$

where $|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle$, and $|\Psi^-\rangle$ are four Bell states. Then Alice makes a Bell measurement on the ciphertext state. This measurement generates output which is one of four Bell states. In addition, this measurement changes Bob's particle state. Subsequently, all possible quantum states of the particle hold by Bob are associated with Alice's possible measurement results. The relationships are shown in Table 5.1.

After having performed the Bell measurements, Alice sends the measurement results to Bob. According to the received measurement results from Alice, Bob operates his particles using one of suitable unitary transformations from $U = \{U_1, U_2, U_3, U_4\}$ to obtain the message state, where U_i are

Table 5.1. Correlation between Alice's Bell measurements and Bob's quantum states

$\|\Psi^+\rangle$	$\alpha^m\|1\rangle - \beta^m\|0\rangle$
$\|\Phi^-\rangle$	$\alpha^m\|1\rangle + \beta^m\|0\rangle$
$\|\Psi^+\rangle$	$-\alpha^m\|0\rangle + \beta^m\|1\rangle$
$\|\Psi^-\rangle$	$-\alpha^m\|0\rangle - \beta^m\|1\rangle$

expressed by

$$\begin{cases} U_1 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \\ U_2 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \\ U_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \\ U_4 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \end{cases} \tag{5.4.34}$$

After these transformations Bob obtains the plaintext states according to the following transformations,

$$\begin{cases} |1\rangle = U_1 \begin{pmatrix} \alpha^m \\ \beta^m \end{pmatrix} \Rightarrow |\psi^m\rangle = U_1^{-1}|1\rangle, \\ |2\rangle = U_2 \begin{pmatrix} \alpha^m \\ \beta^m \end{pmatrix} \Rightarrow |\psi^m\rangle = U_2^{-1}|2\rangle, \\ |3\rangle = U_3 \begin{pmatrix} \alpha^m \\ \beta^m \end{pmatrix} \Rightarrow |\psi^m\rangle = U_3^{-1}|3\rangle, \\ |4\rangle = U_4 \begin{pmatrix} \alpha^m \\ \beta^m \end{pmatrix} \Rightarrow |\psi^m\rangle = U_4^{-1}|4\rangle. \end{cases} \tag{5.4.35}$$

5.5 Quantum Block Cipher

Investigations on the block cipher is motivated by engineering considerations. Currently, this technique has been widely used in the classic cryptology. In principle, there are not new physical laws being involved for the block cipher, however, the blocking operation influences security of the involved algorithm from the viewpoint of cryptology. This section introduces a new notion called

quantum block cipher by analogy with the classic block cipher, and investigates influences of the blocking operation on the security of the involved quantum block cipher.

5.5.1 Theoretical Model

Usually, the encoded message string, i.e., the plaintext string, is very long so that the direct encryption and decryption operations are not convenient in engineering applications. Accordingly, the plaintext string is usually divided into blocks before the encryption operation, and then each block is encrypted using the same key. In the classic cryptology such a kind of cryptosystems is called the block cipher. By analogy with the classic block cipher, a new concept called quantum block cipher is suggested in this section.

Let the plaintext string be $x_1, x_2, \ldots, x_i, \ldots, x_N$. Divide this string into M blocks and the length of each block is m. For example, the first block is denoted $\mathbf{x}_1 = \{x_0, x_1, \ldots, x_{m-1}\}$. If length of the last block, i.e., Mth block, is less than m, some "0" bits are added so that the length of this block is the same as the others. After having finished the blocking operation, Alice encrypts each block in turn with the same key $\mathbf{k} = \{k_0, k_1, \ldots, k_{l-1}\}$ and generates ith output (i.e., ciphertext) $\mathbf{y}_j = \{y_0, y_1, \ldots, y_{n-1}\}$ (a vector with length n) with $j = 1, 2, \ldots, M$. The encryption algorithm denotes $\mathcal{E} : \mathbb{V}_n \times \mathbb{K} \to \mathbb{V}_{n'}$, where $\mathbb{V}_n, \mathbb{K}$, and $\mathbb{V}_{n'}$ denote an n-dimension plaintext space, key space, and ciphertext space, respectively. One should note here that each block is encrypted and decrypted using same transformation which controls under the same key. Of course, the employed key is usually transformed according to a determined rule, e.g., permuting key elements in $\mathbf{k}$ so that the generated key used in each turn is different although they are evolved from a same initial key $\mathbf{k}$. The aim of this operation is to enhance the privacy of the key.

Like the classic block cipher one may define the so-called quantum block cipher. Let the plaintext string be $|x_1\rangle, |x_2\rangle, \ldots, |x_i\rangle, \ldots, |x_N\rangle$. Divide this string into M blocks as the classic block cipher and the length of each block is m. Then encrypting each block with the same key $\mathbf{k} = \{k_0, k_1, \ldots, k_{l-1}\}$ generates output (i.e., ciphertext) $|\mathbf{c}\rangle_j = \{|c_0\rangle, |c_1\rangle, \ldots, |c_{n-1}\rangle\}$. The encryption algorithm denotes $\mathcal{QE} : \mathscr{H}_{2^n}^x \otimes \mathscr{H}_{2^l}^k \to \mathscr{H}_{2^n}^c$, where $\mathscr{H}_{2^n}^x, \mathscr{H}_{2^n}^k, \mathscr{H}_{2^n}^c$ denote the Hilbert space of plaintext state, key state and ciphertext state, respectively. In addition, each block is encrypted using the same transformation which controls under the same key, i.e., the employed encryption algorithms are the same.

There are differences between the quantum block cipher and quantum Vernam cipher. In the quantum Vernam cipher each plaintext element is encrypted using one key element. Although the key may be used repeatedly in various private communications, but the key is not admitted to encrypt

multi-qubit in the same plaintext string. However, in the quantum block cipher the key may be used many times which depends on the number of blocks in the same plaintext string. Especially, the same key element may be used for many times in the encryption procedures.

The blocking operations will naturally influence the security of the employed algorithm. Although the key is transformed in each turn using suitable operations such as permutation, position shift, etc., there exists always available information leakage to Eve. Therefore, the classic block cipher cannot reach an unconditional security like that in the Vernam cipher. Actually, its security depends on a complexity problem which is generated by operations, e.g., permutation and shift operations, in each turn. In the quantum scenario, however, the quantum block cipher can still reach an unconditional security like the quantum Vernam cipher. Denote the encryption algorithm Q_E^k, the encryption procedure for ith qubit in ι block is given by

$$\mathcal{Q}_E^{k_i}(|x_i\rangle) \to |c_j\rangle. \tag{5.5.1}$$

Similarly, the encryption procedure for ith qubit in $\iota + \ell$ block is given by

$$\mathcal{Q}_E^{k_i}(|x_i'\rangle) \to |c_j'\rangle. \tag{5.5.2}$$

Since plaintext states $|x_i\rangle$ and $|x_i'\rangle$ are different, even if the key elements which are employed for encrypting these plaintext states are the same, the encryption procedures give different ciphertext states. Actually, a suitable operation for each turn to change the position of key element is always employed in practices. Thus, it is very difficult to obtain same ciphertext states. According to the quantum no-cloning theorem, the ciphertext states are indistinguishable.

As an example, consider the situation that both plaintext state and cipher state are B-qubits. According to the mathematical properties introduced in Chapter 3, only the point and its opposite point in the Bloch sphere are orthogonal. For others, one has

$$\langle c_j|c_j'\rangle = \langle x_i|(\mathcal{Q}_E^{k_i})^\dagger(\mathcal{Q}_E^{k_i})|x_i'\rangle = \langle x_i|x_i'\rangle. \tag{5.5.3}$$

In practical application, two arbitrary plaintext qubits $|x_i\rangle$ and $|x_i'\rangle$ from the blocks ι and $\iota + \ell$, respectively, may be assumed to be different since two same blocks string can be disturbed with permutation operations. Thus, one can always obtain the result

$$\langle c_j|c_j'\rangle \neq 0.$$

This means that the total ciphertext state is a mixed state. Accordingly, the quantum no-cloning theorem guarantees the unconditional security of the quantum block encryption algorithm.

5.5.2 Quantum Block Algorithm for Binary Bits

Making use of the above theory, this subsection exemplifies how to encrypt binary bits via a quantum block algorithm. Divide the plaintext $\mathbf{X}$ into N blocks, and each block has l elements, where $l < N$. Then the plaintext is represented by

$$\mathbf{X} = (\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_i, \ldots, \mathbf{x}_N),$$

with the block $\mathbf{x}_i = (x_1, x_2, \ldots, x_l)$ $(i = 1, 2, \ldots, N)$, and the key is denoted $K = (k_1, k_2, \ldots, k_l)$.

1) Encryption Algorithm

Let us consider the encryption procedure of the classical plaintext bit in ith block. The encryption algorithm executes the following steps.

Step 1: Encoding. Alice chooses randomly a binary-bit string denoted by $\mathbf{s} = \{s_1, s_2, \ldots, s_l\}$ with $s_j \in \{0, 1\}$ $(j = 1, 2, \ldots, l)$. Encoding the random number $\mathbf{s}$ and plaintext bits $\mathbf{x}_i$ $(i = 1, 2, \ldots, N)$ into a qubit yields a result $|C_1\rangle$ expressed by

$$|C_1\rangle = \{|s_1 s_2 \ldots s_l x_1 x_2 \ldots x_l\rangle\}, \tag{5.5.4}$$

where $\{\ldots\}$ denotes a set, $s_j, x_j \in \{0, 1\}, j = 1, 2, \ldots, l$. Note, the random string $\mathbf{s}$ is independent of the plaintext bits $\mathbf{x}_i$ and key bits k_i.

Step 2: Controlled-NOT operation. Alice performs a controlled-NOT operation on the random bit s_j and plaintext bit x_j according to the key element k_j. If $k_j = 0$, the random bit s_j in $|C_1\rangle$ is regarded as the control qubit of the controlled-NOT operation; otherwise Alice takes the value $y_j = s_j \oplus s_{j+1}$ (when $j = l$ the value is $y_l = s_l \oplus s_1$) as the control-qubit for the controlled-NOT operation. The qubit x_j in $|C_1\rangle$ always acts as the target qubit. Then, the resulting ciphertext state is formulated by

$$\begin{aligned} |C_2\rangle &= (\delta_{k_j,0} C_{s_j,x_j} + \delta_{k_j,1} C_{y_j,x_j})|C_1\rangle \\ &= \{|s_1 s_2 \ldots s_l \alpha_1 \alpha_2 \ldots \alpha_l\rangle\}, \end{aligned} \tag{5.5.5}$$

where $C_{\alpha,\beta}$ denotes the controlled-NOT gate operating on the control qubit α and the target qubit β, and $\alpha_j = (\delta_{k_j,0} s_j + \delta_{k_j,1} y_j) \oplus x_j$ with $j = 1, 2, \ldots, l$. The last l bits in each state of $|C_1\rangle$ are the original information bits, but in each state of $|C_2\rangle$ they are the result of the controlled-NOT transformation and are no longer the original information bits themselves.

Step 3: Permutation. The existing algorithms usually fix a qubit position to represent the private information qubit, which may pose threats to the security of the encryption system in some special cases. Actually, Alice can permute any two qubits in the resulting state $|C_2\rangle$ using a permutation operation. For clearly, a simple approach is presented here: permutate the qubits according to the value of the key element k_j. In detail, if k_j is 0, no permutation is applied, otherwise swap the positions of jth and $(j + l)$th qubits. For example, suppose the state $|C_2\rangle = |000_{m_j}\rangle$, then the resulting

state is $|000_{m_j}\rangle$ when the key element is 0, or else $|00_{m_j}0\rangle$. And suppose that one state is $|C_2\rangle = |010_{m_j}\rangle$, the resulting state is $|010_{m_j}\rangle$ as the key element is 0, or else $|00_{m_j}1\rangle$. Using this rule, the set of the possible ciphertext state $|C_3\rangle$ is given as following,

$$|C_3\rangle = \left\{ \left[\bigotimes_{j=1}^{l} (|s_j\rangle\delta_{0,k_j} + |\alpha_j\rangle\delta_{1,k_j}) \right] \left[\bigotimes_{j=1}^{l} (|\alpha_j\rangle\delta_{0,k_j} + |s_j\rangle\delta_{1,k_j}) \right] \right\}. \quad (5.5.6)$$

Ciphertext states in $|C_3\rangle$ are different in form from those in $|C_1\rangle$, the first l qubits of each state of $|C_3\rangle$ may involve information about the message (plaintext), unlike those of $|C_1\rangle$ where the information about the plaintext is just confined to the last l qubits. Thus the ciphertext space is doubled.

Step 4: Non-orthogonality. Up to now, the intermediate ciphertext states Alice obtained are orthogonal. Although these ciphertext are private without discovering the key k, but this procedure has only the security level like the classic encryption algorithm. To enhance the security a novel quantum property, i.e., the nonorthogonality, is employed, so that the ciphertext is hard to be distinguished by the attacker. To reach this aim, Alice carries out quantum computation on the ciphertext states in $|C_3\rangle$ under the control key elements combination, i.e., $k'_j = k_j k_{j+1}$. If the key elements are 00 or 11, no operation is applied. However, if the key element is 01, Alice applies an H gate onto the $(j+l)$th qubit and this operation results an output state $|+\rangle$ if the input state is $|0\rangle$, or $|-\rangle$ if the input state is $|1\rangle$. On the other hand, when the key element is 10, Alice applies ZH gate onto the third qubit and the resulting output state is $|-\rangle$ corresponding to the input state $|0\rangle$, or $|+\rangle$ corresponding to the input state $|1\rangle$. The possible ciphertext states in C_4 obtained from this step are expressed as

$$|C_4\rangle = \left\{ \left[\bigotimes_{j=1}^{l} (\delta_{00,k'_j} I\otimes I + \delta_{11,k'_j} I\otimes I + \delta_{01,k'_j} I\otimes H + \delta_{10,k'_j} I\otimes (ZH)) \right] |C_3\rangle \right\}, \quad (5.5.7)$$

where I denotes the unitary matrix. Clearly, Eq.(5.5.7) indicates that the ciphertext states are nonorthogonal, and the message bits do not hide in the fixed position. Furthermore, the ciphertext space is doubled again.

After the above steps for each element are finished, the block $\mathbf{x_i}$ is encrypted. Then, other blocks are done in the same ways. Sometimes, new keys are generated using suitable transformations on the original key for different blocks. For example, using the key for ith block, one may obtain a new key $K^{i+1} = K^i P$ for the next block, i.e., $(i+1)$th block, where P is an $l \times l$ permutation matrix.

2) Decryption Algorithm

The sequence of decryption process is right inverse of that of the encryption process. Because the above quantum operations are unitary, the decryption process can be completed easily under the guidance of the pre-shared

keys. The decryption process is as follows.

Step 1: Decrypting $|C_4\rangle$ with k'. If the key element is 01, i.e., H gate is applied while encrypting, one applies the same H gate to the ciphertext while decrypting. If the key element is 10, i.e., ZH gate is applied while encrypting, one applies the HZ gate to the ciphertext while decrypting. If the key element is 00 or 11, let the ciphertext stay put.

Step 2: Decrypting $|C_3\rangle$ with k_j. If the key element is 0, leave it alone. If the key element is 1, permute the second and third qubits with the bit swap circuit.

Step 3: Decrypting $|C_2\rangle$ with k_j. The decryption is described as

$$|a\rangle|a \oplus b\rangle \rightarrow |a\rangle|a \oplus (a \oplus b)\rangle = |a\rangle|b\rangle, \tag{5.5.8}$$

where $a, b \in \{0, 1\}$ and this transformation is still a Controlled-NOT transformation. Therefore if the key element is 0, Bob applies the gate $C_{1,3}$ to the ciphertext states, otherwise he applies the gate $C_{2,3}$ to the ciphertext states.

Step 4: Decoding $|C_1\rangle$. The $2l$ bits of each quantum state in the result derived in the step 3 corresponds to initial classical message bit. Cascading all the initial classical message bits, Bob gets the bit string of plaintext.

All the quantum computations in the encryption process are under the control of the pre-shared key k. In order to speed up the encryption and decryption, one need not apply quantum operations to all the intermediate states. For example, in Step 3 of the encryption process, provided the key element is 0, no operation acts, and in Step 4 of the encryption process, provided the key element is 00 or 11, no operation functions either. Therefore, the efficiency of the proposed algorithm can still be acceptable.

3) Security analysis

Making use of the security model in Section 5.3.4, a brief security analysis is presented.

Firstly, consider the security of the ith block. According to Eq.(5.5.7), the density matrix of the final ciphertext state is given by

$$\rho_c = |C_4\rangle\langle C_4| = |C_3\rangle\langle C_3|. \tag{5.5.9}$$

For example, $|C_4\rangle = \bigotimes_{j=1}^{l}(I \otimes I)|C_3\rangle$ when $k'_j = 00$, then

$$\rho_c = \bigotimes_{j=1}^{l}(II^\dagger) \otimes (II^\dagger)|C_3\rangle\langle C_3| = |C_3\rangle\langle C_3|$$

in this situation. In addition, since

$$|C_3\rangle = P|C_2\rangle = PC_{NOT}|C_1\rangle,$$

and both the permutation operator P and the controlled-NOT operator C_{NOT} are all unitary operators which have been addressed in Section 2.2.4, one may easily get

$$\rho_c = |C_1\rangle\langle C_1| = I. \tag{5.5.10}$$

Eq.(5.5.10) demonstrates that the ciphertext in the ith block is homogeneous and includes no plaintext information.

Secondly, consider the security of the different blocks, e.g., the arbitrated ith and jth blocks. They are encrypted using same key, however, this procedure will not influence the security according to Eq.(5.5.3). Even if the plaintexts in ith and jth blocks are the same, the resulting ciphertexts are different due to the introduction of the random strings in Eq.(5.5.4). Thus, the algorithm is secure in this case.

Combing the above two situations, one finds that the proposed quantum cryptographic algorithm is perfect privacy.

5.6 Quantum Public Key Cryptosystem

The previous sections have addressed the symmetrical-key cryptosystem (SKC), the involved ciphers include the quantum Vernam cipher and quantum block cipher. They may reach unconditional security. However, there is still a drawback in engineering application. Currently, the Vernam cipher is the only one which has been proven secure in the classic cryptology, but it cannot be used efficiently in practical applications because of difficulties in the key management. Although QKD techniques provide an efficient way to solve this issue, the problem of availability of the Vernam cipher has not been completely solved since SKC cannot be used efficiently in a large communication network. For example, when a communication network system holds N communicators, at least $N(N-1)/2$ keys are necessary. Consequently, the key management becomes difficult. This drawback motivated the investigation on the so-called public-key cryptosystem (PKC).

The quantum counterpoint of the classic PKC is a quantum PKC. Although the quantum PKC has not been investigated extensively, it is still an interesting topic. This section introduces briefly the principle and typical quantum public key algorithms.

The classic PKC, which was proposed in 1978, may provide high availability for the cryptosystem. However, since the classic PKC relies on the assumption of computational complexity such as the difficulty of factoring large numbers, up-to-date none of the existing classic PKCs has been proven secure, even against an attacker with limited computational power. In addition, the rapid development of quantum computers [**?**] increasingly endangers the security of current cryptosystem. Research shows for example that a quantum computer may easily break the well-known RSA algorithm [**?**] in a short time.

The key problem of designing a public key algorithm is how to generate the secure key pairs, i.e., the public key and private key. However, in all presented QKD schemes only symmetrical keys can be generated and distributed, therefore, these protocols for the quantum key generation and distribution

can only be used in SKC but are not suitable for PKC.

Let M and C be plaintext and ciphertext, respectively, k_1, k_2 are a key pair, and E^{k_1}, D^{k_2} are the encryption operation and decryption operation, respectively. In cryptographic language, the encryption algorithm of PKC is expressed,

$$C = E^{k_1}(M), \tag{5.6.1}$$

and the decryption algorithm is

$$M = D^{k_2}(C). \tag{5.6.2}$$

Similarly, a quantum PKC could be expressed formally as

$$\rho^c = Q_E^{k_1}(\rho^m), \tag{5.6.3}$$

and the decryption algorithm is

$$\rho^m = Q_D^{k_2}(\rho^c). \tag{5.6.4}$$

where $\rho^m, \rho^c \in \mathscr{H}$ are plaintext and ciphertext, respectively, and $Q_E^{k_1}, Q_D^{k_2}$ denote the quantum encryption algorithm and quantum decryption algorithm, respectively.

The concept of PKC introduced by Diffie and Hellman [**?**] and various theories for proving the security of PKCs and related protocols (e.g., [**?**]) have been constructed based on the Turing machine (TM) model. In other words, PKCs and related theories are founded on Church's thesis, which asserts that any reasonable model of computation can be efficiently simulated on a probabilistic TM. Thus, the security of a classic PKC algorithm depends on the complexity of the employed mathematical problem. For example, security of the RSA algorithm relies on the difficulty of solving the lager-integer factorization which is a NP problem according to the classic complexity theory.

A new model of computing, i.e., the quantum TM, has been investigated since the 1980's. Several recent results provide informal evidences that the Quantum TM violates the feasible computation version of Church's thesis. The most successful result in this field was Shor's (probabilistic) polynomial time algorithms for integer factorization and discrete logarithm in the quantum TM model, since no (probabilistic) polynomial time algorithm for these problems has been found in the classical TM model. Shor's result, in particular, greatly impacted practical PKCs such as RSA, since almost all practical PKCs are constructed on integer factoring or discrete logarithm problem. Therefore, if a quantum TM is realized in the future, almost all practical PKCs will be lost.

Although these results demonstrate the positive side of the power of quantum TM, other results indicate the limitation of the power of quantum TM. Bennett, Bernstein, Brassard, and Vazirani shown that relative to an oracle chosen uniformly at random, with probability 1, class NP cannot be solved on a quantum TM in time $o(2^{n/2})$. Although this result does not rule out

the possibility that $NP \subseteq BQP$, many researchers consider that it is hard to find a probabilistic polynomial time algorithm to solve an NP-complete problem even in the quantum TM model, or conjecture that $NP \nsubseteq BQP$. This indicates that quantum PKC based on quantum TM is possible. In addition, one perhaps believes that it is possible to design an unconditionally secure quantum PKC with novel quantum characteristic, e.g., the entanglement.

The quantum computing is expected to challenge most of the cryptographic methods in use today, e.g. to break today's common asymmetric cryptographic algorithms in polynomial time. Therefore, most of the cryptographic methods in use today have to be revised. Just migrating all implementations to better methods is considered a huge task in itself, which will take years. But cryptography will be able to cope with that situation. While for symmetric algorithms a doubling of the key lengths seems to be sufficient for most applications, the situation for asymmetric algorithms is more complex. A candidate for improvements over today's RSA-algorithms is e.g. SFLASH (new version) by Patarin. Quantum public-key systems have been proposed, as well as quantum digital signatures, where the quantum state of a string of quantum bits is used as a key. There is an ongoing research project systematically investigating asymmetric cryptography methods able to resist quantum computer's attacks. Therefore, QKD, quantum public-key systems and classical cryptographic methods should not be perceived as alternatives, but as synergistic contributions to the task of ensuring secure communications under increasingly powerful attacks. In most cases, also economical and practical aspects have to be taken into account.

5.7 Typical Quantum Public-key Algorithms

Although there are few investigations on the quantum PKC, this section introduces two quantum public-key algorithms. One is based on the quantum complexity theory so that its security is computational security. Another is associated with the pure quantum laws which may reach an unconditional security.

5.7.1 Algorithm based Subset-sum Problem

The basic idea to realize the quantum PKC is to employ an appropriate NP-hard problem as an intractable primitive problem, since the concept of quantum PKC is based on the assumption, NP-complete $\nsubseteq$ BQP. Then finding the most suitable NP-hard problem is necessary. Since the algorithms to solve the subset-sum (or subset product) problem and the ways to realize public-key cryptosystems based on this problem have been extensively studied for the last 20 years, the subset-sum (or subset-product) problem has

been employed to design a quantum public key algorithm. Another promising candidate is the lattice problem, which seems to be closely related to the subset-sum problem.

There are two typical trapdoor tricks for the subset-sum or subset-product problems. One is to employ super-increasing vectors for the subset-sum and prime factorization for the subset-product. Such a tractable trapdoor vector is transformed into a public-key vector, which looks intractable. However, almost all transformation tricks from a trapdoor subset-sum or subset-product vector to another subset-sum or subset-product vector, respectively, have been cryptanalyzed due to their linearity and low density.

One promising idea for the transformation is, if computing a logarithm is feasible, to employ a non-linear transformation, exponentiation (and logarithm), that bridges the subset-sum and subset-product problems. Two typical schemes have been proposed on this type of transformation: One is the Merkle-Hellman "multiplicative" trapdoor knapsack scheme [**?**], and the other is the Chor-Rivest scheme [**?**]. Unfortunately, typical realizations of these schemes have been cryptanalyzed.

To overcome the weakness of these schemes, Okamoto and his coworkers proposed a quantum public-key algorithms which employs the ring of integers, $\mathcal{O}_K$, of an algebraic number field, $\mathbb{K}$, which is randomly selected from exponentially many candidates [**?**]. Following is a brief description on this algorithm, which is divided into three parts: key generation, encryption algorithm, and decryption.

1) Key Generation

Step 1: Fix a set $\mathscr{K}$ of algebraic number fields, available to the system.

Step 2: Randomly choose an algebraic number field, $\mathbb{K} \in \mathscr{K}$. Let $\mathcal{O}_K$ be its ring of integers.

Step 3: Fix size parameters $n, k \in \mathbb{Z}$, where $\mathbb{Z}$ denotes the integer field.

Step 4: Choose a prime ideal $\mathbf{p} \in \mathcal{O}_K$, and randomly choose an element, $g \in \mathcal{O}_K$ such that g is a generator of the multiplicative group of finite field $\mathcal{O}_K/p$. Here, an element in $\mathcal{O}_K/p$ is uniquely represented by basis $[1, \omega_2, \ldots, \omega_l]$ and integer tuple $(e_1, e_2, \ldots, e_l)$, where $e_1 = p$. That is, for any $x \in \mathcal{O}_K$, there exist rational integers $x_1, x_2, \ldots, x_l \in \mathbb{Z}$ $(0 \leq x_i < e_i)$ such that $x \equiv x_1 + x_2\omega_2 + \ldots + x_l\omega_l (\mod p)$. Note that p is the rational prime below $\mathbf{p}$.

Step 5: Choose n integers $p_1, \ldots, p_n$ from $\mathcal{O}_K/p$ with the condition that $N(p_1), \ldots, N(p_n)$ are co-prime, and for any subset $\{p_{i_1}, p_{i_2}, \ldots, p_{i_k}\}$ from $\{p_1, p_2, \ldots, p_n\}$, there exist rational integers $a_1, a_2, \ldots, a_l (0 \leq a_i < e_i)$ such that $\prod_{j=1}^{k} p_{i_j} = a_1 + a_2\omega_2 + \ldots + a_l\omega_l$.

Step 6: Use Shor's factorization algorithm for finding discrete logarithms to get $a_1, \ldots, a_n$ such that $p_i \equiv g^{a_i} (\mod p)$, where $a_i \in \mathbb{Z}/(N(p)-1)\mathbb{Z}$, and $1 \leq i \leq n$.

Step 7: Randomly choose a rational integer, $d \in \mathbb{Z}/(N(p)-1)\mathbb{Z}$.

Step 8: Compute $b_i = (a_i + d) \mod (N(p) - 1)$ for each $1 \leq i \leq n$.

Step 9: The public key is $(K, n, k, b_1, b_2, \ldots, b_n)$, and the private key is $(K, g, d, p, p_1, p_2, \ldots, p_n)$.

2) Encryption Algorithm

Step 1: Fix the length of plaintext M to $\lfloor \log \binom{n}{k} \rfloor$.

Step 2: Encode M into a binary string $m = (m_1, m_2, \ldots, m_n)$ of length n and of Hamming weight k, i.e., of having exactly k 1's, as follows:

(a) Set $l \leftarrow k$.

(b) For i from 1 to n do the following: If $M \geq \binom{n-i}{l}$ then set $m_i \leftarrow 1, M \leftarrow M - \binom{n-i}{l}, l \leftarrow l - 1$. Otherwise, set $m_i \leftarrow 0$. Notice that $\binom{l}{0} = 1$ for $l \geq 0$, and $\binom{0}{l} = 0$ for $l \geq 1$.

Step 3: Compute ciphertext c by $c = \sum_{i=1}^{n} m_i b_i$.

3) Decryption Algorithm

Step 1: Compute $r = (c - kd) \mod (N(p) - 1)$.

Step 2: Compute $u \equiv g^r \pmod{p}$.

Step 3: Find m as follows: If $p_i | u$ then set $m_i \leftarrow 1$. Otherwise, set $m_i \leftarrow 0$. After completing this procedure for all p_i's $(1 \leq i \leq n)$, set $m = (m_1, \ldots, m_n)$.

Step 4: Decode m to plaintext M as follows: (a) Set $M \leftarrow 0, l \leftarrow k$. (b) For i from 1 to n do the following: If $m_i = 1$, then set $M \leftarrow M + \binom{n-i}{l}$ and $l \leftarrow l - 1$.

5.7.2 Algorithm based Quantum Coding

The above algorithm is actually a classic public key algorithm based on the quantum computational complexity. This section presents another quantum public key algorithm which employs quantum coding techniques [21]. Similarly, the algorithm includes three stages: the key generation, encryption and decryption algorithms.

1) Key Generation

Let $\mathbf{x} = \{x_i, p(x_i) | i = 1, 2, \ldots, k\}$ be a random variable in a k-dimension real space, i.e., $\mathbf{x} \in \mathbb{R}^k$, and let $\mathscr{G}_h$ be a universal class of hash function. Choose $2k - 1$ hash function $g_j(\mathbf{x}) \in \mathscr{G}_h (j = 1, 2, \ldots, 2k - 1)$ to construct a

random variable $\mathbf{y} = \{g_j(\mathbf{x}), p[g_j(\mathbf{x})]|j = 0, 1, \ldots, 2k-1\}$ with $g_0(\mathbf{x}) = x_1$, where $p(\omega)$ denotes the probability of the variable ω. Any k-element subset of $\mathbf{y}$ is linearly independent. Then, there exists a non-singular $k \times k$ matrix P such that,

$$P \begin{pmatrix} g_{\lambda_1} \\ g_{\lambda_2} \\ \vdots \\ g_{\lambda_k} \end{pmatrix} = \begin{pmatrix} x_1 \\ g_{\lambda_{k+1}} \\ \vdots \\ g_{\lambda_{2k-1}} \end{pmatrix}, \tag{5.7.1}$$

where $(\lambda_1, \lambda_2, \ldots, \lambda_{2k})$ is an arbitrary permutation of indices $(0, 1, \ldots, 2k-1)$.

Given P one may find a unitary matrix U such that,

$$U|g_{\lambda_1}(\mathbf{x})\rangle \ldots |g_{\lambda_k}(\mathbf{x})\rangle = |P|^{1/2}|x_1\rangle|g_{\lambda_{k+1}}(\mathbf{x})\rangle \ldots |g_{\lambda_{2k-1}}(\mathbf{x})\rangle, \tag{5.7.2}$$

where elements of the matrix U are expressed by

$$\langle \mathbf{x}'|U|\mathbf{x}''\rangle = |P|^{\frac{1}{2}} \prod_{i=0}^{k-1} \delta \left(\sum_{j=0}^{k-1} P_{ij} x_j'' - x_i' \right). \tag{5.7.3}$$

In the above expression, $\langle x_i|x_j\rangle = \delta(x_i - x_j)$ and P_{ij} denotes an element of the matrix P. Eq(6.7.4) shows the matrix U depends simultaneously on the non-singular $k \times k$ matrix T and the k-dimension vector $\mathbf{x}$.

According to the above model, the public key is expressed as

$$K_p = \{g_1(\mathbf{x}), \ldots, g_{2k-1}(\mathbf{x})\}, \tag{5.7.4}$$

and the private key K_s is

$$K_s = \{x_1, x_2, \ldots, x_k\}. \tag{5.7.5}$$

2) Encryption Algorithm

Step 1: Suppose that the involved states are continuous variables. Encoding the public key to be qubit yields

$$|K_p\rangle = \{|g_1(\mathbf{x})\rangle, \ldots, |g_{2k-1}(\mathbf{x})\rangle\}. \tag{5.7.6}$$

Step 2: Encrypt the plaintext state $|\psi\rangle$ using the technique of quantum-error-correction code for continuous variable qubit. This operation generates the following $2k$-particle entanglement state,

$$|C\rangle = \int_{\mathbb{R}^k} |\psi\rangle|g_1(\mathbf{x})\rangle \ldots |g_{2k-1}(\mathbf{x})\rangle \mathrm{d}^k\mathbf{x} \tag{5.7.7}$$

3) Decryption Algorithm

Step 1: Calculate the unitary matrix U using the private key K_s.
Step 2: Decrypt the ciphertext state in following way,

$$\begin{aligned} U|C\rangle &= J|P|^{\frac{1}{2}} \int \{|\psi\rangle|x_1\rangle_{\lambda_1}|g_{\lambda_k+1}(\mathbf{x})\rangle_{\lambda_2} \ldots \times \\ &\quad |g_{\lambda_k+1}(\mathbf{x})\rangle_{\lambda_k} \ldots |g_{\lambda_{2k-1}}(\mathbf{x})\rangle_{\lambda_k}|y_{\lambda_{2k-1}}(\mathbf{x})\rangle_{\lambda_{2k-1}}\} \, \mathrm{d}\mathbf{x} \\ &= J|P|^{\frac{1}{2}}|\psi\rangle_{\lambda_1}|\Theta\rangle_{\lambda_2,\lambda_{k+1}}|\Theta\rangle_{\lambda_3,\lambda_{k+2}} \ldots |\Theta\rangle_{\lambda_k,\lambda_{2k-1}}. \end{aligned} \tag{5.7.8}$$

4) Security Analysis

Here, a simple security analysis is presented. This algorithm is clearly different from the above algorithm based on the intractable problem of subset sum. In this algorithm, the continuous-variable entanglement state is employed so that the quantum characteristics is apparent.

This algorithm is apparently secure since the following reasons. First, the public key K_p reveals no information on the private key K_s since $g(\mathbf{x})_j \in \mathscr{G}_h$ and $\mathscr{G}_h$ is a hash function in the universal class of hash function. Second, without the private key the attacker cannot obtain a suitable U subsequently the decryption procedure is impossible.

References

[1] Schneier B (1994) Applied cryptography: protocols, algorithms, and source code in C. Wiley, NewYork

[2] Diffie W, Helman M E (1976) New directions in cryptography. IEEE Transactions on Informtion Theory, 22(6): 644 – 654

[3] Rivest R L, Shamir A, Adelman L M (1978) A method for obtaining digital signature and public key cryptosystems. Communications of the ACM, 21: 120 – 126

[4] Assche G V (2006) Quantum cryptography and secret-key distillation Cambridge University Press, London

[5] Boykin P O, Roychowdhury V (2003) Optimal encryption of quantum bits. Physical Review A, 67, 042317

[6] Mosca M, Tapp A, Wolf R (2000) Private quantum channels and the cost of randomizing quantum Information, arXiv: 0003101

[7] Zhang Y, Li C, Guo G (2001) Quantum key distribution via quantum encryption, Physical Review A, 64: 024302

[8] Leung D W (2001) Quantum vernam cipher. Quantum information and computation, 1(2): 14 – 34

[9] Zeng G H, Fan J P (2001) Quantum vernam algorithm based on non-orthogonal entanglement states. XXII International Solvay Conference in Physics of Communication, Delphi, 24 – 30

[10] Beveratos A, Brouri R, Gacoin T, et al (2002) Single photon quantum cryptography. Physical Review Letters, 89: 187901/1 – 4

[11] Waks E, Inoue K, Santori C, et al (2002) Quantum cryptography with a photon turnstile. Nature, 420: 762 – 766

[12] Shannon C E (1949) Communication theory of secrecy systems. Bell System Technical Journal, 28(4): 656 – 715

[13] Deutsch D, Ekert A, Jozsa R, et al (1996) Quantum privacy amplification and the security of quantum cryptography over noisy channels. Physical Review Letters, 77: 2818 – 2821

[14] Gisin N, Ribordy G, Tittel W, et al (2002) Quantum cryptography. Reviews of Modern Physics, 74: 145 – 195

[15] Goldreich O (1997) On the foundations of modern cryptography. Advances in Cryptology-CRYPTO 97, Santa Barbara, 17 – 19 August 1997. Kaliski Jr B S (et), Lecture Notes in Computer Science (LNCS), Springer, Heidelberg, 1294: 46 – 74

[16] Naccache D, Stern J (1997) A new public-key cryptosystem. Advances in Cryptology-EUROCRYPT 97, Konstanz, 11 – 15 May 1997, pp 27 – 36

[17] Chor B, Rivest R L (1988) A knapsack-type public key cryptosystem based on arithmetic in finite fields. IEEE Transactions on Informtion Theory, 34: 901 – 909

[18] Chuang I L, Laflamme R, Shor P W, et al (1995) Quantum computers, factoring, and decoherence. Science, 270: 1633 – 1635

[19] Shor P W (1997) Polynomial-times algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on computing, 26: 1484 – 1509. Initially appear in the Proceedings of the 35th Annual Symposium on Foundations of computer Science, Los Alamos, 1994: 124 – 134

[20] Okamoto T, Tanaka K, Uchiyama S (2000) Quantum public-key cryptosystems. Advances in Cryptology-CRYPTO 2000: 20th Annual International Cryptology Conference, Santa Barbara, 20 – 24 August 2000. In: Bellare M (ed) Lecture Notes in Computer Science (LNCS). Springer Heidelberg, 1880: 147 – 165

[21] Zeng G H (2006) Quantum cryptology. Science Press, Beijing

6 Quantum Authentication

In the quantum private communication, the identity authentication, message verification, and channel authentication are involved. The identity authentication ensures authenticity of communicators, the message verification guarantees real originator and integrality of the transmitted message, and the channel authentication verifies perfectness of the employed channel. These functions can be implemented using message authentication codes, identity authentication protocols, signature schemes, or channel authentication schemes.

The confidentiality guaranteed by cryptosystems such as a symmetrical key cryptosystem or public key cryptosystem has been introduced in Chapter 5. This characteristic is a basic requirement for implementing the private communication. The authentication is another important ingredient for ensuring the creditability of the private communication. This chapter investigates fundamental principles of the quantum authentication and several typical quantum authentication schemes.

The classic message authentication code theory is introduced in this chapter since the message authentication codes have been involved in the quantum key distribution (QKD) system for ensuring the security of the authentication channel. Then the quantum identity authentication scheme, especially the quantum identity authentication combining QKD techniques are investigated. After that, the principle of the quantum signature and some important quantum schemes are presented. Finally, the so-called channel authentication is briefly introduced.

6.1 Introduction

In a private communication system, the communicator Alice transmits her private information to Bob using a proper cryptosystem. With protection of the chosen cryptographic algorithm on the private information the attacker obtains no information without keys so that the confidentiality of the private communication is ensured. However, an attacker called Oscar as usual, may benefit himself by impersonating one of two legitimate communicators, using the so-called Man-in-the-middle attack strategy as described in Chapter 4, or

changing directly a few of transmitted messages in the channel. Clearly, all these attack strategies are different from those with eavesdropping operations on the encrypted message transmitted in the secure communication channel. To prevent such kinds of strategies, authentication techniques have been employed in the classic private communication [**?**].

The authentication can be implemented not only in a classic way but also in a quantum way. If the authentication system is associated with quantum laws, it is usually called a quantum authentication [**?**]; otherwise, it is called a classic authentication [**?**]. Generally, the authentication including the quantum authentication as well as classic authentication involves two functions, i.e., the communicator's identity authentication and transmitted message verification. The identity authentication is employed to verify communicators' identities so that the forgery attack may be against in the private communication system. While the message verification is used for verifying the originator or the integrality of the transmitted message. In the quantum private communication, except for the identity verification and message verification there is a novel characteristic, i.e., the channel authentication, which is applied to verify the perfectness of the employed quantum channel in quantum private communication. Note, the channel authentication is always associated with an authenticated channel. Such channel has been adopted in the QKD schemes which have been discussed in Chapter 4.

By far, a number of authentication schemes have been presented. The proposed authentication schemes include the message authentication code [3 – 6], identity authentication protocol [7 – 13], signature scheme [14 – 17], and channel authentication protocol [**?**, **?**]. The message authentication code is usually employed for the identity authentication and message verification, but it is only a theoretical model which is theorized with Simon authentication theory. In practices, the identity verification is always guaranteed by the identity authentication protocol. All the symmetrical-key algorithms and parts of the public-key algorithms may be employed for the identity authentication. The signature scheme is usually used for the message verification, although it might also be employed for the identity authentication. Generally, signature schemes are divided into two categories, i.e., the true signature scheme and the arbitrated signature scheme. Since a trustable arbitrator is necessary in the arbitrated quantum signature scheme, there are a few limitations for this kind of signature schemes in practical applications. A more popular signature scheme is the true signature scheme. In this category, the signature algorithm and verification algorithm are executed independently by the signatory and receiver, respectively. The channel authentication protocol is employed to verify the perfectness of the communication channel. Consequently, using channel authentication schemes communicators may detect the eavesdropping operations which influence the channel perfectness. Clearly, it is impossible for channel authentication in the classic scenario. The channel authentication has been widely used in the QKD scheme. As an independent cryptography scheme, however, there are few investigations on this issue.

In the modern cryptology, the authentication scheme is always associated with cryptographic algorithms. If the authentication scheme is designed based on a symmetrical-key cryptosystem, such kind of schemes is called the symmetrical-key authentication scheme, otherwise, it is called the asymmetrical-key authentication scheme. Generally, to ensure the confidentiality the symmetrical-key cryptosystem is always adopted in the classic secure communication system since its fast computational speed, so that the encryption and decryption procedures do not burden the cost of the communication network. While the authentication schemes are always associated with the asymmetrical-key cryptosystem due to the availability of such kind of algorithms.

According to requirements in practical applications, there are one-way authentication and two-way authentication. In a private communication system, if only one part needs to be verified, the authentication scheme is called the one-way authentication protocol; otherwise, it is called the two-way authentication scheme. Both the one-way authentication and two-way authentication have been widely applied in practical systems, especially in the communication network.

6.2 Authentication Theory

Since the authentication theory model was first proposed by Simmons [**?**, **?**], various authentication schemes and implementation techniques have been developed quickly [**?**]. Currently, the authentication has become an important ingredient for ensuring the private communication. Commonly, there are three categories authentication systems, including communicator's identity authentication, message verification, and channel perfectness authentication which exists only in the quantum scenario. To implement these functions, various authentication techniques including the message authentication code, identity verification protocol, signature scheme, and channel authentication scheme are presented. Generally, if the employed scheme is implemented technically in the classic physics way, the corresponding scheme is called the classic authentication scheme, otherwise, it is called the quantum authentication scheme.

6.2.1 Authentication Categories

In the private communication, three aspects including the identity authentication, message verification, and channel authentication are always involved. The details on these notions are described in this subsection.

1) Identity Authentication

Why the identity authentication is needed in the private communication is because there exist many frauds in practices, such as the chess Grandmaster problem, Mafia fraud, multiple identity fraud, etc. To prevent such kind of attacks, one has to verify participants' legitimate identities so that these forgeries are prevented in the private communication. Generally, an identity authentication system involved three participants, i.e., a prover, a verifier, and an attacker. In some cases, a trustable arbitrator or certification authority (CA) needs to be involved for judging arguments among communicators. Mathematically, the identity authentication system is defined as follows.

Definition 6.2.1 An identity authentication system is a tri-tuple, i.e., $\{\mathscr{I}, \mathscr{T}, \mathscr{D}\}$, where $\mathscr{I}$ denotes a set of possible personal information of the prover, $\mathscr{T}$ is a family of information processing system, and $\mathscr{D}$ represents a set of possible database which stores the prover's personal information.

If communicators Alice and Bob are mutual verifiers, the identity authentication is a two-way authentication system. Otherwise, it is a one-way identity authentication system.

There are many tools for the identity authentication, such as the password system, certificate system, fingerprint-recognition system, face-recognition system, digital watermark system, etc. Generally, there are two kinds identity authentication. One is the identity verification and another is the identity recognition. For example, both the fingerprint-recognition system and the face-recognition system are all identity recognition systems. This book focuses on the identity authentication scheme associated with the cryptographic algorithm.

To verify communicator's legitimate identities the cryptographic algorithms are always employed in a private communication system. If using the symmetrical-key cryptosystem, the communicators Alice and Bob should pre-share a short authentication key. This key may be generated using QKD techniques. Actually, as mentioned in Chapter 3, a secure QKD system needs a classic authenticated channel. With the authentication procedure the QKD system is actually a key expansion system since a short key should be pre-shared for the identity authentication.

In most of the identity authentication systems, communicators know each other their personal information used for authentication after the communicators have finished the identity authentication processing. In some situations, however, the prover wants not to show his personal information to the verifier, to reach this aim the zero-knowledge proof problem is always adopted. Here, the so-called zero-knowledge proof problem is described as follows: the prover adopts a proper encoding rule to encode his personal information so that it may not leak to anyone including Bob, but Bob can verify each operation so that Bob believes Alice knows the proof. The zero-knowledge proof problem is divided into the minimum disclosure proof and the zero knowledge proof.

2) Message Verification

The identity verification is associated with the authenticity verification of prover's personal information, while the message authentication system focuses on the verification of originator or integrality of the transmitted message so that the revisions, forgery, and delay of the transmitted message in the secure communication are prevented. In short, the identity authentication focuses on the authenticity of participants' identities, while the message authentication regards the reliability of message. Clearly, the identity authentication is associated with the communicators' personal information such as password, private key, etc. But the message verification is associated with the message itself. Thus, one may use the original message to generate an authentication code so that the verifier may check the originator or integrality using the generated authentication code. Mathematically, a message verification system may be defined as follows.

Definition 6.2.2 A message verification system is a tri-tuple $\{\mathscr{M}, \mathscr{G}, \mathscr{V}\}$, where $\mathscr{M}$ is the message, $\mathscr{G}$ represents approaches of generating authentication code and $\mathscr{V}$ denotes the verification approach.

From the above definition, the key problem in the message verification is how to generate the authentication code. Technically, the message verification may be implemented using many ways, such as the message authentication code (MAC) scheme and signature scheme. In the message authentication code scheme, the authentication code is the well known MAC which is generated using encoding rules like the error-correction code or hash function. In the digital signature scheme, the signature is actually a kind of the authentication code.

3) Channel Authentication

Consider a scenario: Alice and Bob are communicating, simultaneously, they want to know whether the employed channel is perfect or not, how to do it? This issue is essentially associated with how to check the perfectness of the involved communication channel, i.e., the channel authentication. The novel uncertainty characteristics of qubits, which follows the well-known Heisenberg uncertainty principle, ensures the quantum channel authentication so that communicators may judge whether the attacker is online or not.

One may find that the channel authentication focuses on the perfectness verification of the involved communication channel. It is clearly different from the identity authentication and message verification. Exactly, we note that the channel authentication relates to the online eavesdropping detection and the perfectness verification of the communication channel. While the identity authentication and the message verification focus on the authenticity of the communicators' identities and integrality of the received message, respectively. Thus they are associated with different mechanisms.

Definition 6.2.3 A channel authentication is a tri-tuple $\{\mathscr{C}, \mathscr{D}, \xi\}$, where $\mathscr{C}$ is the involved communication channel, $\mathscr{D}$ represents the adopted

detection approaches including both the quantum and classic method, and ξ denotes the threshold for perfectness of the involved channel $\mathscr{C}$.

A main application of the channel authentication scheme is for online eavesdropping detection so that communicators can find the eavesdropping attacks when they are communicating. This is, obviously, very useful in the private communication. Unfortunately, there is no way by far to reach this aim in the classic secure communication. However, it becomes easy in the quantum private communication since the novel property of some quantum laws such as the Heisenberg uncertainty principle.

6.2.2 Security Model

1) Security Requirements

Generally, an authentication system involves usually three participants: the sender Alice, the receiver Bob and the attacker Oscar. Sometime, a fourth participant called arbitrator or CA is participated for judging arguments. Because a kind of different attack strategies is associated in the authentication system, the attacker is denoted "Oscar" instead of "Eve". In Chapter 5, the aim is to ensure the confidentiality of the private communication. In order to obtain the confidentiality of the information, the attacker has to eavesdrop on the channel so that he can benefit himself. In such situation, the involved attack strategy is called passive attack since the attacker can passively join the communication system. However, the attacker may change the transmitted message via the impersonation or substitution ways which must be prevented using authentication techniques. Therefore, the involved attack strategy is called an active attack.

The aim of the authentication is to ensure the legitimate communicators and creditability of the message. To reach this aim, a secure authentication system should satisfy the following general requirements:

- Verifiability: Legitimate receivers may check and verify the authenticity of the message, and communicators may verify each other their authentic identities without leakiness of their private personal information.
- No disavowals: Any communicator may not successfully disavow what he/she sends, and what he/she received.
- No forgery: Neither a receiver nor a possible attacker are able to forge the legitimate message so that the attack is succeeded.
- Judgement: When necessary, an arbitrator or CA may take part in the communication procedures and make a fair judgement for the argument.

These requirements provide a general rule for reaching a secure authentication system. However, how to design available authentication schemes is not demonstrated. This gives rise to the diversity of the authentication schemes.

2) Security Theory

Generally, there are two kinds of attack strategies for an authentication scheme, i.e., impersonation fraudulent and substitute fraudulent. The first one is called the impersonation attack. This attack may be stated as follows. After seeing t messages, e.g., from m_1 to m_t, the attacker (Oscar) creates an optimal message m'_{t+1} in himself ways. With the created message the attacker makes the receiver believe that the received message is legitimate in maximal probability. If the receiver accepts the message including the impersonation message m'_{t+1}, the attack is succeeded. The second one is called the substitution attack. In this attack, Oscar modifies a message m_t and replaces it with him own message m'_t after seeing t messages m_1 to m_t. With this substitution, the attacker tries to let the message be accepted by the receiver as legitimate. If the receiver accepts the message including the substitution m'_t, the attack is succeeded.

Denote maximal success probabilities for these two attack strategies by p_I and p_d, respectively. Then one may define the maximal success probability p_d for tamper's attack strategy,

$$p_d = \max\{p_I, p_s\}. \tag{6.2.1}$$

Similar to the security model for the confidentiality, there are also unconditional security and computational security for an authentication system. To reach perfect authentication, i.e., an authentication with unconditional security, the p_d should follow the Gilbert's bound which is described using the following theorem.

Theorem 6.3.1 For any authentication system with an unconditional security, the success probability p_d of tamper's attacks should satisfy the following conditions,

$$p_d \geq \frac{1}{\sqrt{\#\{\mathscr{K}\}}}, \tag{6.2.2}$$

where $\#\{\mathscr{K}\}$ denotes the element number with a nonzero probability in the key space $\mathscr{K}$.

Theorem 6.3.1 demonstrates that the necessary key number in an authentication system with unconditional security is at least $1/p_d^2$.

The security theory for channel authentication is different from the above security model. Since the channel authentication has been introduced in Chapter 4, here is not repeated again.

6.3 Message Authentication Code

In the previous section a supper bound of p_d for the unconditionally secure authentication system has been presented. This section shows how to reach this bound. An optimal candidate is the authentication code. There are many

approaches for designing the authentication code. This section introduces two approaches. One is associated with the encoding technique and another is based on the well-known hash function.

6.3.1 Encoding Approach

Motivated by the error-correction code, the authentication code has been investigated. Technically, using cryptographic approaches, one may create the redundancy information on the original message. This redundancy may be employed in the identity authentication and message verification. The involved approach is called the message authentication code (MAC) scheme. The created redundancy information is called the authenticator. This kind authentication scheme may reach the unconditional security, which has been suggested to apply in the QKD scheme.

More precisely, suppose that arbitrated two communicators Alice and Bob in a communication network pre-share a short key. In terms of the message content, the redundancy information is created using appropriate encoding rules with the pre-shared key. Then the redundancy is added to the original message for the authentication. Such kind of schemes is called the authentication code scheme. The redundancy information added to the original message is called the message authentication code or authenticator. Mathematically, the MAC is defined as follows,

$$y = (m|MAC_k(m)), \tag{6.3.1}$$

where $m,\ y,\ k$, and MAC denote the original message, output of the original message with an authenticator, a pre-shared key, and an authenticator, respectively. Obviously, from the viewpoint of the authentication, the original message may be public. This is different from the confidentiality protection where the message must be secret. Since the communicators' personal information, i.e., the private key k, and the message content m are associated, the MAC scheme may be employed for the identity authentication and message verification.

6.3.2 Hash Function Approach

The hash function has been employed in the QKD scheme for the privacy amplification. Actually, the hash function has been extensively applied in the classic cryptology, especially for the authentication aim. The hash function is a one-way function. Mathematically, a hash function is defined as follows. Given a map $h : y = h(x)$, if the output y may be easily computed with the input x but the vice versa is difficult or impossible, then h is a hash function.

Suppose that communicators Alice and Bob pre-share an authentication key k. Given a hash function h which is controlled under the key, then one may create a MAC, i.e.,

$$MAC(m) = h_k(m), \tag{6.3.2}$$

where m denotes the input message.

In most cases, the adopted hash function is computational security. However, for the unconditional security QKD system, one has to choose a hash function with an unconditional security. For this aim, the so-called strongly universal family for hash functions was suggested. This notion is defined exactly as follows.

Definition 6.3.1 Given two sets $\mathscr{A}$ and $\mathscr{B}$, a class $\mathscr{G}$ of functions $\mathscr{A} \to \mathscr{B}$ is $\epsilon/|\mathscr{B}|$-almost strongly 2-universal if the following two conditions are satisfied:

(1) for any $x_1 \in \mathscr{A}$ and any $y_1 \in \mathscr{B}$, the size of the set $\{h \in \mathscr{G} : h(x_1) = y_1\}$ is at most $|\mathscr{G}|/|\mathscr{B}|$;

(2) for any $x_1 \neq x_2 \in \mathscr{A}$ and any $y_1, y_2 \in \mathscr{B}$, the size of the set $\{h \in \mathscr{G} : h(x_1) = y_1 \wedge h(x_2) = y_2\}$ is at most $\epsilon|\mathscr{G}|/|\mathscr{B}|^2$.

If the last condition is satisfied for $\epsilon = 1$, the class is simply called strongly 2-universal.

As an example, a strongly 2-universal family of hash function is given as follows. Let $\mathscr{A} = GF(2^a)$ and $\mathscr{B} = \{0,1\}^b$. Let $h_{c,d}(x)$ be defined as the first b bits of the affine function $cx + d$ in a polynomial representation of $GF(2^a)$. The set $\mathscr{G}^{(1)}_{GF(2^a)\to\{0,1\}^b} = \{h_{c,d} : c, d \in GF(2^a)\}$ is a strongly 2-universal family of hash function [**?**].

6.4 Quantum Identity Authentication

Many quantum identity authentication (QIA) schemes have been presented. Of the most interesting schemes are those of combining QIA with QKD techniques. This section exemplifies a one-way QIA scheme between two parties [**?**], i.e., a reliable CA named Alice and a common user called Bob. In this scheme, Bob's identity needs to be verified when he communicates with Alice, or logins in a network where Alice is an authentication center [**?**].

6.4.1 Scheme Description

According to the general model for identity authentication, to implement QIA an authentication key is necessary. Generally, the employed authentication key may be a classic key or quantum key. Suppose that Alice and Bob have shared a binary key $k_a = \{k_1, k_2, \ldots, k_{2n}\}$ as the authentication key. Since

Alice is a reliable CA, only Bob's identity needs to be verified. The protocol executes the following steps.

Step 1: Preparing an EPR pair by the reliable CA. Alice generates two particles h and t in the following state,

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0_h 0_t\rangle + |1_h 1_t\rangle). \tag{6.4.1}$$

The home particle h is kept in Alice's laboratory while the traveling particle t is sent to Bob.

Step 2: Encoding the secret authentication information on photon by user's operations. Having received the traveling particle t, the user, Bob, prepares a new particle m (information particle) in the state,

$$|\phi_m\rangle = |k_{2i-1} \oplus k_{2i}\rangle, \tag{6.4.2}$$

where $1 \leq i \leq n$, the symbol $\oplus$ denotes modular 2 plus. Applying a quantum controlled-NOT gate on the traveling particle and the information particle creates a tri-particle entanglement state,

$$|\Phi_w\rangle = C_p(|\Psi\rangle \otimes |\phi_m\rangle), \tag{6.4.3}$$

where $C_p = C_0$ at $k_{2i-1} = 0$ and $C_p = C_1$ at $k_{2i-1} = 1$. C_0 and C_1 are defined as follows,

$$\begin{cases} C_0 = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes \sigma_x, \\ C_1 = |+\rangle\langle +| \otimes I + |-\rangle\langle -| \otimes \sigma_x. \end{cases} \tag{6.4.4}$$

After above operations, Bob preserves particle t and returns particle m to Alice. We note here that the particle t will be returned to Alice in ping-pong ways like that in the QKD schemes [**?**, **?**], while it is kept by Bob and a new particle is returned to Alice in this scheme. Subsequently, the proposed scheme may be called as a revised ping-pong scheme.

Step 3: Decoding the state of particle m by CA. After receiving the particle m, Alice applies a quantum controlled-NOT gate C_p on the particles h and m. This operation gives

$$|\Phi'_w\rangle = C_p|\Phi_w\rangle = |\Psi\rangle \otimes |\phi_m\rangle. \tag{6.4.5}$$

Step 4: Verifying the identification of user. Having obtained the state $|\phi_m\rangle$, Alice measures particle m in the basis σ_z. The measurement result can either be 0 or 1. For a legitimate user, the measurement result must be $|k_{2i-1} \oplus k_{2i}\rangle$. If the measurement results in accord with the authentication key, i increases 1 and two communicators return to Step 1 to authenticate next two key bits. If all the key bits have been authenticated, the user's identity is true.

Step 5: Updating the authentication key. After the authentication of two bits, i.e., $k_{2i-1}k_{2i}$, Alice and Bob update the two bits, denoted $k'_{2i-1}k'_{2i}$. Since the home particle h and the traveling particle t, which are kept secretly by Alice and Bob after the identity authentication, are in a maximally entangled state $|\Psi\rangle$, Alice and Bob's measurement results on home and travel particle are correlated. The first key bit k'_{2i-1} can be obtained by measuring the state $|\Psi\rangle$. The approach is described as follows. Bob measures the particle t in basis σ_z, then the measurement result is just the bit k'_{2i-1} in the updated key. Since Alice creates initially the state $|\Psi\rangle$, she knows exactly this key bit by measuring the home particle h. The second key bit, say k'_{2i}, is determined by the first two bits of the old key and k'_{2i-1},

$$k'_{2i} = k_{2i-1} \oplus k_{2i} \oplus k'_{2i-1}. \tag{6.4.6}$$

Obviously, even if the attacker (Oscar) has obtained the old key, he cannot obtain the new key. Consequently, the security is strengthened.

6.4.2 Security Analysis

The security requirement of the QIA scheme is different from that of the QKD scheme which has been analyzed in Chapter 4. Accordingly, details for the security analysis is presented in this subsection. According to the Simmons theory [**?**], there are two kinds of attack strategies in the QIA scheme. First, attackers may try to pass the identity authentication by forging a new qubit without the authentication key, which may be called the impersonated fraudulent attack. Second, the attacker may try to obtain the authentication key so that he can impersonate Bob, which may be called the substitution fraudulent attack.

1) Impersonated Fraudulent Attack Strategy

To impersonate Bob, an optimal attack strategy for Oscar is to operate the traveling particle t transmitted from Alice to Bob. Suppose that Oscar employs a general operation on the traveling particle, which are denoted as follows,

$$\begin{cases} |0_t\chi\rangle \to a_0|0_t0_e\rangle + b_0|0_t1_e\rangle + c_0|1_t0_e\rangle + d_0|1_t1_e\rangle, \\ |1_t\chi\rangle \to a_1|0_t0_e\rangle + b_1|0_t1_e\rangle + c_1|1_t0_e\rangle + d_1|1_t1_e\rangle, \end{cases} \tag{6.4.7}$$

where $|\chi\rangle$ is an ancillary state created by Oscar, $|a_0|^2 + |b_0|^2 + |c_0|^2 + |d_0|^2 = |a_1|^2 + |b_1|^2 + |c_1|^2 + |d_1|^2 = 1$, the subscript e refers to Oscar's state.

Oscar's operation creates a new state, i.e., $|\Psi\rangle \to |\Psi'\rangle$. This state is given

by

$$|\Psi'\rangle = \frac{1}{\sqrt{2}}(a_0|0_h0_t0_e\rangle + b_0|0_h0_t1_e\rangle + c_0|0_h1_t0_e\rangle + d_0|0_h1_t1_e\rangle + a_1|1_h0_t0_e\rangle + b_1|1_h0_t1_e\rangle + c_1|1_h1_t0_e\rangle + d_1|1_h1_t1_e\rangle). \quad (6.4.8)$$

Then Oscar sends an ancillary particle to Alice. There are four possible outputs after Alice's controlled-NOT operation, i.e., $|\Psi_{00}\rangle$, $|\Psi_{01}\rangle$, $|\Psi_{10}\rangle$ and $|\Psi_{11}\rangle$, which corresponds to the two-bit key $00, 01, 10, 11$, respectively. For example, when the two-bit key is 00, Alice's operation gives $|\Psi_{00}\rangle = C_0|\Psi'\rangle$, which is obtained by

$$|\Psi_{00}\rangle = \frac{1}{\sqrt{2}}(a_0|0_h0_t0_e\rangle + b_0|0_h0_t1_e\rangle + c_0|0_h1_t0_e\rangle + d_0|0_h1_t1_e\rangle + a_1|1_h0_t1_e\rangle + b_1|1_h0_t0_e\rangle + c_1|1_h1_t1_e\rangle + d_1|1_h1_t0_e\rangle). \quad (6.4.9)$$

Thus the probability of detecting Oscar, P_{00}, can be calculated from Eq. (6.4.9) in this situation,

$$P_{00} = \frac{1}{2}\left(|a_1|^2 + |c_1|^2 + |b_0|^2 + |d_0|^2\right). \quad (6.4.10)$$

Similarly, P_{01}, P_{10}, and P_{11} are given by

$$P_{01} = P_{10} = \frac{1}{2}\left(|a_0|^2 + |c_0|^2 + |b_1|^2 + |d_1|^2\right), \quad (6.4.11)$$

$$P_{11} = P_{00}. \quad (6.4.12)$$

Consequently, the detection possibility for each communication reads as

$$P_d = \frac{1}{4}\left(P_{00} + P_{01} + P_{10} + P_{11}\right) = \frac{1}{2}. \quad (6.4.13)$$

According to the Simmons theory, Eq.(6.4.13) shows the proposed protocol is unconditionally secure under the impersonated fraudulent attack strategy.

2) Substitution Fraudulent Attack Strategy

To perform the substitution fraudulent attack, the attacker should know the authentication key k_a. Generally, there exist two kinds of attacks for distilling information on the authentication key, i.e., measuring directly channel particles, which are transmitted from Alice to Bob, or attacking the two-way channel of the scheme.

First, consider the attack strategy of direct measurement on channel particles. Since the traveling particle t from Alice to Bob carries no information on the authentication key, only the returned particle m from Bob to Alice needs to be considered in this kind of attacks. According to the Holevo theorem [**?**], the maximal accessible information that Oscar may extract from a quantum channel is

$$\chi(\rho) = S(\rho) - \sum_i P_i S(\rho_i), \quad (6.4.14)$$

where $S(\rho) = -Tr(\rho \log_2 \rho)$ is the Von Neumann entropy, ρ_i is a component in the mixed state ρ, and P_i is the probability of ρ_i in ρ.

Since the attacker has the only access to particle m, $\chi(\rho)$ depends on the reduced density matrix of particle m. Eq.(6.4.14) is rewritten as

$$\chi(\rho_m) = S(\rho_m) - \sum_i P_i S(\rho_{m_i}), \tag{6.4.15}$$

where ρ_m and ρ_{m_i} are reduced density matrixes of ρ and ρ_i, respectively. Whatever the key is, the reduced density matrix for particle m is always in the form,

$$\rho_m = Tr_{ht}(|\Phi_w\rangle\langle\Phi_w|) = \frac{1}{2}I, \tag{6.4.16}$$

and ρ_{m_i} corresponds to the following states,

$$\begin{cases} |\Phi_w^{00}\rangle = \frac{1}{\sqrt{2}}(|0_h 0_t 0_m\rangle + |1_h 1_t 1_m\rangle), \\ |\Phi_w^{01}\rangle = \frac{1}{\sqrt{2}}(|0_h 0_t 1_m\rangle + |1_h 1_t 0_m\rangle), \\ |\Phi_w^{10}\rangle = \frac{1}{\sqrt{2}}(|+_h +_t 1_m\rangle + |-_h -_t 0_m\rangle), \\ |\Phi_w^{11}\rangle = \frac{1}{\sqrt{2}}(|+_h +_t 0_m\rangle + |-_h -_t 1_m\rangle). \end{cases} \tag{6.4.17}$$

Thus $\rho_{m_i} = Tr_{ht}(|\Psi_w^i\rangle\langle\Psi_w^i|) = \frac{1}{2}I$. Substituting ρ_m and ρ_{m_i} into Eq.(6.4.15) gives

$$\chi(\rho_m) = 0, \tag{6.4.18}$$

which means the attacker gets no information on the key in the direct measurement attack from the particle m.

Then, consider the attack strategy on the two-way channel. The attacker may attack the two-way channel to obtain the information on the authentication key. At first, the attacker intercepts the traveling particle from Alice and performs an operation E_1 on both the traveling particle and *ancilla* ε. After this operation, the attacker sends the traveling particle to Bob. When Bob receives the traveling particle, he performs operations as usual since he does not know the attacker's operations. After intercepts the information particle returned by Bob, the attacker performs another operation E_2 on the information particle and the *ancilla* η. By employing the obtained results from ε and η, the attacker tries to achieve some information on the two-bit key. However, not only no key bits are disclosed to the attacker, but also Alice and Bob can detect the attacker's disturbance. The whole procedure of the attack strategy is plotted in Fig.6.1.

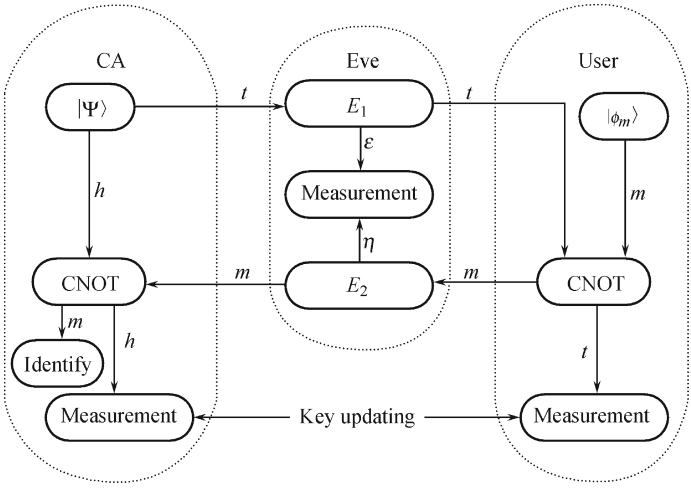

Fig. 6.1. Oscar's attack strategy and process of identification

Attacker's operation E_1 on the traveling particle t can be described in a general presentation,

$$\begin{cases} |0_t\varepsilon\rangle \rightarrow A_\varepsilon|0_t\varepsilon_{00}\rangle + B_\varepsilon|1_t\varepsilon_{01}\rangle, \\ |1_t\varepsilon\rangle \rightarrow B_\varepsilon|0_t\varepsilon_{10}\rangle + A_\varepsilon|1_t\varepsilon_{11}\rangle, \\ |+_t\,\varepsilon\rangle \rightarrow \dfrac{1}{2}|+_t\rangle\left(A_\varepsilon|\varepsilon_{00}\rangle + A_\varepsilon|\varepsilon_{11}\rangle + B_\varepsilon|\varepsilon_{01}\rangle + B_\varepsilon|\varepsilon_{10}\rangle\right) \\ \qquad\qquad + \dfrac{1}{2}|-_t\rangle\left(A_\varepsilon|\varepsilon_{00}\rangle - A_\varepsilon|\varepsilon_{11}\rangle - B_\varepsilon|\varepsilon_{01}\rangle + B_\varepsilon|\varepsilon_{10}\rangle\right), \\ |-_t\,\varepsilon\rangle \rightarrow \dfrac{1}{2}|+_t\rangle\left(A_\varepsilon|\varepsilon_{00}\rangle - A_\varepsilon|\varepsilon_{11}\rangle + B_\varepsilon|\varepsilon_{01}\rangle - B_\varepsilon|\varepsilon_{10}\rangle\right) \\ \qquad\qquad + \dfrac{1}{2}|-_t\rangle\left(A_\varepsilon|\varepsilon_{00}\rangle + A_\varepsilon|\varepsilon_{11}\rangle - B_\varepsilon|\varepsilon_{01}\rangle - B_\varepsilon|\varepsilon_{10}\rangle\right). \end{cases} \tag{6.4.19}$$

Similarly, attacker's operation E_2 on the information particle can be expressed as

$$\begin{cases} |0_m\eta\rangle \rightarrow A_\eta\,|0_m\eta_{00}\rangle + B_\eta\,|1_m\eta_{01}\rangle\,, \\ |1_m\eta\rangle \rightarrow B_\eta\,|0_m\eta_{10}\rangle + A_\eta\,|1_m\eta_{11}\rangle\,. \end{cases} \tag{6.4.20}$$

A unitary operation requires $A_\varepsilon^2 + B_\varepsilon^2 = 1, A_\eta^2 + B_\eta^2 = 1, \langle\varepsilon_{00}\varepsilon_{10}\rangle + \langle\varepsilon_{01}|\varepsilon_{11}\rangle = 0$ and $\langle\eta_{00}|\eta_{10}\rangle + \langle\eta_{01}|\eta_{11}\rangle = 0$. To simplify the discussion, assume $\langle\varepsilon_{00}|\ \varepsilon_{01}\rangle = \langle\varepsilon_{10}\mid\ \varepsilon_{11}\rangle = \langle\varepsilon_{00}\mid\ \varepsilon_{10}\rangle = \langle\varepsilon_{01}\mid\varepsilon_{11}\rangle = 0$ and $\langle\eta_{00}|\ \eta_{01}\rangle = \langle\eta_{10}\mid\eta_{11}\rangle = \langle\eta_{00}\mid\ \eta_{10}\rangle = \langle\eta_{01}\mid\eta_{11}\rangle = 0$. Although this simplification eliminates the generality of Oscar's operation, it still preserves the most representative states after Oscar's operation. For those non-orthogonal states,

suppose $\langle\varepsilon_{00} \mid \varepsilon_{11}\rangle = \cos\theta_\varepsilon, \langle\varepsilon_{01} \mid \varepsilon_{10}\rangle = \cos\varphi_\varepsilon, \langle\eta_{00} \mid \eta_{11}\rangle = \cos\theta_\eta$ and $\langle\eta_{01} \mid \eta_{10}\rangle = \cos\varphi_\eta$. When $k_i k_{i+1} = 00$, CA's decoding gives

$$\begin{aligned}|\Psi_e^{00}\rangle &= C_0 E_2\{C_0[E_1(|\Psi\rangle|\varepsilon\rangle)|\phi_m\rangle]|\eta\rangle\} \\ &= \frac{1}{\sqrt{2}}(A_\varepsilon A_\eta|0_h 0_t 0_m \varepsilon_{00}\eta_{00}\rangle + A_\varepsilon B_\eta|0_h 0_t 1_m \varepsilon_{00}\eta_{01}\rangle + \\ &\quad B_\varepsilon B_\eta|0_h 1_t 0_m \varepsilon_{01}\eta_{10}\rangle + B_\varepsilon A_\eta|0_h 1_t 1_m \varepsilon_{01}\eta_{11}\rangle + \\ &\quad B_\varepsilon A_\eta|1_h 0_t 1_m \varepsilon_{10}\eta_{00}\rangle + B_\varepsilon B_\eta|1_h 0_t 0_m \varepsilon_{10}\eta_{01}\rangle + \\ &\quad A_\varepsilon B_\eta|1_h 1_t 1_m \varepsilon_{11}\eta_{10}\rangle + A_\varepsilon A_\eta|1_h 1_t 0_m \varepsilon_{11}\eta_{11}\rangle). \end{aligned} \tag{6.4.21}$$

Oscar will be detected if the state of information particle is not $|0_m\rangle$. In such case, the probability of detecting Oscar reads as

$$P_d(k_i = 0) = (A_\varepsilon B_\eta)^2 + (B_\varepsilon A_\eta)^2. \tag{6.4.22}$$

Further calculations show the detection probability also satisfies Eq.(6.4.22) when $k_i k_{i+1} = 01$. In the same way, the probability of detecting Oscar when $k_i = 1 (k_{i+1} \in \{0, 1\})$ is given by

$$\begin{aligned}P_d(k_i = 1) = \frac{1}{2}[&(A_\varepsilon B_\eta)^2(1 + \cos\theta_\varepsilon) + (B_\varepsilon B_\eta)^2(1 + \cos\varphi_\varepsilon) + \\ &(A_\varepsilon A_\eta)^2(1 - \cos\theta_\varepsilon) + (B_\varepsilon A_\eta)(1 - \cos\varphi_\varepsilon)]. \end{aligned} \tag{6.4.23}$$

Combining Eqs.(6.4.22) and (6.4.23) gives the total detection probability in the authentication process,

$$P_d = \frac{1}{2}[P_d(k_i = 0) + P_d(k_i = 1)]. \tag{6.4.24}$$

In order to lower the possibility to be detected, Oscar should make P_d be minimal. Denote d the minimal detection possibility, it can be easily calculated from Eq.(6.4.24) in the condition of $A_\varepsilon = A_\eta = 1$,

$$d \equiv \min(P_d) = \frac{1}{4}(1 - \cos\theta_\varepsilon). \tag{6.4.25}$$

Above equation shows the minimal detection probability is independent of θ_η. Consequently, Oscar may choose a best strategy at the operation E_2 so that η_{00} and η_{11} can be distinguished.

Attacker's operations at the positions E_1 and E_2 consist of an attack strategy $\mathcal{E}$, and therefore attacker's information on the two-bit key under the attack strategy $\mathcal{E}$ is given by

$$I(K, \mathcal{E}) \equiv \sum_{x,y} P(K, \mathcal{E}) \log_2 \frac{P(K, \mathcal{E})}{P(K)P(\mathcal{E})}, \tag{6.4.26}$$

where x is the two-bit key, i.e., $x \in \{00, 01, 10, 11\}$, K denotes the random variable of the two-bit key x, and y is the joint measurement results of Oscar at the positions E_1 and E_2, i.e., $y = \varepsilon_{ij}\eta_{\mu\nu}$ with $i, j, \mu, \nu \in \{0, 1\}$.

Since $P(K,\mathcal{E}) = P(K)P(\mathcal{E}|K)$, to obtain $I(K,\mathcal{E})$ one only needs to calculate $p(K)$ and $P(\mathcal{E}|K)$. Obviously, $P(x) = 1/4$. Regarding the conditional probability $P(\mathcal{E}|K)$, the special case of $P(\varepsilon_{00}\eta_{00}|00)$ is calculated, as an example, in the follows. In the condition with the minimal detection probability, which corresponds to a special attack strategy, Eq.(6.4.21) is simplified as

$$|\Psi_e^{00}\rangle = \frac{1}{\sqrt{2}}(|0_h 0_t 0_m \varepsilon_{00}\eta_{00}\rangle + |1_h 1_t 0_m \varepsilon_{11}\eta_{11}\rangle). \tag{6.4.27}$$

Above equation shows attacker's measurement result is either $\varepsilon_{00}\eta_{00}$ or $\varepsilon_{11}\eta_{11}$ with the same possibility $1/2$ when $k_{2i-1}k_{2i} = 00$. Since $\langle\varepsilon_{00} \mid \varepsilon_{11}\rangle = \cos\theta_\varepsilon$, there is an inconclusive result with a probability of $(1+\sin\theta_\varepsilon)/2$ in attacker's measurement results [**?**], i.e., $P(\varepsilon_{00}\eta_{00}|00) = (1+\sin\theta_\varepsilon)/2$. Thus, one has

$$P(00, \varepsilon_{00}\eta_{00}) = P(00)P(\varepsilon_{00}\eta_{00}|00) = \frac{1+\sin\theta_\varepsilon}{8}. \tag{6.4.28}$$

Similarly, attacker's measurement result is either $\varepsilon_{00}\eta_{11}$ or $\varepsilon_{11}\eta_{00}$ when $k_{2i-1}k_{2i} = 01$, and one of four possible results $\{\varepsilon_{00}\eta_{00}, \varepsilon_{00}\eta_{11}, \varepsilon_{11}\eta_{00}, \varepsilon_{11}\eta_{11}\}$ when $k_{2i-1}k_{2i} = 10, 11$. In the same way, the other conditional probabilities can be calculated. Hence, the mutual information on the two-bit key under the attack strategy $\mathcal{E}$ is given by

$$I = \frac{1}{4}[(1+\sin\theta_\varepsilon)\log_2(1+\sin\theta_\varepsilon) + (1-\sin\theta_\varepsilon)\log_2(1-\sin\theta_\varepsilon)]. \tag{6.4.29}$$

Since $\sin\theta_\varepsilon = \sqrt{8d-16d^2}$ one obtains

$$I = \frac{1}{4}\left[\left(1+\sqrt{8d-16d^2}\right)\log_2\left(1+\sqrt{8d-16d^2}\right) + \left(1-\sqrt{8d-16d^2}\right)\log_2\left(1-\sqrt{8d-16d^2}\right)\right]. \tag{6.4.30}$$

The relationship between I and d is plotted in Fig.6.2. One finds that the probability of detecting the attacker is none-zero if the attacker wants to get the information on the two-bit key. Fig.6.2 shows attacker's maximal information on the two-bit key is 0.5 bits while the detection probability is 25%.

The obtained mutual information I is Oscar's information on only two-bit key $x \in \{00, 01, 10, 11\}$. Consider the possibility for Oscar successfully getting the authentication key k_a. In each communication, Oscar has to decide what the two-bit key is, which has four possible results, i.e., $00, 01, 10, 11$. According to Oscar's measurement results $y = \varepsilon_{ij}\eta_{\mu\nu}$ with $i, j, \mu, \nu \in \{0, 1\}$, Oscar can judge the two-bit key with a proper probability. For example, if the measurement result is $\varepsilon_{00}\eta_{11}$, Oscar can guess the key to be one of $00, 10$, or 11 with possibility $\frac{1}{2}$, $\frac{1}{4}$, and $\frac{1}{4}$, respectively. Suppose that Oscar decides

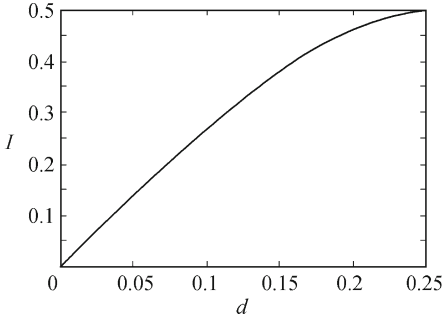

Fig. 6.2. Relationship between I and d

the key to be 00 or 01 with probability c and $1-c$ for 10 and 11, and consider the inconclusive measurement results, then total possibility of Oscar's successfully guessing the two-bit key is

$$P_s = \frac{1+\sin\theta_\varepsilon}{2}\left[\frac{1}{2}c+\frac{1}{4}(1-c)\right]+\frac{1-\sin\theta_\varepsilon}{2}\left[\frac{1}{4}(1-c)\right]$$
$$= \frac{1}{8}\left[(3c-1)\sin\theta_\varepsilon+2\right]. \tag{6.4.31}$$

Obviously, P_s is maximized at $c=1$. Consequently,

$$P_s^{max} = \frac{1}{4}(\sin\theta_\varepsilon+1) = \frac{1}{4}(\sqrt{8d-16d^2}+1). \tag{6.4.32}$$

Thus, the possibility of Oscar successfully obtaining the authentication key k_a is

$$P = [P_s^{max}(1-d)]^{\frac{n}{2}} = [\frac{1}{4}(\sqrt{8d-16d^2}+1)(1-d)]^{\frac{n}{2}}. \tag{6.4.33}$$

The relationship among P, d, and n is plotted in Fig.6.3. Obviously, $P \to 0$ when n is larger. For example, when $n=16$ and $d=25\%$, $P=3.91\times 10^{-4}$, which can be neglected. Accordingly, although Oscar can obtain some information on the two-bit key, the information on the authentication key k_a may be neglected. Furthermore, since a key updating scheme is proposed in Step 5, the key may be automatically updated after identification. Thus Oscar's knowledge on the old key will be useless.

6.4.3 In Imperfect Channel

The above QIA scheme in an ideal quantum channel is described, and then its security is analyzed. However, the employed quantum channel is imperfect in practice. Two kinds of quantum channels, i.e., the noisy channel without loss and lossy channel without noise, are always involved.

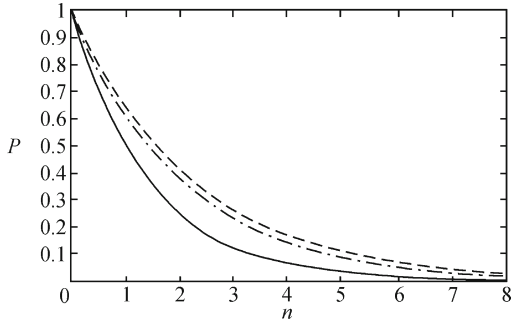

Fig. 6.3. Relationship among P, d and n

$d=0$ for the continuous line. $d=12.5\%$ for the dotted line and $d=25\%$ for the dashed line.

1) Noisy Influences

In a noisy quantum channel, errors occur on the transmitted qubits due to the influence of noise, which influences the final authentication process. Fortunately, the quantum error correction code [**?**] provides an approach of preventing the errors. Thus the above QIA scheme is available with the assistance of the quantum error correction code in a noisy channel.

Without the quantum error correction code, the QIA scheme presented in above is also available in a noise environment with the following revisions. First, the number of distributed entanglement states in Step 1, which may be disturbed possibly by the noise, should be $n'(n' > n)$. Making use of the technique of the quantum privacy amplification [**?**] (actually entanglement purification), CA and Bob distill finally n EPR pairs $|\Psi\rangle$ from the distributed n' pairs. Second, Step 4 needs to be revised since the influence of noise on the particle m. Suppose that the error rate is α, then there are $\varepsilon_0 = \alpha n$ errors in CA's measurement results comparing to the authentication key k_a. The errors E_0 is employed as a threshold of showing whether eavesdropping exists or not. When $\varepsilon > \varepsilon_0$ there is an attacker; otherwise, no attacker.

If attacker adopts the direct measurement strategy on the information particle m, one has

$$\rho'_m = \sum_i^n p_i U_i \rho_m U_i^\dagger = \sum_i^n p_i U_i I U_i^\dagger = I, \tag{6.4.34}$$

where U_i denotes the error operator on the information particle m. Similarly, $\rho'_{m_i} = \rho_{m_i} = I$. Then

$$\chi(\rho'_m) = \chi(\rho_m) = 0, \tag{6.4.35}$$

which illustrates that an attacker would get no information on the authentication key if he directly measures information particle on the noisy channel. If the attacker adopts the attack strategy on two-way channel, he still cannot

get any information on the authentication key because of the quantum privacy amplification process. In fact, the quantum privacy amplification leads the n' distributed entanglement states to be n maximal entanglement states of the home and traveling particles and makes attacker's operation on traveling particles effortless. Therefore, effect of the attack strategy on two-way channel is same as that of the direct measurement strategy. Accordingly, Eq.(6.4.35) is still suitable for this attack strategy.

2) Lossy Influences

Let lossy coefficient of the employed quantum channel be γ. The loss leads that Bob and CA receive respectively $(1-\gamma)n$ traveling particles and $(1-\gamma)^2 n$ information particles when n traveling particles are sent initially to Bob. In this situation, CA can authenticate Bob's identity by decoding the received $(1-\gamma)^2 n$ information particles. Since Bob encodes the authentication information by using $(1-\gamma)n$ particles, the authentication key may be shortened. Thus, the original key k_a is divided into two parts, i.e.,

$$k_a^{loss} = \{k_1^{loss}, k_2^{loss}, ..., k_{2(1-\gamma)n}^{loss}\},$$

and

$$k_a^{rest} = \{k_1^{rest}, k_2^{rest}, ..., k_{2\gamma n}^{rest}\}.$$

Employing the key k_a^{loss} as a new authentication key, then the 5-step protocol presented in above is still available.

If Oscar disturbs directly the quantum channel, CA and Bob can detect Oscar according to the total loss and errors. However, a wise Oscar may replace the lossy channel by an ideal one. Then Oscar may obtain γn particles in the forward line since only $(1-\gamma)n$ particles need to be sent to Bob. However, these particles provide no available information. In the backward line, Oscar may obtain $\gamma(1-\gamma)n$ particles since only $(1-\gamma)^2 n$ particles are employed in Alice's authentication process. Obviously, there are two available particle sets in the backward line, i.e, intercepted particles and authentication particles. For clearly, the particles intercepted by Oscar and the particles employed in the final authentication process by sets $\mathscr{E}$ and $\mathscr{A}$ are denoted as follows, respectively,

$$\mathscr{E} = \{p_e^1, p_e^2, ..., p_e^{\gamma(1-\gamma)n}\}, \tag{6.4.36}$$

$$\mathscr{A} = \{p_a^1, p_a^2, ..., p_a^{(1-\gamma)^2 n}\}, \tag{6.4.37}$$

where $p_x^i (x = e, a)$ denotes the particle. For the particles in the set $\mathscr{A}$, one may analyze the security using the same way in the Section 6.4.2. In the following the information leakage in the set $\mathscr{E}$ is mainly investigated. If Oscar uses the attack strategy of two-way channel on the particle set $\mathscr{E}$, the eavesdropping cannot be detected because these particles do not need to return Alice. Like the way presented in the Section 6.4.2, Oscar may obtain information I which is expressed in Eq.(6.4.30). Using this information Oscar may try to obtain the authentication key k_a^{loss}.

A slight modification may prevent the influence of the information leakage on the authentication key k_a^{loss}. Since the particle set $\mathscr{E}$ has been intercepted by Oscar without being detected, CA and Bob discard the key bits which have been encoded by Bob in the particle set $\mathscr{E}$. Employing the key bits in k_a^{rest} and key bits encoded in the particle set $\mathscr{A}$, CA and Bob construct the updated key as follows,

$$k'_{2i} = \hat{k}_{2i-1} \oplus \hat{k}_{2i} \oplus k'_{2i-1}, \tag{6.4.38}$$

where $\hat{k}_{2i-1}, \hat{k}_{2i} \in \{\hat{k}_a^{loss}, k_a^{rest}\}$, $\hat{k}_a^{loss}$ denotes the set of key bits encoded in the particle set $\mathscr{A}$, and k'_i is obtained by measuring the received $(1-\gamma)n$ traveling particles by Bob and the corresponding home particles hold by Alice. Thus all of the updated key bits $k'_{2i-1}k'_{2i}(i = 1, 2, \ldots, (1-\gamma)n)$ are completely new to Oscar, and the intercepted particle set $\mathscr{E}$ does not influence the security of the updated key.

Next, consider the influence of the lossy channel on the authentication efficiency. Due to the lossy channel, if Alice sends n travel particle t to Bob, Bob only gets γn of them. Bob then encodes $2\gamma n$ secret key information into the information particle m and returns them to Alice. Since there exists a two-way channel, Alice can only get $\gamma^2 n$ information particles. Suppose that Alice and Bob need to authenticate $2n$ bits to verify the identity, in order to authenticate all of those bits, Alice has to initially generate n/γ^2 travel particles. Therefore, the lossy channel would cause an efficiency loss.

6.5 Quantum Signature Principle

An important issue in the classic cryptography as well as quantum cryptography is the reliable assignment of a message to its originator and the integrality verification of a message, which is called a signature scheme [**?**]. The signature scheme is developed classically so far for this purpose as an addition to a message such that the message can neither be disavowed by the signatory nor can it be forged or changed by the receiver or a possible attacker. Up to now, conventional (handwritten) and digital approaches have been employed in practical applications. While conventional signatures cannot be transmitted in the electronic network and are vulnerable with respect to forgery. Digital signatures have been used widely and with considerable success in e-commerce. However, classical cryptography and thus also classical signature schemes are in general not theoretically secure and are in addition difficult to assign to messages in qubit format. Especially, the rapid development of quantum computers increasingly jeopardizes the security of digital signature scheme which depends on classically computational complexity.

There are two categories of signature schemes, i.e., the arbitrated signature scheme and true signature scheme, in the digital signature as well as the quantum signature. The arbitrated signature scheme involves directly three

partners, i.e., the signatory, receiver and arbitrator. The arbitrator takes part in the signature and/or verification procedure [**?**, **?**]. Since a trustable arbitrator is always necessary in the arbitrated quantum signature scheme, there are a few limitations on this kind of signature schemes in practical applications. A more popular signature scheme is the so called true signature scheme. In this category, the signature algorithm and verification algorithm are executed independently by the signatory and receiver, respectively. The signature key is secret but the verification key is public. An arbitrator is called only to settle possible disagreements or disputes between the signatory and the receiver. In practices, the true signature algorithm is in general favorable.

Similar to classical digital signatures the following rules are required for quantum signatures. Compare to the classic case, only the last one is characteristic for quantum signature schemes:

- No modifications and no forgery: Neither a receiver nor a possible attacker is able to change the signature or the attached message after completion. The signature may not be reproduced as well.
- No disavowals: The signatory may not successfully disavow the signature and signed message. It needs to be possible for the receiver to identify the signatory. The receiver may not successfully deny the receipt of message and signature.
- Firm assignments: Each message is assigned anew to a signature and may not be separated from it afterwards.
- Quantum nature: The signature involves purely quantum mechanical features without a classical analog and is therefore by nature non reproducible and may not be disavowed or forged.

By analogy with the digital signature scheme, a quantum signature scheme consists of three phases: the initial phase, signature phase, and verification phase. In the initial phase, communicators generate and distribute a private and public key which will be employed in the signature phase and verification phase, respectively. In the signature phase, the signatory signs the message and obtains a signature of the message via a signature algorithm. The signature is employed to verify the authenticity and integrality of the message. In the verification phase, the receiver verifies independently signatory's signature via a verification algorithm.

As usual the signatory, receiver and possible attacker are referred to as Alice, Bob, and Oscar, respectively, where appropriate. Let the message be signed carried by a quantum state $|P\rangle$. The signing algorithm is denoted $Q_s^{k_s}$ with key k_s to be used in the signature phase. In the verification phase, the resulting signature $|S\rangle$ with $|S\rangle = Q_s^{k_s}(|P\rangle)$ can subsequently be verified using a verification algorithm $Q_v^{k_v}$ with key k_v. Note the keys k_s and k_v may be the same (symmetrical key cryptosystem) or be different (public key cryptosystem) [**?**]. Given a pair $(|P\rangle, |S\rangle)$, the verification algorithm when applied is required to result "true" or "false" depending on whether the signature is authentic or forged.

A quantum signature scheme is defined as a 5-tuple $(\mathscr{P}, \mathscr{S}, \mathscr{K}, \mathscr{Q}_s, \mathscr{Q}_v)$ with following abbreviations: $\mathscr{P}$ is a set of possible messages carried by qubits. $\mathscr{S}$ is a set of possible signatures, which may consist of qubits or classical bits. $\mathscr{K}$ is a set of possible keys, and it may be a quantum key or classical key. $\mathscr{Q}_s$ is a set of possible quantum signature algorithms. $\mathscr{Q}_v$ is a set of possible quantum verification algorithms.

For each key $k \in \mathscr{K}$, there needs a signature algorithm $Q_s^{k_s} \in \mathscr{Q}_s$ and a corresponding verification algorithm $Q_v^{k_v} \in \mathscr{Q}_v$. $Q_s^{k_s} : \mathscr{P} \to \mathscr{S}$ and $Q_v^{k_v} : \mathscr{P} \times \mathscr{S} \to \{\text{true}, \text{false}\}$ are functions such that the following equation is satisfied for every message $|P\rangle \in \mathscr{P}$ and for every signature $|S\rangle \in \mathscr{S}$:

$$Q_v^{k_v}(|P\rangle, |S\rangle) = \begin{cases} \text{true}, & \text{if } |S\rangle = Q_s^{k_s}(|P\rangle), \\ \text{false}, & \text{if } |S\rangle \neq Q_s^{k_s}(|P\rangle). \end{cases} \tag{6.5.1}$$

The signature $|S\rangle$ and keys may be composed of quantum or classic bits, but the signature and verification algorithms $Q_s^{k_s}$ and $Q_v^{k_v}$ should possess quantum nature. In addition, Eq.(6.5.1) is associated with the comparison of different qubits. In the classic scenarios, the comparison between two bits is very easy. However, it is complicated between two qubits since the qubits may be nonorthogonal states which are indistinguishable. The indistinguishability of qubits and indistinguishability of operators have been described in Section 3.5.3, these properties can be utilized for such kind of comparisons.

According to the classic cryptology, a signature scheme may be designed for a known message or/and unknown message. The unknown message signature scheme is always called as "blind signature" in the classic cryptology [**?**]. Exactly, the blind signature considers the cases of Alice or Bob or even both Alice and Bob do not know the message content to be signed and verified. While the signature scheme for known message consider the case of all participants knowing the message content. There are many examples for this case in the classic cryptology as well as in our daily life. One should note that the known message may be different for different participants since there are possibly forged attacks. This is why the signature schemes are necessary in private communication systems. Accordingly, signature schemes for the known message and for the unknown message are two different cases in the cryptology.

Similar to the digital signature, a secure quantum signature scheme should satisfy three aspects. First, neither a receiver nor a possible attacker is able to change the signature and create a legal signature of the message, also they cannot change the attached message after completion. Second, the signatory may not successfully disavow the signature and signed message. Third, it needs to be possible for the receiver to identify the signatory. In short, complete security in a quantum signature scheme requires that the signatory cannot disavow the signature and that the receiver and attacker can obtain the signature or the signature key with a possibility vanishing exponentially or even a zero possibility.

Referring to the quantum signatures, one may develop a new notion called the qubit signature. There are slight differences between the quantum signature and qubit signature. The quantum signature is associated with a message. Generally, a message should be expressed using a qubit string, this is similar to the classic case. Thus, a quantum signature scheme should treat with many quantum states. But the so-called qubit signature refers to only one quantum state. Of course, if a message can be denoted using one qubit, both cases are the same; otherwise, the qubit signature has only physical application without benefits in the information processing.

To demonstrate the nature of the quantum signature, two quantum signature schemes are exemplified in the following sections.

6.6 Arbitrated Quantum Signature

This section describes an arbitrated quantum signature scheme for the known messages. This scenario has been applied widely in engineering and our daily life. For example, when one withdraws money from a bank, one has to fill out a bank paper. Obviously, the content of the paper, i.e., the message, is known and must be known to any participants. The procedure of signing the name in the paper performs actually a signature procedure. Consequently, possible forged attacks on the original message may be against. This procedure is called as "handwritten signature". If this procedure is executed in a computer network, a digital signature algorithm should be employed. However, if this procedure is executed in a quantum network [32], which is an important topic in the quantum communication, the corresponding signature algorithm must be a quantum signature algorithm. The transmission of known message in a quantum network is very easy. For example, if a quantum state is sent with its amplitude and phase information from Alice to Bob, Bob may know exactly the received quantum state. In the arbitrated quantum signature scheme for the known message one may employ this kind of techniques. An arbitrated quantum signature scheme using the GHZ state and quantum encryption algorithm is described as follows [**?**].

6.6.1 Algorithm Description

The presented arbitrated quantum signature scheme includes three phases, i.e., the initial phase, signing phase, and verification phase. This scheme executes the following phases.

1) Initial Phase

This phase is usually employed to distribute and generate signature key and verification key, and to set initial parameters if needed. This phase exe-

cutes following operations.

Step i1: Generation and distribution of keys. Alice and Bob begin by obtaining their secret keys k_a, k_b, where k_a, k_b are employed in the communications between Alice and arbitrator, and between Bob and arbitrator, respectively. These keys may be obtained by using standard technologies of quantum and classic cryptography. The keys here are assumed to be generated via quantum cryptographic methods because of their unconditional security. The length of these keys depends on the chosen cryptographic algorithms in the signing and verifying phases described in the later.

Step i2: Generation and distribution of GHZ triplet states. This scheme relies crucially on the entanglement of three involved communicators Alice, Bob and the arbitrator. This shall be established here prior each communication by a distribution of one particle of GHZ triplet states to each of the three. For convenience, assume that the arbitrator creates and distributes the GHZ particles. When the arbitrator receives Alice's or Bob's application for an arbitrated communication, he is required to create a string of GHZ triplet states and then to distribute two particles of each GHZ triplet state to each Alice and Bob and to keep the remaining one for himself for each GHZ state. As a consequence, the arbitrator, Alice and Bob are entangled because they hold one particle of each GHZ triplet state. The GHZ states for a three particle system involve eight orthogonal triplet states, here the following state is employed,

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle). \tag{6.6.1}$$

It is emphasized for above procedures, that Step i1 is finished once the system has been set up, and that it is not necessary to repeat it in later communications. Step i2 is necessary to be redone for every single communication, the necessity of which becomes clear in the description of the algorithm.

2) Signature Phase

The signature phase corresponds to the actual signature algorithm Q_s^k, i.e., to sign the message $|P\rangle$ with a suitable signature $|S\rangle$. The following steps are required.

Step s1: Alice encodes a known message using qubits to generate a message state $|P\rangle = \{|p_1\rangle, |p_2\rangle, \ldots, |p_n\rangle\}$ with $|p_i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle$.

Step s2: Alice generates a random string $|R\rangle = \{|r_1\rangle, |r_2\rangle, \ldots, |r_n\rangle\}$ by encrypting her message state. In cryptographic language the $|R\rangle$ is expressed by

$$|R\rangle = M_{k_a}(|P\rangle), \tag{6.6.2}$$

where M_{k_a} denotes an encryption algorithm which is denoted as an operator. Eq.(6.6.2) is a general expression since many approaches may be adopted to generate the random string $|R\rangle$. How to implement the quantum encryption procedure has been described in Chapter 5.

Step s3: Alice entangles each qubit of the information string $|P\rangle$ with one particle each of her equally long GHZ particle string to become a particle-pair. This may be implemented by applying a joint operation on both particles, such as in a quantum logic gate operation. Each combination generates a four-particle entangled state, involving three GHZ particles and the information qubit. Using Eq.(6.6.1) and expression of the state $|p_i\rangle$, the four-particle entangled state is given by

$$\begin{aligned}|\phi\rangle_i &= |p_i\rangle \otimes |\psi\rangle \\ &= \frac{1}{2}\{|\Psi_{12}^+\rangle_a(\alpha_i|00\rangle_{bA} + \beta_i|11\rangle_{bA}) + |\Psi_{12}^-\rangle_a(\alpha_i|00\rangle_{bA} - \beta_i|11\rangle_{bA}) + \\ &\quad |\Phi_{12}^+\rangle_a(\beta_i|00\rangle_{bA} + \alpha_i|11\rangle_{bA}) + |\Phi_{12}^-\rangle_a(\beta_i|00\rangle_{bA} - \alpha_i|11\rangle_{bA})\}, \qquad (6.6.3)\end{aligned}$$

where subscripts a, A and b correspond, respectively, to Alice, the arbitrator, and Bob. $|\Psi_{12}^+\rangle$, $|\Psi_{12}^-\rangle$, $|\Phi_{12}^+\rangle$, $|\Phi_{12}^-\rangle$ denote four Bell states [**?**].

Step s4: Alice executes a Bell measurement on $|\phi\rangle_i$ and obtains the results $\mathbf{m}_a$,

$$\mathbf{m}_a = \{m_a^1, m_a^2, \ldots, m_a^n\}, \qquad (6.6.4)$$

where m_a^i is one of four Bell states in $\{|\Psi_{12}^+\rangle, |\Psi_{12}^-\rangle, |\Phi_{12}^+\rangle, |\Phi_{12}^-\rangle\}$, in particular is the result arising from her Bell measurement on the state $|\phi\rangle_i$ in Eq.(6.6.3). The effect of this measurement is to disentangle Alice's two particles, i.e., the information qubit and GHZ particle, to be in one of the four Bell states and to retain the arbitrator's and Bob's corresponding GHZ particles to be in a two-particle entanglement state as visible in Eq.(6.6.3).

Step s5: Alice creates the signature $|S\rangle$ of the message $|P\rangle$ via encrypting the Bell measurement results $\mathbf{m}_a$ and the generated $|R\rangle$ using a quantum symmetrical key cryptosystem, e.g., the quantum one-time pad algorithm. Mathematically,

$$|S\rangle = k_a(\mathbf{m}_a, |R\rangle). \qquad (6.6.5)$$

The $\mathbf{m}_a$, even though consisting of quantum mechanical Bell states, may be presented by classical bits, and thus be encrypted by a classical one-time pad. Another way would be to encode $\mathbf{m}_a$ into a string of qubits $|m_a^i\rangle$ with $i = 1, 2, \ldots, n$ and then make quantum encryption operations on both $|m_a^i\rangle$ and $|R\rangle$ via M_{k_a}.

Step s6: Alice sends the string of the message $|P\rangle$ followed by the signature $|S\rangle$ to Bob. Please note here that the message state should be followed by the signature $|S\rangle$. This is associated with the definition of the signature scheme.

3) Verification Phase

A verification algorithm Q_V^k is developed here such that Bob is enabled to verify Alice's signature $|S\rangle$ and consequently judge the authenticity of the information qubit $|P\rangle$. The verification process in this scheme requires the help of the arbitrator because Bob does not possess Alice's key which is necessary for the verification of the signature. The verification phase is executed by the following procedure:

Step v1: Bob measures his GHZ particles and obtains the results $\mathbf{m}_b$, then he encrypts $\mathbf{m}_b, |S\rangle$, and $|P\rangle$ with his key k_b to obtain y_b,

$$y_b = k_b(\mathbf{m}_b, |S\rangle, |P\rangle). \tag{6.6.6}$$

After that Bob sends y_b to the arbitrator.

Step v2: The arbitrator becomes active now and generates a verification parameter γ based on the communication from Bob, which contains the information also from Alice. After receiving y_b, the arbitrator decrypts it using k_b, and obtains $|S\rangle, |P\rangle, \mathbf{m}_b$. Then the arbitrator decrypts $|S\rangle$ using the key k_a, which he has since the initial phase. This gives rise to $|R'\rangle$, which needs to be compared with $|R\rangle$. With $|R'\rangle$, $|P\rangle$, and M_{k_a}, the arbitrator then creates a parameter γ via

$$\gamma = \begin{cases} 1 & \text{if } |R'\rangle = |R\rangle = M_{k_a}|P\rangle, \\ 0 & \text{if } |R'\rangle \neq |R\rangle = M_{k_a}|P\rangle. \end{cases} \tag{6.6.7}$$

In this step the arbitrator generates $|R\rangle$ using the message state decrypted from y_b using k_b, the precise mathematical description is the same as that in Eq.(6.6.2). Then, the arbitrator decrypts the $|S\rangle$ to obtain $|R'\rangle$, i.e.,

$$|R'\rangle = {k_a}^{-1}(|S\rangle). \tag{6.6.8}$$

Comparing the obtained $|R\rangle$ and $|R'\rangle$, the arbitrator creates a parameter γ. Since $|P\rangle$ is a known message, the arbitrator may easily perform the comparison operation.

Step v3: The arbitrator sends his GHZ particles and the encrypted result $y_{tb} = k_b(\mathbf{m}_a, \mathbf{m}_b, \gamma, |S\rangle)$ to Bob.

Step v4: Bob obtains the arbitrator's GHZ particles. In addition, Bob obtains $\mathbf{m}_a, \mathbf{m}_b, |S\rangle$ and γ via decrypting the received y_{tb}.

Step v5: Bob performs the initial verification via the parameter γ. If $\gamma = 0$, the signature has obviously been forged and Bob may reject the message $|P\rangle$ immediately. If $\gamma = 1$, Bob goes on for further verification to the next step.

Step v6: Bob performs a further verification via comparing the states $|P\rangle$ and $|P'\rangle$, where $|P'\rangle$ is obtained according to the correlation of the GHZ triplet state. The approach is as follows. Bob chooses a proper transformation operator sequence $\mathbf{m}_t$ on the GHZ particles from the arbitrator. According to the correlation Bob obtains the state $|P'\rangle$. One should note here that parameters $\mathbf{m}_a, \mathbf{m}_b$, and $\mathbf{m}_t$ must be correlated. The correlation of these parameters has been illustrated clearly in the Table 6.1.

For clearly, how to generate the state $|P'\rangle$ is described in detail as follows. After Alice's Bell measurement in Step s4, Bob's and the arbitrator's GHZ particles become a two-particle entangled state dependently on Alice's Bell measurement result. For example, if Alice result is $|\Psi_{12}^{+}\rangle_a$, Bob's and the

Table 6.1. Correlation of the parameters $\mathbf{m}_a, \mathbf{m}_b$ and $\mathbf{m}_t$

$\mathbf{m}_a$	$\mathbf{m}_b$	$\mathbf{m}_t$
$\|\Psi_{12}^+\rangle$	$\|+x\rangle$	I
$\|\Psi_{12}^+\rangle$	$\|-x\rangle$	σ_z
$\|\Psi_{12}^-\rangle$	$\|+x\rangle$	σ_z
$\|\Psi_{12}^-\rangle$	$\|-x\rangle$	I
$\|\Phi_{12}^+\rangle$	$\|+x\rangle$	σ_x
$\|\Phi_{12}^+\rangle$	$\|-x\rangle$	$\sigma_x\sigma_z$
$\|\Phi_{12}^-\rangle$	$\|+x\rangle$	$\sigma_x\sigma_z$
$\|\Phi_{12}^-\rangle$	$\|-x\rangle$	σ_x

arbitrator's entangled state must be

$$\begin{aligned}|\varphi\rangle_{bA} =&\alpha_i|00\rangle_{bA} + \beta_i|11\rangle_{bA}\\ =&\frac{\sqrt{2}}{2}\left\{|+x\rangle_b\left(\alpha_i|0\rangle_A + \beta_i|1\rangle_A\right) + |-x\rangle_b\left(\alpha_i|0\rangle_A - \beta_i|1\rangle_A\right)\right\}.\end{aligned}$$

After Bob's measurement on his GHZ particles in the step v1, arbitrator's GHZ particle becomes a single qubit which has the state

$$|\theta\rangle = \begin{cases}\alpha_i|0\rangle + \beta_i|1\rangle, & \text{if } \mathcal{M}_b^i = |+x\rangle,\\ \alpha_i|0\rangle - \beta_i|1\rangle, & \text{if } \mathcal{M}_b^i = |-x\rangle.\end{cases} \tag{6.6.9}$$

According to the results $m_a^i \in \mathbf{m_a}$ and $m_b^i \in \mathbf{m_b}$ Bob applies a proper operator $m_t^i \in \mathbf{m_t}$ on the received GHZ particle from the arbitrator. Subsequently, the state $|p_i'\rangle$ is obtained. For example, if $m_b^i = |+x\rangle$, Bob should choose $m_t^i = I$ on the received arbitrator's GHZ particle, then he may obtain the message state $|p_i'\rangle = |\theta\rangle$. While if $m_b^i = |-x\rangle$, Bob should choose $m_t^i = \sigma_z$ on the received arbitrator's GHZ particle. Then Bob may also obtain the message state with an operation $|p_i'\rangle = \sigma_z|\theta\rangle$. In the above only one case for outputting the state $|p_i'\rangle$ has been analyzed. For other situations one may analyze the mathematical procedures using a similar way.

The presented quantum signature scheme is referred to known message. In principle this scheme is suitable for the unknown message. The precise security definition is the same as that for the known message. In this case, the scheme associates with the comparison test of unknown message states. The controlled-swap approach presented in Section 3.5.3 is employed to compare the state $|P\rangle$ (or $|R\rangle$). Recall that the employed state $|P\rangle$ (or $|R\rangle$) is an n-qubit string, which can then be compared independently. To guarantee the security of the arbitrated quantum signature scheme, one notes here that all comparison tests for n pairs qubits in $|P\rangle$ and $|P'\rangle$ (or in $|R\rangle$ and $|R'\rangle$) should pass the verification, otherwise one judges the verification phase cannot be passed. According to the nature of the signature scheme, the aim of attacker is to pass the verification phase with forging some qubits in the message state

$|P\rangle$ so that the forged message may benefit himself. To reach this aim, suppose that l qubits need to be forged successfully. Then, according to Eq.(3.5.27) the failure probability of the verification phase is just the total error probability for l qubits in $|P\rangle$ (or $|R\rangle$), which may be expressed as

$$p_t^e = \left(\frac{1+\varepsilon_1^2}{2}\right)\cdots\left(\frac{1+\varepsilon_l^2}{2}\right) \leq \left(\frac{1+\varepsilon^2}{2}\right)^l, \tag{6.6.10}$$

where $\varepsilon = \max\{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_l\}$ and $\varepsilon_i (i = 1, 2, \ldots, l)$ is the inner product of the ith pair qubits in $|P\rangle$ and $|P'\rangle$ (or in $|R\rangle$ and $|R'\rangle$).

Consider that l may be not enough larger in some case, one has to make a slightly revision on the presented quantum signature scheme, which lets the message state be $|\tilde{P}\rangle = \otimes_{i=1}^{N}|P\rangle$(i.e., N copies) in Step s1. This revision may reduce further the error probabilities. In this case, the arbitrator may create N copies of the state $|R\rangle$ and $|R'\rangle$ in Step v2, and Bob may obtains N copies of $|P\rangle$ and $|P'\rangle$ in Step v6. Then, the independent comparison of N copies leads the error probabilities on ith qubit in $|P\rangle$ or $|R\rangle$ to be

$$\tilde{p}^e \leq \left(\frac{1+\varepsilon_i^2}{2}\right)^N. \tag{6.6.11}$$

Thus, with a finite number N the error probability p^e may be arbitrary smaller. This means even if only one qubit (i.e., $l = 1$) has been forged the attack strategy cannot be succeed. Combining Eqs.(6.6.10) and (6.6.11), one obtains the failure probability of the verification phase in this case for a dishonest Bob,

$$\tilde{p}_t^e \leq \left(\frac{1+\varepsilon^2}{2}\right)^{lN}. \tag{6.6.12}$$

For an attacker who is not the participant of the scheme, since the verification is associated with both comparisons between $|R\rangle$ and $|R'\rangle$ and between $|P\rangle$ and $|P'\rangle$, the failure probability of the verification phase is

$$\tilde{p}_t^e \leq \left(\frac{1+\varepsilon^2}{2}\right)^{2lN}. \tag{6.6.13}$$

Obviously, with a finite number N the failure probability may decrease exponentially. This means the failure probability of the verification phase can be reduced in principle to an arbitrary small $\epsilon > 0$ by choosing a proper parameter N. Of course, many copies of the message state may add complexity of the proposed quantum signature algorithm, thus simpler schemes need to be investigated further.

Since the quantum state comparison involved in the verification phase of the arbitrated quantum signature scheme is actually a kind of identification procedures of two different operations on a given state, i.e., the message

state $|P\rangle$ or the state $|R\rangle$, it is different from the discrimination of arbitrated unknown states which cannot be perfectly distinguished. As described in Section 3.5.3, different quantum operations (e.g., U and V) on a given state can be perfect distinguished [32 – 34]. This approach might be employed for the quantum state comparison in the arbitrated quantum signature scheme.

6.6.2 Security Analysis

The security analysis of the quantum signature scheme is different from that of the QKD scheme which has been described in Chapter 4. According to the security requirements of the quantum signature presented in previous section, this subsection demonstrates the unconditional security of the above quantum signature scheme.

1) Impossibility of Forgery

A dishonest Bob or an attacker may seek to forge Alice's signature, to his own benefit. We begin by assuming that Bob is dishonest and tries to forge Alice's signature. If successful, this is beneficial for him because he can change Alice's signature and design a new signature to a message favorable to him. This is impossible, however, because the signature key k_a is secretly kept by Alice and the arbitrator. As a consequence, Bob cannot obtain the correct state $|R\rangle$, which is necessary for the generation of the signature. Subsequently, the parameter γ is not correct, so that this forgery can be noted when the arbitrator is called to settle a dispute between Alice and Bob.

The attacker is bound to be without success in the above algorithm, because the only public parameters are $|P\rangle, |S\rangle, y_b, y_{tb}$ and they do not offer any information of the secret keys k_a and k_b. Especially, when communicators encrypt the messages by a one-time pad algorithm which is relatively easy to be implemented in quantum cryptography, the security is very high. Even if the attacker does somehow get hold of Alice's and Bob's keys, a forgery remains still impossible. This is because the attacker has no access to Alice's measurement result $\mathbf{m}_a$, which is secret and involved in generating the quantum signature $|S\rangle$. The verification condition $|P'\rangle = |P\rangle$ cannot be satisfied without the correct $\mathbf{m}_a$. Thus, the correlation of the GHZ triplet state avoids forgery by an attacker.

2) Impossibility of Disavowal for Signatory

If Alice disavows her signature, it is very easy to discover it, because Alice's key is contained in the signature $|S\rangle$. Thus, if Alice and Bob are engaged in a dispute because of Alice's disavowal, they just need to send the signature $|S\rangle$ to the arbitrator. If the signature $|S\rangle$ contains Alice's key k_a, this signature has been carried out by Alice, otherwise, the signature has been forged by Bob or the attacker. Therefore, the arbitrator is in the position to judge whether Alice has disavowed her signature.

3) Impossibility of Denial for Receiver

A conventional and a digital signature scheme is termed undeniable if Bob cannot deny his receiving of Alice's files. This feature is not generally demanded of a signature, but it may be useful for many practical applications. The above algorithm contains this property, i.e. Bob cannot disavow his receiving of the signature $|S\rangle$ and the information qubit string $|P\rangle$. This is essentially impossible because he needs the assistance of the arbitrator in the verification process. In addition, one can reduce the dependence on the arbitrator by small modifications without losing this property of having an undeniable signature scheme. In the verification procedure, Bob obtains y_b in Step v1 and sends it to Alice rather than to the arbitrator as in the original version. Then Alice obtains the new signature $|\tilde{S}\rangle = k_a(\mathbf{m}_a, |R\rangle, y_b)$ and sends it to the arbitrator. The arbitrator then modifies y_{ta} in Step v3 to be

$$\tilde{y}_{tb} = k_b(\mathbf{m}_a, \mathbf{m}_b, \mathbf{m}_t, \gamma, |\tilde{S}\rangle). \tag{6.6.14}$$

After these modifications Alice's and Bob's key are included in the signature $|\tilde{S}\rangle$. Then Bob cannot disavow the fact that the received files have come from Alice, i.e., Bob's receipt of the files is undeniable.

6.7 True Quantum Signature

The arbitrated quantum signature scheme relies on an arbitrator. This dependence limits the practical application. This section presents a true quantum signature scheme [**?**].

6.7.1 Algorithm Description

Like the arbitrated quantum signature scheme, there are also three stages, i.e., the initial phase, signature phase, and verification phase, in the true quantum signature scheme.

1) Key Generation

This phase generates keys for the signature phase and verification phase, i.e., the signature key and verification key. To construct these keys, a linear transformation which expands a k-dimension vector to a $2k$-dimension vector in real space is adopted. Then an arbitrary non-singular $k \times k$ matrix from a set with C_{2k-1}^{k} elements is chosen to compose a unitary matrix. Finally, a pair of keys is generated by employing the k-dimension vector and composed unitary matrix. The signature key is private but the verification key is public. Although the linear transformation has been exploited at the starting, the relationship between two keys is nonlinear which guarantees the uncondi-

tional security of the private key. This property will be proven mathematically in later.

Choose a linear mapping L in the real space $\mathbb{R}$, i.e., $L : \mathbb{R}^k \to \mathbb{R}^{2k}$. For an arbitrary vector denoted $\mathbf{x} = (x_0, x_1, \ldots, x_{k-1}) \in \mathbb{R}^k$, a $2k \times 1$ matrix may be created by the linear mapping L,

$$L : \mathbf{x} \to y(\mathbf{x}) = [y_0(x), y_1(x), y_2(x), \ldots, y_{2k-1}(x)]^{\mathrm{T}}. \tag{6.7.1}$$

Without loss of the generality, one may let $y_0(x) = x_0$ which can be implemented by choosing an appropriate linear transformation L. In order to satisfy the requirements of signature scheme, the linear mapping L is constrained by the requirement that the components of any k-element subset of $\{x_0, y_1, \ldots, y_{2k-1}\}$ are linearly independent. This requirement can always be satisfied which has been exploited in the quantum error correction code and quantum secret sharing scheme [36, 37]. Let $(r_1, r_2, \ldots, r_{2k})$ be an arbitrary permutation of indices $(0, 1, \ldots, 2k-1)$. As any k-element subset in $\{x_0, y_1, \ldots, y_{2k-1}\}$ is linearly independent, one can easily understand that subsets $\{y_{r_1}, y_{r_2}, \ldots, y_{r_k}\}$ and $\{x_0, y_{r_{k+1}}, \ldots, y_{2k-1}\}$ are linearly independent, respectively. Accordingly, there exists a non-singular $k \times k$ matrix T such that,

$$T \begin{pmatrix} y_{r_1} \\ y_{r_2} \\ \vdots \\ y_{r_k} \end{pmatrix} = \begin{pmatrix} x_0 \\ y_{r_{k+1}} \\ \vdots \\ y_{r_{2k-1}} \end{pmatrix}. \tag{6.7.2}$$

Actually, the matrix T denotes the space transformation from space $\mathbb{V}$ spanned by $\{y_{r_1}, y_{r_2}, \ldots, y_{r_k}\}$ to space $\mathbb{W}$ spanned by $\{x_0, y_{r_{k+1}}, \ldots, y_{2k-1}\}$. Apparently, there exist C_{2k-1}^k transformations like the matrix T. Denote all these matrixes by a set $\mathscr{T}$, then one has $T \in \mathscr{T}$.

Generate states $|\Psi_1\rangle = |y_{r_1}\rangle_{r_1} \ldots |y_{r_k}\rangle_{r_k}$ and $|\Psi_2\rangle = |x_0\rangle_{r_1}|y_{r_k+1}\rangle_{r_2} \ldots |y_{r_{2k-1}}\rangle_{r_k}$ by exploiting k-element subsets $\{y_{r_1}, y_{r_2}, \ldots, y_{r_k}\}$ and $\{x_0, y_{r_{k+1}}, \ldots, y_{r_{2k-1}}\}$, respectively. According to Eq.(6.7.2), $|\Psi_1\rangle$ and $|\Psi_2\rangle$ satisfy the following equation,

$$U|\Psi_1\rangle = |T|^{\frac{1}{2}}|\Psi_2\rangle, \tag{6.7.3}$$

where $|T| = \det T$. Actually, given T, there exists a unitary operator $U(T)$ such that above equation exists. The matrix element of U in the continuous basis $|\mathbf{x}\rangle = \{|x_0\rangle_{r_1}, \ldots, |x_k\rangle_{r_k}\}$ is

$$\langle \mathbf{x}'|U|\mathbf{x}''\rangle = |T|^{1/2} \prod_{i=0}^{k-1} \delta \left(\sum_{j=0}^{k-1} T_{ij} x_j'' - x_i' \right), \tag{6.7.4}$$

where $\langle x_i|x_j\rangle = \delta(x_i - x_j)$, and T_{ij} is an element of the matrix T. Eq.(6.7.4) shows that the matrix U depends simultaneously on the non-singular $k \times k$ matrix T and k-dimension vector $\mathbf{x}$.

Making use of Eqs.(6.7.1) – (6.7.4) one constructs a new transformation G which is expressed as follows,

$$G : \{L, \mathbf{x}, T_{ij}\} \to \{U, |T|^{1/2}\}. \tag{6.7.5}$$

Obviously, there is a special relationship between $\{L, \mathbf{x}, T_{ij}\}$ and $\{U, |T|^{1/2}\}$. That is, making use of the vector $\mathbf{x} \in \mathbb{R}^k$, linear transformation L, and matrix $T \in \mathscr{T}$, one obtains easily an unitary operator $U(T)$. However, the inverse procedure is impossible. This property is concluded by the following theorem.

Theorem 6.7.1 The transformation G expressed in Eq.(6.7.5) is a nonlinear transformation, and the mapping described by G is a one-way function. Here the linear mapping L is constrained by the requirement of any subset of k-element in $\{x_0, y_1, \ldots, y_{2k-1}\}$ is independent, $\mathbf{x} \in \mathbb{R}^k$, $T \in \mathscr{T}$ and U is determined by Eq.(6.7.4).

Proof Since U depends on the multiplication of T and $\mathbf{x}$, the characteristic of G being a nonlinear transformation is straightforward. As example, Eq.(6.7.2) shows that T depends on x_0, combining Eq.(6.7.4) one gains that U is a function of x_0^2, which means G is a nonlinear transformation on x_0.

First, consider the one-way property of the transformation G. One find that an element $U_{x'x''}$ of the matrix U is determined completely by parameters x_i, T_{ij} and $|T|^{1/2}$ from Eq.(6.7.4). If the variables $\mathbf{x}$ and $\mathscr{L}$ are given, the $2k$-dimension vector $y(\mathbf{x})$ can be calculated. Subsequently, the non-singular $k \times k$ matrix set $\mathscr{T}$ is constructed. Choosing a proper matrix T from the set $\mathcal{T}$, then T_{ij} and $|T|^{1/2}$ are obtained. Thus, the construction of the matrix U is straightforward.

Then, consider the inverse transformation G^{-1}. In this situation, the matrix U and thus its elements $U_{x'x''}$ are given, but the parameters $\mathbf{x}$ and T need to be solved. From Eq.(6.7.4) any element of the matrix U depends simultaneously on the vector $\mathbf{x}$ and the matrix T. Although $|T|^{1/2}$ is given, $U_{x'x''}$ is still a function with two kinds of variables, i.e., $T_{i,j}$ and x_i, which can be denoted as

$$U_{x'x''} = g(T_{i,j}, x_i), \tag{6.7.6}$$

where $i, j = 0, 1, \ldots, k-1$. Obviously, T_{ij} and x_i cannot be solved by the above equation. Especially, T is one element of the set $\mathscr{T}$ which is not given. This characteristic improves the difficulty of finding a proper T, and subsequently T_{ij}. Therefore the inverse transformation from $\{U, |T|^{1/2}\}$ to $\{L, \mathbf{x}, T_{ij}\}$ is impossible, which means G is a strict one-way function.

Theorem 6.7.1 shows that the nonlinear transformation G is a strict one-way mapping, which means that from $\{L, \mathbf{x}, T_{i,j}\}$ to $\{U, |T|^{1/2}\}$ is easy but the inverse procedure is impossible. Making using of this characteristic, the signature key and verification key are generated and distributed by the following steps.

Step k1: The signatory chooses secretly a random k-dimension vector $\mathbf{x} = (x_0, x_1, \ldots, x_{k-1})$ in real space as well as an appropriate mapping L as the private key, which will be exploited as a signature key. Denoting the

private key by k_s, which may be expressed mathematically as

$$k_s = \{L, x_i | i = 1, 2, \ldots, k\}. \tag{6.7.7}$$

Then the signatory keeps secretly the generated private key k_s.

Step k2: The signatory chooses randomly a non-singular $k \times k$ matrix from the set $\mathscr{T}$. The elements T_{ij} $(i, j = 0, 1, \ldots, k-1)$ of the matrix T are secret, but $|T|^{1/2}$ is public as a part of the public key which will be composed in the next step.

Step k3: Calculate the operator U by exploiting Eq.(6.7.4) according to the obtained private key and chosen matrix T. Then, the signatory publicly announces the unitary operator $U(T)$ and $|T|^{1/2}$ as the verification key k_v,

$$k_v = \{U(T), |T|^{1/2}\}. \tag{6.7.8}$$

The verification key will be exploited in the verification phase. One should note here that the verification key is a public key which may be announced as a telephone number so that any communicators can obtain it.

The public key, i.e., the verification key k_v depends on the private key k_s. However, except the signatory, i.e., Alice, anyone cannot get the private key by the public key, since the mapping from the signature key k_s to the verification key k_v is a one-way function which is described in Theorem 6.7.1. The security of the key pair will be analyzed in detail in Section 6.7.2.

2) Signature of Message

This phase corresponds to the actual signature algorithm $Q_s^{k_s}$, i.e., to sign the message $|P\rangle$ with a suitable signature $|S\rangle$. The signature algorithm is implemented by encoding the message state and preparing a proper two-particle entangled state according to the private signature key. Since the linear mapping L in Eq.(6.7.1) can always be satisfied, there are no limitations for the message format in the proposed scheme, i.e., the message may be denoted by continuous variables or discrete variables quantum state. This scheme employs the continuous-variable quantum state which has been widely investigated in the quantum computation [**?**], especially in the continuous-variable quantum key distribution [**?**]. The signature algorithm $Q_s^{k_s}$ executes the following steps.

Step s1: The signatory prepares $2k-1$ ancilla states according to the private key k_s. To encode the original message state $|P\rangle$ with wave function $\langle x_0|P\rangle$, Alice firstly creates a $2k \times 1$ matrix $y(\mathbf{x})$ by exploiting the private key k_s. Then she composes a product state $|\omega(\mathbf{x})\rangle$ by exploiting $\{y_1(\mathbf{x}), \ldots, y_{2k-1}(\mathbf{x})\}$. The product state is denoted as

$$|\omega(\mathbf{x})\rangle = |y_1(\mathbf{x})\rangle_1 \ldots |y_{2k-1}(\mathbf{x})\rangle_{2k-1}. \tag{6.7.9}$$

Step s2: The signatory encodes the message state $|P\rangle$. Since the message state $|P\rangle$ consists of continuous variable qubits, the encoding procedure is

denoted as following way,

$$Q^{k_s}|P\rangle \mapsto |\widetilde{S}\rangle = \int |P\rangle|\omega\rangle \mathrm{d}\mathbf{x}, \tag{6.7.10}$$

where Q^{k_s} denotes an quantum algorithm controlled under the key k_s. The encoding procedure can be described by a quantum circuit plotted in Fig.6.4. The input states are the message state $|P\rangle$ and the ancilla state $|\omega\rangle$, while the output state is a 2k-particle entanglement state. The procedure in Fig.6.4 is actually an encoding process of the continuous-variable quantum error correction coding. Since the projective operation of the encoded state on the message state satisfies

$$\begin{aligned} P_{|P\rangle}|\widetilde{S}\rangle &\to \int \langle P(x_0')|P(x_0)\rangle|\omega(\mathbf{x})\rangle \mathrm{d}\mathbf{x} \\ &= \int \delta(x_0' - x_0)|\omega(\mathbf{x})\rangle \mathrm{d}\mathbf{x} \\ &= |\omega(x_0')\rangle \neq |\omega(\mathbf{x})\rangle, \end{aligned} \tag{6.7.11}$$

the state $|\omega(\mathbf{x})\rangle$ associated with the private key k_s cannot be disclosed by decoded states and original message states, where $P_{|P\rangle}$ denotes the projective operator.

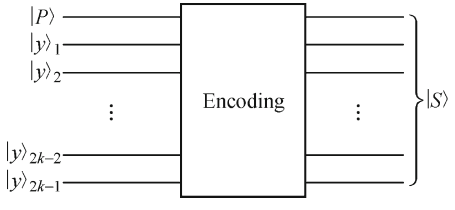

Fig. 6.4. Encoding procedure of message state $|P\rangle$ through quantum signature algorithm

Step s3: The signatory prepares a two-particle entangled state according to the private key. Making use of states $|y_{r_k+1}\rangle_{r_2}$ and $|y_{r_k+1}\rangle_{r_k+1}$ which are associated with the private key k_s, Alice prepares a two-particle entanglement state,

$$|\widetilde{\Omega}\rangle = \int_{\mathbb{R}} |y_{r_k+1}\rangle_{r_2}|y_{r_k+1}\rangle_{r_k+1}\mathrm{d}x. \tag{6.7.12}$$

Obviously, the prepared state $|\widetilde{\Omega}\rangle$ is associated with the private signature key. In addition, $|\widetilde{\Omega}\rangle$ may be an unknown state to the receiver and attacker since $|y_{r_k+1}\rangle_{r_2}$ and $|y_{r_k+1}\rangle_{r_k+1}$ are associated with the private key.

Step s4: The signatory creates a signature of the message, and sends the message followed the signature to receiver. Combining the resulting states $|\widetilde{S}\rangle$ and $|\widetilde{\Omega}\rangle$ yields a signature state,

$$|S\rangle = |\widetilde{S}\rangle \otimes |\widetilde{\Omega}\rangle. \tag{6.7.13}$$

After having created the signature state, Alice sends the message state $|P\rangle$ followed by the signature state $|S\rangle$ to Bob. It is stressed here that the message state $|P\rangle$ may be known or unknown to communicators, i.e., Alice and Bob, and thus to Oscar, while the signature state $|S\rangle$ must be unknown to Bob and Oscar in any situation since the receiver and attacker do not possess the signature key.

The signature is associated with $|P\rangle$ because $|S\rangle$ was generated via the message state. We note also at this state already that Alice's secret key was crucial in preparing the signature such that it appears impossible for Alice to disavow it in the face of the arbitrator or for Bob and an attacker to forge it. In addition, we realize that the separation of the message and its signature by Oscar would not benefit him because the message is valid only with the correct signature and new messages will be assigned new signatures.

3) Verification of Signature

A verification algorithm $Q_v^{k_v}$ is developed here such that the receiver, Bob, is enabled to verify Alice's signature $|S\rangle$ and consequently judge the authenticity of the message state $|P\rangle$. In previous scheme, the verification procedure requires arbitrator's participation because Bob does not possess Alice's key which is necessary for the verification of the signature. However, in this scheme the verification procedure does not need any third party. The verification phase is executed by the following procedures.

Step v1: The receiver performs syndrome measurement on the state $|\widetilde{S}\rangle$. Since the $2k$-particle entanglement state $|\widetilde{S}\rangle$ is actually a quantum error-correction code, Bob applies σ_x (x component of the Pauli matrix) on the $2k$th particle in the state $|\widetilde{S}\rangle$, which is equivalent to introduce a bit flip error on the final particle in the code. This operation leads $|\widetilde{S}\rangle$ changes to be $\sigma_x^{2k}|\widetilde{S}\rangle$, where the subscript $2k$ denotes that σ_x is applied on the $2k$th particles in the state $|\widetilde{S}\rangle$. By performing a syndrome measurement on the state $\sigma_x^{2k}|\widetilde{S}\rangle$, Bob obtains a value of the error syndrome denoted by s_e. If $s_e = 2k$, the state $|\widetilde{S}\rangle$ is a $2k$-particle quantum error-correction code. In this case, Bob applies σ_x^{-1} on the $2k$th particle in the state $|\widetilde{S}\rangle$ and proceeds with the following steps. Otherwise, Bob rejects the signature $|S\rangle$ and stops his further operations since in this situation the state $|\widetilde{S}\rangle$ is forged.

Step v2: The receiver decodes the state $|\widetilde{S}\rangle$ exploiting the verification key k_v. In terms of Eqs.(6.7.3) and (6.7.10), the signature is decoded with an operation $\widetilde{Q}_v^{k_v}$ on the state $|S\rangle$ and gives

$$\begin{aligned} U|\widetilde{S}\rangle &= J|T|^{\frac{1}{2}} \int \Big\{ |P\rangle |x_0\rangle_{r_1} |y_{r_k+1}\rangle_{r_2} |y_{r_k+1}\rangle_{r_k+1} \cdots |y_{r_{2k-1}}\rangle_{r_k} |y_{r_{2k-1}}\rangle_{r_{2k-1}} \Big\} \mathrm{d}\mathbf{x} \\ &= J|T|^{\frac{1}{2}} |P\rangle_{r_1} |\Omega\rangle_{r_2,r_{k+1}} |\Omega\rangle_{r_3,r_{k+2}} \cdots |\Omega\rangle_{r_k,r_{2k-1}}, \end{aligned} \tag{6.7.14}$$

where J is the Jacobian for the transformation from $\mathbf{x}$ to $y(\mathbf{x})$, and $|\Omega\rangle_{i,j} = \int_{\mathbb{R}} |y_l\rangle_i |y_l\rangle_j \mathrm{d}x$ ($i = r_2, r_3, \ldots, r_k, j = r_{i+k-1}, l = r_k + 1, \ldots, r_{2k-1}$), which is

an entanglement state of particles i and j.

Step v3: The receiver verifies the entanglement of the particles i and j after the state $|\widetilde{S}\rangle$ has been decoded. The aim of this operation is to ensure that the received state $|\widetilde{S}\rangle$ is an entanglement state of $2k$ particles so that Bob can judge the authenticity of the signature $|S\rangle$ in the following operations. Eq.(6.7.14) shows the decoded state is a product state of the decoded message state and $k-1$ two-particle entanglement states. Accordingly, Bob only needs to verify the entanglement properties of $k-1$ particle-pairs denoted by $\{r_2, r_{k+1}\}, \{r_3, r_{k+2}\}, \ldots, \{r_{r_k,2k-1}\}$, which correspond to the states $|\Omega\rangle_{r_2,r_{k+1}}, |\Omega\rangle_{r_3,r_{k+2}}, \ldots, |\Omega\rangle_{r_k,r_{2k-1}}$, respectively. The verification of the first state $|\Omega\rangle_{r_2,r_k+1}$ will be presented in later, while the remainder $k-2$ two-particle states are verified via correlation between two particles by employing the Bell theory or the approach presented in Ref.[40]. For the physical mechanism of how to measure the correlation of the entanglement state has been described in Section 3.5.2. If the measurement results show that each particle-pair holds the correlation of two-particle entangled state, Bob continues the remained steps in the verification phase. Otherwise the signature state is forged and Bob stops his operations.

Step v4: The receiver compares the decoded message state and the received (original) message state, and compares the decoded two-particle entangled state $|\Omega\rangle_{r_2,r_k+1}$ and the received state two-particle entangled state $|\widetilde{\Omega}\rangle$. For clarity, the decoded message state is denoted $|P'\rangle$. Since $|P\rangle$ and $|P'\rangle$ as well as $|\Omega\rangle_{r_2,r_k+1}$ and $|\widetilde{\Omega}\rangle$ can be compared by employing the same approach, only the comparison of the decoded message state and the received message state is analyzed. Eq.(6.7.14) shows that the message state $|P\rangle$ can be decoded from the signature $|S\rangle$. If the message state is known to Bob, the verification is very easy since Bob only needs to compare directly the received (original) message state with the decoded message state obtained from Eq.(6.7.14). However, due to the message qubit $|P\rangle$ may be an unknown state, Bob cannot judge directly whether or not the decoded state is the same as the received message state. To verify the authenticity of the signature, the original state $|P\rangle$ and the decoded state $|P'\rangle$ need to be compared. To compare in detail these states, the controlled-swap approached [41] presented in Section 3.5.3 may be still employed here, the details is the same as that described in previous section for the arbitrated quantum signature scheme.

6.7.2 Security Analysis

According to the security requirements of the quantum signature, the above scheme is unconditional security since the attacker (including dishonest Bob) cannot obtain useful information on the private key from public parameters, i.e., the original message state and public key, and the signatory cannot

disavow the signature. This subsection presents a detail security analysis of the presented true quantum signature algorithm.

Consider firstly the impossibility of disavowal for the signatory. If Alice disavows her signature, it is very easy to discover it, because Alice's key is contained in the signature $|S\rangle$. Thus, if Alice and Bob get into a dispute because of Alice's disavowal, they just need to send the signature $|S\rangle$ and message to the arbitrator. If the signature $|S\rangle$ can be decoded by Alice's public key k_v, this signature has been carried out by Alice, otherwise, the signature has been forged by Bob or the attacker. Obviously, the arbitrator is only in the position to judge whether Alice has disavowed her signature when the dispute or disagreement occurs.

Then, other possible attack strategies are investigated through the following theorems.

Theorem 6.7.2 Given a message state $|P\rangle$ and its signature $|S\rangle$ generated by Eq.(6.7.13). Let $|S'\rangle = |\widetilde{S}'\rangle \otimes |\widetilde{\Omega}'\rangle$, where $|\widetilde{S}'\rangle$ and $|\widetilde{\Omega}'\rangle$ are a $2k$-particle entangle state and a two-particle entangle state, respectively. Then $|S'\rangle$ is the signature of the message state $|P\rangle$ if and only if $|S'\rangle = |S\rangle$, and two states, i.e., $|S\rangle$ and $|S'\rangle$, are constructed under the same private key k_s.

Proof Consider the situation of given a private key. Suppose that there is another signature $|S'\rangle$ of the given message state $|P\rangle$, i.e., both $|S'\rangle$ and $|S\rangle$ are simultaneously the different signature of the same message state $|P\rangle$, and

$$|S'\rangle \neq |S\rangle. \tag{6.7.15}$$

Then, in terms of Eq.(6.7.13) and definition of $|S'\rangle$ one acquires,

$$|\widetilde{S}'\rangle \otimes |\widetilde{\Omega}'\rangle \neq |\widetilde{S}\rangle \otimes |\widetilde{\Omega}\rangle. \tag{6.7.16}$$

Applying $U(T)$ on Eq.(6.7.16) gives

$$|P'\rangle \otimes |\Gamma'\rangle \otimes |\widetilde{\Omega}'\rangle \neq |P\rangle \otimes |\Gamma\rangle \otimes |\widetilde{\Omega}\rangle. \tag{6.7.17}$$

where $|\Gamma\rangle = J|T|^{1/2} \prod_{i=2}^{k} |\Omega\rangle_{r_i, r_{i+k-1}}$ and $|\Gamma'\rangle = J'|T'|^{1/2} \prod_{i=2}^{k} |\Omega'\rangle_{r_i, r_{i+k-1}}$. For a given private key k_s, above equation gives

$$|P'\rangle \neq |P\rangle, \tag{6.7.18}$$

which is inconsistent with the assumption. Accordingly, one must have the following result,

$$|S'\rangle = |S\rangle. \tag{6.7.19}$$

Secondly, suppose that there are two different keys k_s^1, k_s^2 with $k_s^1 \neq k_s^2$, and these keys create the same signature for a given message state $|P\rangle$, i.e., $|S'\rangle_{k_s^1} = |S\rangle_{k_s^2}$. Since $|\omega(\mathbf{x})\rangle$ is generated from the private key, one gets two different states, i.e., $|\omega^1(\mathbf{x})\rangle$ and $|\omega^2(\mathbf{x})\rangle$, which corresponds to k_s^1 and k_s^2, respectively. From Eq.(6.7.10) one obtains,

$$|\widetilde{S}'\rangle_{k_s^1} = \int |P\rangle |\omega^1(\mathbf{x})\rangle \mathrm{d}\mathbf{x}, \tag{6.7.20}$$

and

$$|\widetilde{S}\rangle_{k_s^1} = \int |P\rangle|\omega^2(\mathbf{x})\rangle \mathrm{d}\mathbf{x}. \tag{6.7.21}$$

Then

$$\int |P\rangle(|\omega^1(\mathbf{x})\rangle - |\omega^2(\mathbf{x})\rangle)\mathrm{d}\mathbf{x} = 0. \tag{6.7.22}$$

Since $|P\rangle \neq 0$, above equation gives $|\omega^1(\mathbf{x})\rangle = |\omega^2(\mathbf{x})\rangle$, subsequently, $k_s^1 = k_s^2$, which contradicts the assumption.

Theorem 6.7.2 implicates the signature state is unique for a given message state with a given private key k_s, i.e., a given message state generating a unique signature state and vice versa. Since the attacker doesn't know the private key k_s, a forged signature $|S'\rangle$ which is not consistent with Eq.(6.7.13) leads $|S'\rangle \neq |S\rangle$, and subsequently Eq.(6.7.18) exists. According to the verification phase, different inputs $|P\rangle$ and $|P'\rangle$ will be detected easily with a measurement result "1" in the employed controlled-swap approach. While signature states created under different signature keys are different, subsequently the attacker may be detected by employing Step v3 in the verification phase. Thus the attacks' forgery shall be not successful, which means this kind of attack strategies cannot be succeeded.

Besides the above situation, the attacker cannot forge the signature for a given message by employing the public parameters k_v, $|P\rangle$ and $|\widetilde{\Omega}\rangle$. This conclusion is given in the following theorem.

Theorem 6.7.3 Let $|P\rangle$ be a given message state which may be a known state or an unknown state, and $|S\rangle$ be an unknown signature state. Then the signature state $|S\rangle$ may not be derived from the public key k_v and the transmitted states $|P\rangle$ and $|\widetilde{\Omega}\rangle$ in channel.

Proof Theorem 6.7.1 and definitions of k_s and k_v show that the transformation from the public key to private key is impossible, i.e.,

$$k_v \nrightarrow k_s, \tag{6.7.23}$$

where the symbol $A \nrightarrow B$ denotes that from A to B is impossible. Therefore,

$$Q^{k_v}|P\rangle \nrightarrow Q^{k_s}|P\rangle \tag{6.7.24}$$

where Q^{k_v} denotes an quantum algorithm controlled under the key k_v. From the signature phase, one may find the following transformation,

$$Q^{k_s}|P\rangle \longrightarrow |\widetilde{S}\rangle. \tag{6.7.25}$$

For a fixedly private key, Eqs.(6.7.24) and (6.7.25) give

$$Q^{k_v}|P\rangle \nrightarrow |\widetilde{S}\rangle. \tag{6.7.26}$$

In addition, the clone of the state $|\widetilde{\Omega}\rangle$ is impossible according to the quantum no-clone theorem since it is an unknown state. Thus the signature cannot be created by the public parameters k_v, $|P\rangle$ and $|\widetilde{\Omega}\rangle$.

In theorems 6.7.2 and 6.7.3, the message state is given, i.e., there is no forgery on the message state. However, the following situation always exist in practices. Suppose that the attacker has forged a message state $|\widehat{P}\rangle$ and created a forged signature $|\widehat{S}\rangle$. Since the attacker does not possesses the private key k_s, the signature $|\widehat{S}\rangle$ must be created by another key $\widehat{k}_s$. However, the forged message and signature cannot pass successfully the verification phase according to the following theorem.

Theorem 6.7.4 Let $|P\rangle$ and $|\widehat{P}\rangle$ be the original message state and a forged message state, respectively. If these states are different, i.e., $|\widehat{P}\rangle \neq |P\rangle$, any operation $\mathcal{E}$ cannot give a legitimate signature state so that the verification phase can be passed.

Proof To forge a message state $|\widehat{P}\rangle$ which is different from the original message state $|P\rangle$, and then generate a legitimate signature state based on the forged message state $|\widehat{P}\rangle$, the state $|\widehat{P}\rangle$ needs to be encoded by employing Eq.(6.7.10) and a two-particle state $|\widetilde{\Omega}\rangle$ needs to be prepared. However, the legitimate signature key is absent to the attacker, then a forged key $\widehat{k}_s$ would be used. Let $|\widehat{\omega}\rangle$ be generated by the key $\widehat{k}_s$, one gets

$$|\widehat{S}\rangle = \int |\widehat{P}\rangle|\widehat{\omega}\rangle \mathrm{d}\mathbf{x}. \tag{6.7.27}$$

Since the key-pair, i.e., k_s and k_v, is a strict one-way mapping, any forgery on the private key results in destruction of the transformation relationship between the private key k_s and the public key k_v. Due to the state $|\widehat{\omega}\rangle$ does not match up the verification key k_v, applying the unitary operator U on the state $|\widehat{S}\rangle$ will not accord with Eq.(6.7.14). Accordingly, any operation $\mathcal{E}$ cannot give a legitimate signature state so that the verification phase can be passed.

Due to the unitary property of the operator U in the verification key, there is a special case in Theorem 6.7.4 which is demonstrated in the following corollary.

Corollary 1 Let $|P\rangle$ and $|\widehat{P}\rangle$ be an original message state and a forged message state, respectively. Making use of the unitary transformation U and the forged message state $|\widehat{P}\rangle$ may generate a new signature state $|X\rangle$. However, the generated state $|X\rangle$ cannot pass the verification phase.

Proof Suppose that the attacker prepares a forged state $|F\rangle$ to forge the signature by employing the inverse of U as follows. Applying the inverse of the unitary operation U and a forged message state $|\widehat{P}\rangle$, the attacker creates a state $|X\rangle$,

$$|X\rangle = U^{-1}|F\rangle, \tag{6.7.28}$$

where U^{-1} denotes the inverse of the unitary operation U, and $|F\rangle$ is the state associated with the forged message state $|\widehat{P}\rangle$. The generated state $|X\rangle$ is regarded as a signature state by the attacker. Then the attacker sends the state $|\widehat{P}\rangle$ together with $|X\rangle$ and a two-particle state $|\widehat{\Omega}\rangle$ which plays the same role as the state $|\widetilde{\Omega}\rangle$ to Bob. In the following we prove the impossibilities of

forging successfully the signature by using U^{-1}. Three situations are analyzed in the follows. Firstly, suppose that $|F\rangle$ is a product-state of the state $|\widehat{P}\rangle$ and $k-1$ two-particle entangled states, i.e., $|F\rangle = |\widehat{P}\rangle \otimes |F_\omega\rangle$, where $|F_\omega\rangle$ denotes the product-state of $k-1$ two-particle entangled states. Apparently, attacker's strategy can pass the verification without Step v1 in the verification phase. However, since the forged signature state $|X\rangle$ is not a quantum error correction code, Bob cannot obtain a corrected value of the error syndrome in Step v1. Thus the state $|X\rangle$ cannot pass the verification. Secondly, suppose that $|F\rangle$ is a $2k$ particles entanglement state and $|X\rangle$ is a quantum error correction code which is different from the state $|S\rangle$. In this case, the first step in the verification phase can be passed. However, attacker's strategy cannot pass Steps v2 $-$ $v4$. Even if Step v2 has been passed, Steps v3 and v4 cannot be bypassed since the attacker does not possess the private key. Finally, if $|F\rangle$ is an arbitrary mixed state of $2k$ particles, Theorem 6.7.4 has shown the impossibility of passing the verification.

There is a special situation for Theorem 6.7.4, i.e., the initial message state and forged state are symmetrical. Easily, one may find that this attack strategy is also impossible. It is shown in the following corollary.

Corollary 2 The attack strategy using a symmetrical state of the message state as the forged message state cannot be successful.

Proof The symmetrical state, which satisfies $|P\rangle|P'\rangle = |P'\rangle|P\rangle$, can pass the verification. Fortunately, this situation follows still the verification algorithm since one can easily obtain $|P'\rangle = c|P\rangle$, where c is a constant which can be eliminated by the normalization treatment. Accordingly, $|P\rangle$ and $|P'\rangle$ represent the same message state. This means that there exists no forgery in this case. Another case is that the message state is an entangled symmetric state. For simplicity, we consider an entangled symmetric state with two particles, e.g., p_1 and p_2. Then the message state can be written as $|\psi(p_1, p_2)\rangle$,

$$|\psi(p_1, p_2)\rangle = \frac{1}{\sqrt{2}} \left(|p_1\rangle|p_2\rangle + |p_2\rangle|p_1\rangle\right). \tag{6.7.29}$$

Suppose that an entangled symmetrical state $|\psi'\rangle = |\psi(p_2, p_1)\rangle$ has been exploited to forge the original message by the signatory or Oscar. Making use of the quantum nature of the symmetrical state, i.e, $|\psi(p_2, p_1)\rangle = |\psi(p_1, p_2)\rangle$, one can easily obtain $|\psi'\rangle = |\psi(p_1, p_2)\rangle$. Accordingly, $|\psi'\rangle$ and $|\psi\rangle$ denote the same message, which means no any forgery can be succeeded via such a kind of symmetrical states.

A more interest trick exploiting the entangled symmetric state is describe as follows. A message is encoded in the state $|\psi(p_1, p_2)\rangle$, however, the signature state is generated employing only one particle (e.g., p_1) and another particle p_2 is sent to Bob as if it was the message. Fortunately, this trick is unavailable, which can be demonstrated by using at least three ways. Firstly, this trick cannot pass the verification in Step v1. When one employs the above trick to generate the signature, the generated signature should be a $(2k+1)$-

particle quantum error-correction code. At Step v1, the obtained value of error syndrome is $s_e = 2k + 1$ when Bob induces one bit-flip error on the final particle in the code. Accordingly, this thick cannot pass the verification since $s_e \neq 2k$. In addition, this kind of trick does not follow the nature of the quantum signature scheme since only one particle (e.g., p_2) in a two-particle entanglement state cannot denote a determined message. One should note here again the difference between the quantum signature and qubit signature as mentioned in Section 6.5. Subsequently, this trick may be detected by the arbitrator when Alice and Bob have disputes. Furthermore, this trick can also be prevented directly by employing a simple quantum error-correction code. Before performing the comparison of $|P\rangle$ and $|P'\rangle$ in Step v4, Bob encodes the particle p_2 with two ancilla $|0\rangle$ states, then a three qubits bit-flip code is generated [**?**]. If p_1 and p_2 are not entangled, the encoding procedure is

$$|P\rangle|P'\rangle \rightarrow |C_1\rangle = (a|000\rangle + b|111\rangle) \otimes (a'|0\rangle + b'|1\rangle), \tag{6.7.30}$$

where $|P\rangle = a|0\rangle + b|1\rangle$ and $|P'\rangle = a'|0\rangle + b'|1\rangle$ are exploited with $|a|^2 + |b|^2 = 1$ and $|a'|^2 + |b'|^2 = 1$. If p_1 and p_2 consist of an entangled symmetrical state $|\psi(p, p')\rangle$, the encoding procedure is denoted as

$$\begin{aligned} |P\rangle|P'\rangle + |P'\rangle|P\rangle \rightarrow & |C_2\rangle \\ = & (a|000\rangle + b|111\rangle) \otimes (a'|0\rangle + b'|1\rangle) + \\ & (a'|000\rangle + b'|111\rangle) \otimes (a|0\rangle + b|1\rangle). \end{aligned} \tag{6.7.31}$$

Apply the operator σ_x on the fourth particle which is equivalent to introduce a bit-flip error on the codes $|C_1\rangle$ and $|C_2\rangle$. Simple calculation shows that syndromes of codes $|C_1\rangle$ and $|C_2\rangle$ are 0 and 4, respectively. Then, what Bob needs to do is to measure the error syndromes of these codes. If the syndrome $s = 4$ which corresponds to the code $|C_2\rangle$, Bob judges that p_1 and p_2 are entangled and rejects the signature. Otherwise Bob recovers the states of particles p_1 and p_2 by applying σ_x^{-1} on the fourth particle in code $|C_1\rangle$ and then decoding the code $|C_1\rangle$ according to the theory of quantum error-correction codes. After having finished these operations, Bob moves on to the remained steps.

According to the above theorems, one may find that if Oscar can get the private key, i.e., the signature key k_s, the forgery attack strategy is possible. Fortunately, this strategy may not be successful since the attacker, i.e., Oscar, cannot get useful information on the private key. Let K_s, K_v, S, and P be random variables corresponding to the private key k_s, the public key, i.e., the verification key k_v, signature state $|S\rangle$, and message state $|P\rangle$, respectively. Suppose that the attacker employs an arbitrary attacking strategy $\mathcal{E}$ on the proposed algorithm. The random variable of the attacking strategy is denoted E. Then, at the situation of given the public key, signature, and message states, there is a bound on information of the attacker obtaining, which can be described by the following theorem.

Theorem 6.7.5 Let $I(K_s, E|K_v, S, P)$ be the Shannon mutual information between the random variables K_s and E given K_v, S, P, i.e., given the public key K_v, message state P, and its signature S. For every $\sigma > 0$, $\xi > 0$, and $L^{max} > 0$, the mutual information what the attacker obtains about the private key K_s is less than $\sigma/\ln 2 + L^{max}\xi$.

Proof In Shannon theory, the condition mutual information is defined as

$$I(X, Y|Z) = \sum_z p(z) \left(H_z(X) - H_z(X|Y)\right), \tag{6.7.32}$$

where $H_z(X)$ and $H_z(X|Y)$ are defined respectively by

$$H_z(X) = -\sum_{x,y} p(x, y|z) log_2 p(x), \tag{6.7.33}$$

and

$$H_z(X|Y) = -\sum_{x,y} p(x, y|z) log_2 p(x|y). \tag{6.7.34}$$

From Theorems 6.7.2 and 6.7.3 one obtains $S(|P\rangle) = |S\rangle$, thus

$$p(K_v, S, P) = p(K_v, S). \tag{6.7.35}$$

Note the public key K_v and S are independent, and the determined public key in the proposed algorithm leads $K_v(\mathcal{E}) = k_v$ so that $p(K_v) = 1$. Thus one has

$$p(K_v, S) = p(K_v)p(S) = p(S). \tag{6.7.36}$$

In addition, the secrecy of signature states depends directly on the private key K_s via a one-to-one mapping according to Eq.(6.7.10), then,

$$p(S) = p(K_s). \tag{6.7.37}$$

Combining Eqs.(6.7.35),(6.7.36), and (6.7.37) yields

$$p(K_v, S, P) = p(K_s). \tag{6.7.38}$$

For simplicity, substitute $\{K_v, S, P\}$ using a new symbol $\{\Theta\}$ in the follows. According to Eq.(6.7.32), the mutual information between K_s and E given K_v, S, P is expressed as

$$I(K_s, E|\Theta) = \sum_{k_s} p(k_s) \left(H_{k_s}(K_s) - H_{k_s}(K_s|E)\right). \tag{6.7.39}$$

Since $p(k_s) = \sum_{k_s, \mathcal{E}|K_s(\mathcal{E})=k_s} P(k_s, \mathcal{E})$, above equation gives

$$\begin{aligned} I(K_s, E|\Theta) &= \sum_{k_s,\mathcal{E}} p(k_s, \mathcal{E}) \left(H(K_s) + \log_2 p(k_s|\mathcal{E})\right), \\ &= \sum_{k_s,\mathcal{E}} p(k_s, \mathcal{E}) H(K_s) + \sum_{k_s,\mathcal{E}} p(k_s, \mathcal{E}) \log_2 p(K_s|\mathcal{E}). \end{aligned} \tag{6.7.40}$$

Denote the event $\mathfrak{E}$ which is true whenever the attacker can obtain information on the private key from the public parameters, i.e., K_v, S and P, then one obtains

$$\sum_{k_s,\mathcal{E}} p(k_s,\mathcal{E})H(K_s) = \sum_{k_s,\mathcal{E}|\mathfrak{E}} p(k_s,\mathcal{E})H(k_s) + \sum_{k_s,\mathcal{E}|\overline{\mathfrak{E}}} p(k_s,\mathcal{E})H(k_s), \quad (6.7.41)$$

where $\overline{\mathfrak{E}}$ denotes the events which are not included in the event $\mathfrak{E}$. This property exists also for the second term in Eq.(6.7.40). Since the event of $\mathcal{E} \in \overline{\mathfrak{E}}$ implies $H(K_s) = 0$ and $p(k_s|\mathcal{E}) = 1$. Eq.(6.7.40) is rewritten as

$$I(K_s, E|\Theta) = \sum_{k_s,\mathcal{E}|\mathfrak{E}} p(k_s,\mathcal{E}) \left\{H(k_s) + \log_2 p(k_s|\mathcal{E})\right\}. \quad (6.7.42)$$

Define a new event $\mathfrak{N}_\sigma$ which is true whenever the attacking strategy $\mathcal{E}$ is σ-information about k_s, where the conception of σ-information about variable ζ is borrowed from Ref.[?]. Then one gains the following expression for any $\sigma \geq 0$ in the event $\mathfrak{N}_\sigma$,

$$\left| p(k_s|\mathcal{E}) - 2^{-H(k_s)} \right| \leq 2^{-H(k_s)}\sigma. \quad (6.7.43)$$

Making use of the event $\mathfrak{N}_\sigma$, Eq.(6.7.42) is rewritten as

$$\begin{aligned} I(K_s, E|\Theta) = & \sum_{(k_s,\mathcal{E})|\mathfrak{F}} p(k_s,\mathcal{E}) \left\{H(k_s) + \log_2 p(k_s|\mathcal{E})\right\} + \\ & \sum_{(k_s,\mathcal{E})|\mathfrak{E}\cap\bar{\mathfrak{F}}} p(k_s,\mathcal{E}) \left\{H(k_s) + \log_2 p(k_s|\mathcal{E})\right\} \leq \\ & \sum_{(k_s,\mathcal{E})|\mathfrak{F}} p(k_s,\mathcal{E}) \log_2(1 + \lambda_{k_s,\mathcal{E}}) + \\ & \sum_{(k_s,\mathcal{E})|\mathfrak{E}\cap\bar{\mathfrak{F}}} p(k_s,\mathcal{E})H(k_s), \end{aligned} \quad (6.7.44)$$

where $\mathfrak{F} = \mathfrak{N}_\sigma \cap \mathfrak{E}$, and $\lambda_{k_s,\mathcal{E}} \leq \sigma$.

Let L^{max} be the maximal Shannon entropy of $H(k_s)$, and $Pr(\mathfrak{E}\cap\bar{\mathfrak{F}}) \leq \xi$, where the probability $Pr(\cdot)$ is defined by $Pr(X) = Pr(X = x)$. Making use of the inequality $\log_2(1+x) \leq |x|/\ln 2$ for any $x > -1$, one obtains finally,

$$I(K_s, E|K_v, S, P) \leq \frac{\sigma}{\ln 2} + L^{max}\xi. \quad (6.7.45)$$

Theorem 6.7.5 gives an upper bound on the amount of information of what the attacker can obtain. Since σ and ξ are any positive numbers, Eq.(6.7.45) shows that the mutual information $I(K_s, E|K_v, S, P)$ may be arbitrary small even tending to zero. Thus the attacker cannot obtain useful information on the private key by any attacking strategy, although there are publicly given parameters, i.e., $K_v, |P\rangle$, and $|S\rangle$. Therefore, the private key is unconditional security.

6.8 Quantum Channel Authentication

Comparing to the classic private communication, a distinct feature of the quantum private communication is that any disturbance on the channel can be detected in principle using quantum laws. An approach has been described in Chapter 4 for the eavesdropping detection in the QKD scheme. For example, to detect disturbance of the attacker or environment on a channel, in the BB84 protocol the qubits which are transmitted from Alice are measured randomly by Bob. Then Alice and Bob compare their measurement results. With the error rate and Heisenberg uncertainty principle, the disturbance is detected. Cryptographically, this approach involves the so-called channel authentication.

There exit several drawbacks in the above approach which has been employed in the QKD scheme. First, a classic channel is necessary so that the quantum communication system becomes complicated. Secondly, the transmitted qubits employed for the quantum channel authentication are destroyed, subsequently, they cannot be utilized again. In addition, perfectness of the channel is verified by only using a small fraction of qubits without strict proof. This section introduces an new approach which uses entanglement property. In this approach, perfectness of the involved quantum channel can be verified without destroying the employed qubits.

Suppose that the pre-shared quantum channel between Alice and Bob consists of N entanglement states pairs. Each state is expressed by the following maximally entangled state (MES),

$$|\Phi_j^+\rangle = \frac{1}{\sqrt{2}}\left(|0_a^j 0_b^j\rangle + |1_a^j 1_b^j\rangle\right), \tag{6.8.1}$$

where $j = 1, 2, \ldots, n$, subscripts a, b refer to Alice's and Bob's particles denoted by p_a^j and p_b^j, respectively, in the MES. Making use of a random number θ_j, Alice prepares a qubit expressed by

$$|\psi_m^j\rangle = \cos\theta_j|0\rangle + \sin\theta_j|1\rangle. \tag{6.8.2}$$

Let particle p_m^j carry the qubit $|\psi_m^j\rangle$. Alice applies a controlled-NOT gate C_{am} on the entangled particle p_a^j and particle p_m^j. The employed quantum controlled-NOT gate C_{am} may be public, i.e. anybody knows this gate. The above operation entangles the particle p_m^j and particles p_a^j and p_b^j. Then these particles become a three-particle entangled state, which has the following form,

$$\begin{aligned}
|\psi_c^j\rangle &= C_{am}|\Phi_j^+\rangle|\psi_m^j\rangle \\
&= \sum_{l=0,1} \gamma_l(|0_a 0_b l_m\rangle + |1_a 1_b (l\oplus 1)_m\rangle) \\
&= \frac{1}{\sqrt{2}}\sum_{l=0}^{1} |l_a l_b\rangle \otimes (\mathbf{I}\delta_{l,0} + X_m\delta_{l,1})\,|\psi_m^j\rangle,
\end{aligned} \tag{6.8.3}$$

where $\gamma_l = (\alpha\delta_{l0} + \beta\delta_{l1})/\sqrt{2}, \alpha = \cos\theta_j, \beta = \sin\theta_j$, the subscript m specifies the particle p_m^j, and X_m is a X gate to the particle p_m^j. After this operation Alice sends the particle p_m^j to Bob. Please note here the state of particle p_m^j is different from its initial state, i.e., the state presented in Eq.(6.8.2).

When receiving this particle p_m^j, Bob applies a quantum logic gate C_{bm} on the particles p_b^j and p_m^j. If there is no disturbance on the channel, Bob's operation gives

$$C_{bm}|\psi_c^j\rangle = |\Phi_j^+\rangle \otimes |\psi_m^j\rangle. \tag{6.8.4}$$

The above equation means that the three-particle entangled state is disentangled. Thus the state of the particles p_m^j is independent of the MES pair after Bob's operation. However, if there is a disturbance on the channel, Eq.(6.8.4) cannot be obtained. Suppose that the attacker introduces an ancilla state $|E_{init}\rangle$ to entangle the MES, then a composite state is given by

$$|\Phi_{ABE}\rangle = |\Phi_j^+\rangle \otimes |E_{init}\rangle. \tag{6.8.5}$$

Attacker's arbitrary operation $\mathcal{E}$ on the state $|\Phi_{ABE}\rangle$ by employing a unitary transformation $U(\mathcal{E})$ yields

$$\begin{aligned} U(\mathcal{E})|\Phi_{ABE}\rangle = {} & |0_a0_b\rangle \otimes |E_1\rangle + |0_a1_b\rangle \otimes |E_2\rangle + \\ & |1_a0_b\rangle \otimes |\tilde{E}_1\rangle + |1_a1_b\rangle \otimes |\tilde{E}_2\rangle, \end{aligned} \tag{6.8.6}$$

where the Schmidt decomposition has been employed [**?**], $|E_1\rangle \perp |E_2\rangle$ and $|\tilde{E}_1\rangle \perp |\tilde{E}_2\rangle$. Thus Eq.(6.8.3) is rewritten as

$$\begin{aligned} |\psi_{c'}^j\rangle &= C_{am}\left(U(\mathcal{E})|\Phi_{ABE}\rangle\right)|\psi_m^j\rangle \\ &= \frac{1}{2}\left[\cos\theta_j|0_a0_b0_m\rangle + \sin\theta_j|0_a0_b1_m\rangle\right] \otimes |E_1\rangle + \\ &\quad \frac{1}{2}\left[\cos\theta_j|0_a1_b0_m\rangle + \sin\theta_j|0_a1_b1_m\rangle\right] \otimes |E_2\rangle + \\ &\quad \frac{1}{2}\left[\cos\theta_j|1_a0_b1_m\rangle + \sin\theta_j|1_a0_b0_m\rangle\right] \otimes |\tilde{E}_1\rangle + \\ &\quad \frac{1}{2}\left[\cos\theta_j|1_a1_b1_m\rangle + \sin\theta_j|1_a1_b0_m\rangle\right] \otimes |\tilde{E}_2\rangle, \end{aligned} \tag{6.8.7}$$

and Eq.(6.8.4) becomes

$$\begin{aligned} C_{bm}|\psi_{c'}^j\rangle = {} & \frac{1}{2}\left[\cos\theta_j|0_a0_b0_m\rangle + \sin\theta_j|0_a0_b1_m\rangle\right] \otimes |E_1\rangle + \\ & \frac{1}{2}\left[\cos\theta_j|0_a1_b1_m\rangle + \sin\theta_j|0_a1_b0_m\rangle\right] \otimes |E_2\rangle + \\ & \frac{1}{2}\left[\cos\theta_j|1_a0_b1_m\rangle + \sin\theta_j|1_a0_b0_m\rangle\right] \otimes |\tilde{E}_1\rangle + \\ & \frac{1}{2}\left[\cos\theta_j|1_a1_b0_m\rangle + \sin\theta_j|1_a1_b1_m\rangle\right] \otimes |\tilde{E}_2\rangle \\ \neq {} & |\Phi_j^+\rangle \otimes |\psi_m^i\rangle. \end{aligned} \tag{6.8.8}$$

The above equation shows that the entanglement state and the probing particle state cannot construct a product state after Bob's operation if there exists arbitrary disturbance.

Consider a more general case for the two-particle entangled state. Suppose that the distributed entanglement state is as follows,

$$|\phi_j^+\rangle = \sum_{i=1}^{4} \lambda_i^j |\mu_i^a \nu_i^b\rangle, \tag{6.8.9}$$

where $\mu_i^a, \nu_i^b \in \{0,1\}$. Applying a controlled-NOT operation on particles p_a^j and p_m^j yields

$$C_{am}|\phi_j^+\rangle|\psi_m^j\rangle = \sum_{i=1}^{4} \left(\lambda_i^j \cos\theta_j |\mu_i^a \nu_i^b \mu_i^a\rangle + \lambda_i^j \sin\theta_j |\mu_i^a \nu_i^b (\mu_i^a \oplus 1)\rangle\right). \tag{6.8.10}$$

After received the particle p_m^i, Bob's decoding operation outputs the following state,

$$\begin{aligned}
|\psi_b\rangle &= C_{bm}\left(C_{am}|\phi_j^+\rangle|\psi_m^j\rangle\right) \\
&= \sum_{i=1}^{4} \left(\lambda_i^j \cos\theta_j |\mu_i^a \nu_i^b (\mu_i^a \oplus v_i^b)\rangle + \lambda_i^j \sin\theta_j |\mu_i^a \nu_i^b (\mu_i^a \oplus \nu_i^b \oplus 1)\rangle\right) \\
&= \sum_{i=1}^{4} |\phi_j^+\rangle \otimes \left(\cos\theta_i |\mu_i^a \oplus v_i^b\rangle + \sin\theta_i^b |\mu_i^a \oplus \nu_i^b \oplus 1\rangle\right), \\
&= \begin{cases} |\phi_j^+\rangle \otimes |\psi_m^j\rangle, & \text{if} \quad \mu_i^a = \nu_i^a, \\ |\phi_j^+\rangle \otimes C|\psi_m^j\rangle, & \text{if} \quad \mu_i^a \neq \nu_i^a. \end{cases}
\end{aligned} \tag{6.8.11}$$

Generally, the state $|\phi_j^+\rangle$ is known to the communicators, i.e., Alice and Bob, in a determined quantum communication scheme, above equation shows that the output state of the particle p_m^j is determined after C_{bm} operation. The above equation implies that the state $|\psi_m^j\rangle$ can be obtained exactly after Bob's operation.

Suppose that the attacker employs an arbitrary strategy $\mathcal{E}$ to disturb the channel. In a same way, one can easily verify that the product state of the entangled state and the probing state does not exist under attacker's disturbance, i.e.,

$$C_{bm}\left(C_{am}(|\varphi\rangle|\psi_m^j\rangle)\right) \neq \begin{cases} |\phi_j^+\rangle \otimes |\psi_m^j\rangle, & if \quad \mu_i^a = \nu_i^a, \\ |\phi_j^+\rangle \otimes X_m|\psi_m^j\rangle, & if \quad \mu_i^a \neq \nu_i^a, \end{cases} \tag{6.8.12}$$

where $|\varphi\rangle$ is expressed by

$$|\varphi\rangle = U(\mathcal{E})(|\phi_j^+\rangle \otimes |E_{init}\rangle).$$

Employing the above mechanisms, we now show how to verify the perfectness of the involved channel associated with the state $|\Phi_j^+\rangle$ or $|\phi_j^+\rangle$. Since two situations can be verified using the same approach, only the former is described in the follows.

Suppose the parameter θ_j in the probing qubit $|\psi_m^j\rangle$ is only known to Alice. In this situation, Bob returns the decoded particle p_m^j to Alice. After received the qubit from Bob, Alice identities whether or not the state of the received particle is the same as the original probing state by measuring the received particle p_m^j. If Alice's measurement results show that θ_j is the same as the original one, the involved channel is perfect and no disturbance exists. Obviously, Eq.(6.8.8) cannot give an exact θ_j since the state $C_{bm}|\psi_{c'}^j\rangle$ is entangled among the entangled particles, probing particle, and attacker's ancilla particle. Subsequently, Alice cannot always get an exact parameter θ_j. However, Eq.(6.8.4) shows that the state $C_{bm}|\psi_c^j\rangle$ is a product state of the probing particle p_m^j and entangled particles p_a^j and p_b^j. The parameter θ_j can be obtained exactly. Therefore Eq.(6.8.4) demonstrates that the involved channel is perfect.

In case of verifying the quality and the integrity of the whole quantum channel, Alice and Bob alternately repeat Eqs.(6.8.3) and (6.8.4). For example, Alice does the operation on particles p_a^j and p_m^j according to Eq.(6.8.3). After Bob decodes the qubit $|\psi_m^j\rangle$, he entangles the received particle (denoted by p_m^{j+1} for convenience) with particles p_b^{j+1} in the state $|\Phi_{j+1}^+\rangle$ as Alice has done in Eq.(6.8.3), and sends the particle p_m^{j+1} to Alice. After receiving the p_m^{j+1} particle, Alice verifies the channel. These procedures is executed step by step until N entangled pairs have been verified. If Alice and Bob obtain the results shown in Eq.(6.8.4) for the whole quantum channel, the channel is judged to be perfect. In this way, any disturbance on the channel can be detected. Obviously, this approach can be employed for checking the eavesdropping in QKD.

Actually, the approaches presented in Section 3.5.3 are also suitable for the quantum channel authentication. In this case, the state $|\psi_m^j\rangle$ may be unknown. One may analyze this way as that used in the quantum signature algorithm.

References

[1] Schneier B (1994) Applied cryptography: protocols, algorithms, and source code in C. Wiley, New York

[2] Zeng G H (2006) Quantum cryptology. Science Press, Beijing

[3] Simmons, G J (1988) Message authentication with arbitration of transmitter/ receiver disputes. In: Nyberg Kaisa, Hartmanis J, Nyberg K (eds) Advances in Cryptology-EUROCRYPT 98, Espoo, Finland, May/June 1998. Lecture Notes in Computer Science (LNCS), Springer, Heidelberg, 304: 151 – 165

[4] You H, Zhou F (1995) Construction of Cartesian authentication codes from pseudo symplectic geometry. Journal of Information Optimal Science, 16: 113 – 125

[5] Curty M, Santos D J (2001) Quantum authentication of classical messages. Physical Review A, 64: 062309

[6] Curty M, Santos D J, Pérez E, et al (2002) Qubit authentication. Physical Review A, 66: 022301

[7] Wegman M N, Carter J L (1981) New hash function and their use in authentication and set equality. Journal of Computer and System Science, 22: 265 – 287

[8] Dušěk M, Haderka O, Hendrych M, et al (1999) Quantum identification system. Physical Review A, 60: 149 – 156

[9] Zeng G H, Zhang W P (2000) Quantum identity verification. Physical Review A, 61: 1 – 5

[10] Ljunggren D, Bourennane M, Karlsson A (2000) Authority-based user authentication in quantum key distribution. Physical Review A, 62: 1 – 7

[11] Shi B, Li J, Liu J, et al (2001) Quantum key distribution and quantum authentication based on entangled state. Physics Letters A, 281: 83 – 87

[12] Mihara T (2002) Quantum identification schemes with entanglements. Physical Review A, 65: 052326

[13] Zhou N R, Zeng G H, Zeng W J, et al (2005) Cross-center quantum identification scheme based on teleportation and entanglement swapping. Optics Communications, 254: 380 – 388

[14] Meijer H, Akl S G (1981) Digital signature schemes. Advances in Cryptology-Proceedings of Crypto 81: IEEE Workshop on Communications Security, Santa Barbara, August 1981, 65 – 70

[15] Zeng G H, Keitel C H (2002) An arbitrated quantum signature algorithm. Physical Review A, 65: 1 – 8

[16] Lee H, Hong C, Kim H. et al (2004) Arbitrated quantum signature scheme with message recovery. Physics Letter A, 321: 295 – 300

[17] Lü X, Feng D G (2004) An arbitrated quantum message signature scheme. International Symposium on Computational and information Science, Shanghai, 15 – 17 December 2005. Lecture Notes in Computer Science (LNCS), Springer, Heidelberg, 3314: 1054 – 1060

[18] Fujiwara A (2001) Quantum channel identification problem. Physical Review A, 63: 1 – 4

[19] Zeng G H (2004) Quantum authentication without lost of quantum channel. ChinCrypt'2004, pp 141 – 146

[20] Simmons, G J (1979) Authentication without secrecy: A secure communication problem uniquely solvable by asymmetrical encryption techniques. Proceedings of IEEE EASCON 79, Washington, DC, 9 – 11 October, pp 661 – 662

[21] Simmons, G J (1985) Authentication theory/coding theory. Advances in Cryptology-Proceedings of Crypto 84, Barbara, 19 – 22 August 1984. Lecture Notes in Computer Science (LNCS), Springer, Heidelberg, 196: 411 – 431

[22] Nielsen M A, Chuang I L (2000) Quantum computation and quantum information. Cambridge University Press, London

[23] Zhang Z S, Zeng G H, Zhou N R, et al (2006) Quantum identity authentication based on ping-pong technique for photons. Physics Letters A, 356(3): 199 – 205

[24] Biham E, Huttner B, Mor T (1996) Quantum cryptographic network based on quantum memories. Physical Review A, 1996, 2651

[25] Boström K, Felbinger T (2004) Deterministic secure direct communication using entanglement. Physical Review Letters, 89: 1 – 4

[26] Wójcik A (2004) Eavesdropping on the "Ping-pong" quantum communication protocol. Physical Review Letters, 90: 1 – 4

[27] Holevo A S (1973) Statistical problems in quantum physics. Proceedings of the second Japan-USSR Symposium on probability theory, Kyoto, 1972. In: Maruyama and Prokhorov J V (eds) Lecture Notes in Math. Springer, Berlin, 330: 104 – 119

[28] Gisin N, Ribordy G, Tittel W, et al (2002) Quantum cryptography. Reviews of Modern Physics, 74: 145 – 195

[29] Deutsch D, Ekert A, Jozsa R (1996) Quantum privacy amplification and the Security of quantum cryptography over noisy channels. Physical Review Letters, 77: 2818 – 2821

[30] Acín A, Cirac J I, Lewenstein M (2007) Entanglement percolation in quantumnetworks. Nature (London), 3: 256 – 259

[31] Kwiat P G, Mattle K, Weinfurter H, et al (1995) New high-intensity source of polarization-entangled photon pairs. Physical Review Letters, 75: 4337 – 4340

[32] Acín A (2001) Statistical distinguishability between unitary operations. Physical Review Letters, 87: 177901

[33] Sacchi M F (2005) Optimal discrimination of quantum operations. Physical Review A 71: 062340

[34] Duan R, Feng Y, Ying M (2008) Local distinguishability of multipartite unitary operations. Physical Review Letters, 100: 020503

[35] Zeng G H, Lee M H, Guo Y, et al (2007) Continuous variables quantum siganture signature algorithm. International Journal of Quantum Information, 5(3): 553 – 573

[36] Cleve R, Gottesman D, Lo H K (1999) How to share a quantum secret. Physical Review Letters, 83: 648 – 651

[37] Tyc T, Sander B C (2002) How to share a continuous-variable quantum secret by optical interferometry. Physical Review A, 65: 042310

[38] Braunstein S L, Loock P V (2005) Quantum information with continuous variables. Reviews of Modern Physics, 77: 513 – 577

[39] Grosshans F, Assche G V, Wenger J, et al (2003) Quantum key distribution using Gaussian-modulated coherent states, Nature, 421: 238 – 241

[40] Bennett C H, Brassard G, Mermin N D (1992) Quantum cryptography without Bell's theorem. Physical Review Letters, 68: 557 – 559

[41] Buhrman H, Cleve R, Watrous J, et al (2001) Quantum Fingerprinting. Physical Review Letters, 87: 167902

[42] Mayers D (2001) Unconditional security in quantum cryptography. Journal of the ACM, 48: 351 – 406

[43] Peres A (1997) Quantum Theory: Concepts and Methods. Kluwer Academic Dordrecht

7 Private Communication Using Single Photon Signal

The physical implementation of the quantum private communication is an important issue. This chapter introduces how to implement experimentally the private communication in quantum ways using single photon signals. Core techniques such as the single photon signal generation, transmission, detection, and discrete-variable qubit preparation are introduced. Then several experimental systems for the quantum private communication are exemplified.

The basic theory and typical schemes of the quantum private communication have been presented in the previous chapters. Since the implementation of the quantum private communication is an important issue, the final part of this book focuses on various physical implementation techniques of the private communication in quantum ways. Basically, there are two ways for implementing the private communication in quantum ways. One is the way of using the single photon signal, and the other is implemented using the continuous variable quantum signal. Based on these implementation ways, typical techniques of the quantum private communication have been applied in several practical communication systems.

This chapter describes the physical implementations of the quantum private communication using single photon signals. From the viewpoint of communication, the single photon signal sources, physical transmission properties of single photon, and detection techniques of the single photon signals are introduced. Then basic principles of both one-way and two-way quantum key distribution (QKD) schemes in fiber are described. Finally, some typical quantum private communication techniques such as experimental implementations of QKD with Einstein-Podosky-Rosen (EPR) entanglement state and QKD in free space are presented.

7.1 Single photon Source

Generally, to transmit information from one communicator to others through a physical channel, a suitable signal should be adopted to carry the encoded information. Since its excellent transmission properties, the optical quantum

signal is often used to carry the information which is encoded using qubits in a quantum communication system. There are several typical optical quantum signals including the single photon signal, coherent state signal, squeezing state signal, etc. Currently, the single photon signal is always employed to implement the quantum private communication with discrete variable qubits, while the coherent state signal and squeezing state signal are associated with the quantum private communication using continuous variable qubits. In this section, several single photon sources based on various technologies are introduced, and their advantages and drawbacks are compared.

7.1.1 Basic Principle

To understand the physical nature of the single photon signal, the Fock state is recalled briefly. In quantum mechanics, a Fock state is any state of the Fock space with a well-defined number of particles, e.g., photon, in each state. Thus, a Fock state is also called a number state. For simplicity, we limit to a single mode in the follows. Then, a Fock state is of the type $|n\rangle$ with n an integer value. Fock states form the most convenient basis of the Fock space. They are defined to obey the following relations,

$$\begin{cases} \hat{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle, \\ \hat{a}|n\rangle = \sqrt{n}|n-1\rangle, \end{cases} \tag{7.1.1}$$

where $\hat{a}\dagger$ and $\hat{a}$ are annihilation operator and creation operator for single mode, respectively. Using Eq.(7.1.1), one obtains a general expression of the Fock state,

$$|n\rangle = \frac{1}{\sqrt{n!}}\hat{a}^\dagger|0\rangle, \tag{7.1.2}$$

where $|0\rangle$ corresponds to the ground state. It has the following properties,

$$\begin{cases} \langle\hat{a}^\dagger\hat{a}\rangle = \mu, \\ Var(\hat{a}^\dagger\hat{a}) = 0, \end{cases} \tag{7.1.3}$$

where μ is the mean photon number. Defining a photon number operator $\hat{n} = \hat{a}^\dagger\hat{a}$, one obtains $\mu = \langle\hat{n}\rangle$.

Clearly, a single photon signal is exactly a Fock state with $n = 1$. That is, a single photon signal holds the state $|1\rangle = \hat{a}^\dagger|0\rangle$ in the Fock space. Accordingly, a single photon signal is a state of the most convenient basis of the Fock space.

In principle, the single photon signal is an excellent quantum signal for the quantum private communication system since the security could be guaranteed well in this situation. However, it is difficult to realize experimentally. Nowadays, most practical implementations rely on a faint laser source, where the photon number distribution of each pulse obeys the Poisson statistics.

This way leads to a small probability of generating more than one photon at a time. Even if the loss of quantum channel is very large, this small possibility of multi-photons can cause serious secure problems, e.g., the well-known photon-number splitting (PNS) attack. With fast development of the quantum private communication and quantum information technology, the call for true single photon sources is becoming more and more significant [**?**].

7.1.2 Faint Laser Pulses

The easiest way to approximate single photon source is to attenuate coherent light with ultra-low mean photon number μ in each pulse by using standard semiconductor lasers and calibrated attenuators. This kind of quantum signals is usually called a faint laser pulse or a dim laser pulse. According to this preparation way for the faint laser pulse, such kind of quantum signals is actually a special coherent state with smaller μ, i.e., $\mu \ll 1$.

A coherent state can be expressed generally in following form which will be described in detail in Section 8.1.1,

$$|\alpha\rangle = a_0|0\rangle + a_1|1\rangle + \ldots + a_n|n\rangle + \ldots, \tag{7.1.4}$$

where n denotes photon numbers. In the output pulse, the probability to have n photons in a coherent light pulse follows the Poisson statistics,

$$P(n,\mu) = \frac{\mu^n}{n!}\mathrm{e}^{-\mu}. \tag{7.1.5}$$

When $\mu \ll 1$, the probability of an empty pulse is

$$P(0,\mu) = \mathrm{e}^{-\mu} \simeq 1 - \mu + \frac{\mu^2}{2}, \tag{7.1.6}$$

and the probability of a pulse with only one photon is

$$P(1,\mu) = \mu\mathrm{e}^{-\mu}. \tag{7.1.7}$$

In addition, the probability of a pulse with multi-photon is

$$P(n>1,\mu) = 1 - (1+\mu)\mathrm{e}^{-\mu}. \tag{7.1.8}$$

Consequently, the probability that a non-empty pulse with multi-photons is

$$\begin{aligned} P(n>1,\mu|n>0,\mu) &= \frac{P(n>1,\mu)}{P(n>0,\mu)} \\ &= \frac{1-\mathrm{e}^{-\mu}(1+\mu)}{1-\mathrm{e}^{-\mu}} \\ &\simeq \frac{\mu}{2} \end{aligned} \tag{7.1.9}$$

Clearly, there exits empty pulse, single photon pulse, and multi-photon pulse in the prepared faint laser pulse quantum signal. The empty pulse

is not available for the private communication, and the multi-photon pulse could be split by eavesdropper for the PNS attack as mentioned in Chapter 4. Consequently, the value of μ cannot be too large, also, it cannot be too small.

In practice, the detectors' dark count which not only decreases the communication rate but also increases the quantum bit error rate in the QKD scheme is an important issue. This prevents the use of really low photon numbers and most experiments rely on $\mu = 0.1$. As pointed out by Brassard in 2000 [**?**], there is an optimal μ depending on the transmission loss. After key distillation, the security is just as good with faint laser pulses as with real single photon states, and the tradeoff lies in a reduction of the bit rate.

7.1.3 Single photon Source with Quantum Dots

As mentioned above, making use of a faint laser pulse the prepared quantum signal has drawbacks on the security, dark count and empty pulse. Accordingly, preparing a true single photon source becomes very necessary. Physically, the desired source must emit consecutive photons that have identical wave packets. Semiconductor quantum dots are good candidates for this task since they exhibit a strong photon antibunching in their emission statistics under suitable excitation conditions. The so-called photon antibunching is associated with a sub-Poisson statistic, which is a photon number distribution for which the variance is less than the mean. A coherent light pulse, as output by a laser far above threshold has Poissonian statistics, while a thermal light pulse has super-Poisson statistics. One may easily check that the number fluctuations in the thermal case are larger than a coherent state, but for an antibunched light source they are smaller.

The second-order correlation function $g^{(2)}(0)$ (for zero delay time) may be used to described the photon antibunching. It reads as

$$g^{(2)}(0) = \frac{\langle (\hat{a}\dagger)^2 \hat{a}^2 \rangle}{\langle \hat{a}\dagger\hat{a} \rangle^2}. \tag{7.1.10}$$

According to the quantum theory presented in Chapter 2, one has

$$\langle \triangle \hat{n}^2 \rangle - \langle \hat{n} \rangle = \langle (\hat{a}\dagger)^2 \hat{a}^2 \rangle - (\langle \hat{a}\dagger\hat{a} \rangle)^2, \tag{7.1.11}$$

where $\langle \triangle \hat{n}^2 \rangle = Var(\hat{n})$ and $\langle \hat{n} \rangle$ denote the variance and average of the photon number distribution, respectively. Combining the above two equations, one obtains

$$\frac{\langle \triangle \hat{n}^2 \rangle - \langle \hat{n} \rangle}{\langle \hat{n} \rangle^2} = g^{(2)}(0) - 1. \tag{7.1.12}$$

Then the characteristics of the photon antibunching satisfying the sub-Poisson photon statistics yields the definition as follows,

$$g^{(2)}(0) < 1. \tag{7.1.13}$$

The condition in the above expression has become one of important ways for judging photon antibunching characteristics. Since the second-order correlation function $g^{(2)}(0)$ can be measured physically, one may give an experimental judgement.

The frequency of the emitted photon depends on the number of electron-hole pairs present in the quantum dot. After one creates several such pairs by optical pumping or electrically pumping, they will sequentially recombine and hence emit photons at different frequencies. Then, by spectral filtering a single photon pulse is obtained. If quantum dots are planted on a large semiconductor material, output efficiency for coupling into optical fiber is inefficient. In order to strongly enhance the spontaneous emission, these dots can be integrated in solid-states micro-cavities.

A triggered single photon emission from site-controlled InGaAs/AlGaAs quantum dots grown in inverted pyramids has been demonstrated [**?**]. The corresponding second-order correlation functions $g^{(2)}(\tau)$ are shown in Fig.7.1, where $X - X$ denotes the correlation between two single photons. In this figure, both traces exhibit a clear reduction of the probability of multi-photon emission since $P(0)$ has a value below 0.5 (subsequently, $g^{(2)}(\tau) < 1$) as pointed out by Zwiller and his coworkers in 2001 [**?**]. And the single photon counting rate exceeded 2×10^5 cts/s, where the unit cts/s is the abbreviation of "counts/s". When transition was driven close to saturation, resulting in an overall detection probability of $p > 5\%$ for detecting a photon per excitation pulse.

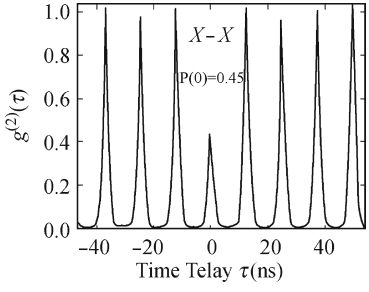

Fig. 7.1. Second-order correlation functions $g^{(2)}(\tau)$ for triggered single photon emission from site-controlled InGaAs/AlGaAs quantum dots

Although single photon sources based on quantum dots have a potential to be widely used in the future, by far it still suffers from many disadvantages. For example, they must work in a very low temperature, the wavelength of output photons are normally around 900 nm and cannot be tuned conveniently, and the output coupling efficiency is very low which is less than 40%. From the viewpoint of application in a communication system, the transmission distance is too short to be applied in practices. In addition, the single photon signal can not resist effectively the influences of the environment and noises.

7.1.4 Other Single photon Sources

A photon gun means that if and only if the source is triggered, one and only one photon is emitted. Besides the single photon source based on quantum dots, there are essentially three different experimental approaches that show photon anti-bunching and come more or less close to this ideal.

A first idea is based on single atom and ion. A stimulated Raman process drives an adiabatic passage between two ground states of a single atom strongly coupled to a single mode of a high-finesse optical cavity. A laser beam illuminating the atom excites one branch of the Raman transition, while the cavity vacuum stimulates the emission of the photon on the other branch. These photons have the same frequency and a Fourier-transform limited linewidth, thus indistinguishable. Moreover, this process is unitary and therefore intrinsically reversible. Recently, a single photon source realized with a cold atomic ensemble has been presented [**?**]. A single excitation, written in an atomic quantum memory by Raman scattering of a laser pulse, is retrieved deterministically as a single photon at a predetermined time. A feedback circuit shows a promising performance in the enhancement of the production rate of single photons while the single photon quality is conserved. This single photon source based on an atomic ensemble has the advantages of narrow band, high quality, and controllable character. However, the manipulation of single atoms requires sophisticated techniques and expensive setups.

The second approach is to work with single nitrogen-vacancy (NV) centers in diamond for generating single photon [**?**]. This material combines the robustness of single atom with the simplicity of experiments with dye molecules. Fluorescence light observed from this NV center exhibits strong photon anti-bunching and the samples are stable at room temperature. The measured pair correlation function shows that only one photon is emitted at a time. However, the disadvantage is the collection efficiency, currently only about 0.1%, and the spectral bandwidth is broad, normally of the order of 100 nm.

Last but not the least, a mesoscopic p-i-n heterojunction driven by an alternating voltage source could be used to generate photons with a well-defined generation timing. The Coulomb blockade and quantum confinement effects together can suppress quantum fluctuations usually associated with electron and hole injection processes in semiconductors. Therefore, it is possible to generate heralded single photon state, i.e., single photon signal. In 1999, the first experimental result has been presented [**?**], but with very low efficiencies and only at temperature below 50 mK.

To sum up, today's single photon sources, except for the faint laser pulse, are still far from being widely used in the quantum communication, and subsequently the quantum private communication systems, because of their complexity in technical and expensiveness in cost. The most commonly used single photon source is still the faint laser pulse with extremely low mean photon numbers μ.

7.1.5 Entangled photon Pairs

Usually, the photon source which generates entangled single photon pairs is also regarded as a single photon source, since the generation of photon pairs provides a way of using one photon as a trigger for the another. In contrast to other sources, the second detector must be activated only when the first one detected a photon, hence circumventing the problem of empty pulse. Although due to limited coupling efficiency into optical fibers, the probability to find the signal photon after detection of the trigger photon can still reach about 2/3 in practical. Compared to the faint laser pulse, photon pairs allow thus to work with lower pulse rates and hence reduced detector-induced errors.

When a laser pump beam is incident upon a nonlinear crystal, pairs of photons that satisfy the type II phase-matching condition, which is described by the following expressions, are emitted.

$$\begin{cases} \omega_p = \omega_e + \omega_o, \\ K_p = K_e + K_o, \end{cases} \tag{7.1.14}$$

where ω denotes angular frequency, K is the wave-number vector, and subscripts p, o, e indicate the incident laser light, the fluorescence photons with ordinary and extraordinary polarization, respectively. The phase-matching allows to choose the wavelength, and determines the bandwidth of the down-converted photons. The number of photon pairs per mode is thermally distributed within the coherence time of photons, and follows a Poissonian distribution for larger time windows. Therefore, the source will either have a low probability of generating exactly one photon or a high probability of generating more than one photon. Clearly, from the viewpoint of the quantum private communication, this source is also not a perfect single photon signal source compared to the true single source signal.

Lately, researchers have proposed an experiment to outperform a simple Poisson distribution single photon source using spontaneous parametric down-conversion by pumping a relatively weak pulse to limit multiple-pair production [**?**]. If a single trigger photon is detected after the pump passes through the crystal, the signal photon switched into a storage cavity using another Pockels cell. If, in subsequent passes of the pump, a new pair of photons is generated, the new signal photon replaces the one previously stored. Replacing photons generated earlier reduces the effect of the cumulative loss of multiple cycles in the storage cavity. After a predetermined number of pump cycles, the photon is released. By keeping the average number of pairs produced low and allowing for many cycles of the pump, the probability of multiple-pair events can be decreased and the probability of a single photon being generated can be increased. This setup is capable of creating a single photon more than 70% of the time, while maintaining the probability of creating two or more photons less than 30%.

7.2 Transmission of Single photon Signal

To perform a common quantum communication or a quantum private communication, the generated quantum signal should be transmitted from a sender to receiver through a physical channel. This is associated with a quantum signal transmission. If the distance between two communicators is short, a direct transmission way in which quantum signal is sent directly from the sender to receiver without any operations during the transmission is enough. However, when two communicators are distant, the so-called quantum repeaters are necessary. Since the employed channels are lossy, any kind of transmissions for the quantum signal suffers from the channel loss. This is the same as that in the classic communication systems.

7.2.1 Transmission Mechanism

From the viewpoint of communication, mechanism of the quantum signal transmission is the same as that of the classic signal transmission. That is, both scenarios suffer from noise so that the transmission distance is limited. To extend the transmission distance, techniques such as the error correction codes should be exploited. However, there are natural differences between two scenarios in physical. In the quantum scenario, even if there are no channel noise, the signal transmission is also influenced by the vacuum fluctuation which does not exist in the classic scenario. Virtually, when a quantum signal is transmitted in a channel, the infinite-mode state of the environment will become entangled with the state of the quantum signal and, subsequently, will deteriorate the coherence of the system. This process is called decoherence which gives rise to the amplitude and phase decays of the transmitted quantum signal.

For simplicity, the decoherence of a B-qubit, which is suitable for describing the single photon signal, in a thermal bath environment has been investigated [**?**]. The bath is modeled by oscillators with infinite degrees of freedom that are described by annihilation, creation operators, and density distributed frequencies denoted $\hat{b}_\lambda$, $\hat{b}^\dagger_\lambda$, and ω_λ, respectively. The quantum signal is modeled by a B-qubit, $|\psi\rangle = c_1|0\rangle + c_2|1\rangle$, with a resonant transition frequency ω. In such a situation the interaction Hamiltonian of the total system has the following form in the interaction picture within the rotating wave approximation and the dipole approximation,

$$H_{sb} = \Gamma^\dagger_a \sigma^- + \Gamma^\dagger_p \sigma_z + H.c., \tag{7.2.1}$$

where $\Gamma^\dagger_a$ and $\Gamma^\dagger_p$ are the bath operators and may be expressed as sums over all modes of the baths (parametrised by λ),

$$\Gamma^\dagger_a = \sum_\lambda g_{a\lambda} b^\dagger_\lambda, \quad \Gamma^\dagger_p = \sum_\lambda g_{p\lambda} b^\dagger_\lambda, \tag{7.2.2}$$

and

$$\Gamma_a = (\Gamma_a^\dagger)^*, \quad \Gamma_p = (\Gamma_p^\dagger)^*. \tag{7.2.3}$$

$g_{\alpha\lambda}$ and $g^*_{\alpha\lambda}(\alpha \in \{a, p\})$ are the corresponding coupling coefficients between the signal and bath. σ^+, σ^- are raising and lowering operators operators defined via

$$\sigma^+ = |1\rangle\langle 0|, \quad \sigma^- = (\sigma^+)^* = |0\rangle\langle 1|, \tag{7.2.4}$$

and σ_z is given by

$$\sigma_z = |1\rangle\langle 1| - |0\rangle\langle 0|. \tag{7.2.5}$$

Employing the Markov approximation, the corresponding master equation of the two-state system in the interaction picture is written as [**?**]

$$\begin{aligned}\frac{\partial\rho}{\partial t} &= L_0\rho \\ &= \frac{\gamma_{\shortparallel}}{2}(N+1)\left([\sigma^-\rho, \sigma^+] + [\sigma^-, \rho\sigma^+]\right) + \\ &\quad \frac{\gamma_{\shortparallel}}{2}N\left([\sigma^+\rho, \sigma^-] + [\sigma^+, \rho\sigma^-]\right) + \\ &\quad \frac{\gamma_p}{4}\left([\sigma_z\rho, \sigma_z] + [\sigma_z, \rho\sigma_z]\right),\end{aligned} \tag{7.2.6}$$

where L_0 is the Liouvillian operator, $\gamma_{\shortparallel}$ and γ_p describe the amplitude and phase decay rates described by the following forms,

$$\gamma_\alpha = 2\pi \sum_\lambda g^2_{\alpha\lambda}\delta(\omega_\lambda - \omega). \tag{7.2.7}$$

Under the condition of a thermal equilibrium, N has the following form,

$$N = \left[\mathrm{e}^{\hbar\omega/k_BT} - 1\right], \tag{7.2.8}$$

with T being the temperature of the environment, and k_B the Boltzmann constant.

Formulating Eq. (7.2.6) in terms of the matrix elements yields

$$\frac{\partial\rho_{11}}{\partial t} = -\gamma\rho_{11} + \theta, \tag{7.2.9}$$

and

$$\frac{\partial\rho_{12}}{\partial t} = -D\rho_{12}, \tag{7.2.10}$$

where $\gamma = \gamma_{\shortparallel}(2N+1)$ and $\theta = \gamma_{\shortparallel}(N+1)$. Consequently, the off-diagonal term ρ_{12} evolves with the following decoherence rate,

$$D = \frac{\gamma_{\shortparallel}}{2}(2N+1) + \gamma_p. \tag{7.2.11}$$

Solving Eq.(7.2.10) gives

$$\rho_{12} = \mathrm{e}^{-Dt}\rho^0_{12}, \tag{7.2.12}$$

where ρ^0_{12} indicates the initial value of the coherence at time $t = 0$.

The decoherence rate D depends on the coupling coefficients $g_{\alpha\lambda}$. In addition, $g_{\alpha\lambda} \to 0$ leads to $D \to 0$, and consequently $\rho_{12} = \rho^0_{12}$, i.e. the coherence

of the signal is preserved. Accordingly, the decoherence is generated by the coupling between the signal and environment. This kind of coupling establishes an entanglement between the system and environment, however induces decoherence of the system. In order to prevent decoherence, the system must be decoupled from the environment. This can be done using the quantum error correction codes [**?**]. However, the quantum error correction codes are not practical by far.

Eq.(7.2.11) also shows that the decoherence rate D is associated with the temperature of the environment. In the low temperature case the decoherence parameter D satisfies the condition,

$$D_1 = N\gamma_{\shortparallel} + \gamma_p. \tag{7.2.13}$$

In the high temperature case the decoherence parameter D becomes

$$D_2 = \frac{\gamma_{\shortparallel}}{2} + \gamma_p = \gamma_{\perp}. \tag{7.2.14}$$

We note that the decoherence is only dependent on the transverse coupling coefficient $\gamma_{\perp}$. In a general situation, the decoherence rate decreases exponentially with the environmental temperature.

Usually, the single photon signal is transmitted in optical fiber or air channel. When the characteristic parameters of the fiber or air channel, i.e., the environment of the quantum signal, have been presented, the transmission properties of the quantum signals can be calculated.

7.2.2 Quantum Repeater

Currently, the quantum private communication over long distances is an important challenge. The direct transmission of single photon signals is limited by the transmission loss. For example, 1000 km of standard telecommunication optical fibers have a transmission loss of order 200 dB. Due to the combination of fiber losses and detectors' noise, the fiber-based quantum private communication systems are limited to hundreds of kilometers. In the QKD system, due to the dark count, whenever a photon is lost there is a chance that a dark count produces an error. Hence, when the probability of a dark count becomes comparable to the probability that a photon is correctly detected, the signal-to-noise ratio (SNR) tends to zero. To exchange information over a long distance, a so-called quantum repeater is likely to be required.

1) Measurement-based quantum repeater

The quantum nondemolition measurement is a special kind of quantum measurements as defined in Chapter 2. Since the qubit is not almost destructed under such a quantum measurement, it is often regarded as a kind of quantum repeaters. Here we call it as a measurement-based quantum repeater. Essentially, the quantum nondemolition measurements provide only

partial information while partially preserve the quantum state of the signal for subsequent users. Such schemes have been widely investigated for continuous variable systems, and recently received attention also for discrete qubits. However, symbols are necessarily encoded in states of a physical system, so the ultimate bound on the performances as a repeater is posed by quantum mechanics. In fact, a perfect quantum repeater cannot be achieved, for example, the quantum information cannot be perfectly copied neither locally nor at a distance. The trade-off between the information gain and quantum state disturbance can be quantified using the fidelity.

The operation of a generic scheme for indirect measurement as a quantum operation without referring to any explicit unitary realization consists of several measurement operators A_k, with the condition $\sum_k A_k^\dagger A_k = I$. Suppose that there is a quantum system prepared in a pure state $|\psi\rangle$. If the outcome k is observed at the output of the repeater, then the estimated signal state is given by $|\phi_k\rangle$, whereas the conditional state $|\psi_k\rangle = \dfrac{1}{\sqrt{p_k}} A_k |\psi\rangle$ is left for the subsequent user. The amount of disturbance is quantified by evaluating the overlap of the conditional state $|\psi_k\rangle$ to the initial one $|\psi\rangle$, whereas the amount of information extracted by the measurement corresponds to the overlap of the inferred state $|\phi_k\rangle$ to the initial one. The corresponding fidelities, for a given input signal $|\psi\rangle$, are given by

$$\begin{cases} F_\psi = \sum\limits_k |\langle\psi| A_k |\psi\rangle|^2, \\ G_\psi = \sum\limits_k p_k |\langle\psi|\varphi_k\rangle|^2, \end{cases} \tag{7.2.15}$$

where the average over outcomes have already been performed. The relevant quantities to assess the repeater are then given by the average fidelities,

$$F = \int_A \mathrm{d}\psi F_\psi, \quad G = \int_A \mathrm{d}\psi G_\psi, \tag{7.2.16}$$

which are obtained by averaging F_ψ and G_ψ over possible input states. F is referred to as the transmission fidelity and G as the estimation fidelity. Apparently if nothing is done, the signal is preserved thus $F = 1$, at the same time the estimation has to be random. While if the maximum information is gained on the signal hence $G = 1$, then the signal after this operation cannot provide any more information on the initial state. The fidelities F and G are not independent of each other. For randomly distributed qubits, assuming a two-dimensional Hilbert space, and with the set of all possible quantum states equal to the whole Bloch sphere, the bound that fidelities should satisfy according to quantum mechanics can be derived,

$$\left(F - \frac{2}{3}\right)^2 + 4\left(G - \frac{1}{2}\right)^2 \leq \frac{1}{9}. \tag{7.2.17}$$

From this equation, one gets the maximum transmission fidelity compatible with a given value of the estimation fidelity or, in other words, the minimum unavoidable amount of noise that is added to the knowledge about a set of signals if one wants to achieve a given level of information.

A class of optimal quantum repeaters for qubits is suggested in 2005 [**?**]. The schemes are minimal and optimal, since they involve a single additional probe qubit and provide the maximum information adding the minimum amount of noises. The information gain and state disturbance are quantified by fidelities which saturate the ultimate bound imposed by quantum mechanics for randomly distributed signals. In this figure, R_2 denotes a rotation operation for preparing a probe qubit $|\omega\rangle_p$ in 2-dimension Hilbert space. The measurement scheme is shown in Fig.7.2.

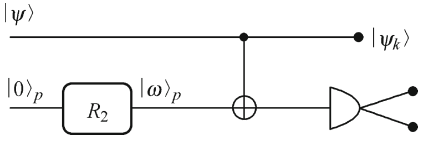

Fig. 7.2. An implementation schematic of a quantum repeater based on quantum nondemolition measurements

The signal qubit

$$|\psi\rangle = \cos\frac{\theta_1}{2}|0\rangle + \mathrm{e}^{\mathrm{i}\varphi_1}\sin\frac{\theta_1}{2}|1\rangle \tag{7.2.18}$$

is coupled with a probe qubit,

$$|\omega\rangle_p = \cos\frac{\theta_1}{2}|0\rangle_p + \mathrm{e}^{\mathrm{i}\varphi_2}\sin\frac{\theta_1}{2}|1\rangle_p \tag{7.2.19}$$

by a control-NOT gate denoted by C_{NOT}. The explicit dependence $F = F(G)$ can be written as,

$$F = \frac{2}{3}\left(1 + \sqrt{-9G^2 + 9G - 2}\right). \tag{7.2.20}$$

This function corresponds to the bound in Eq.(7.2.17) with the equal sign and therefore proves that the scheme is an optimal explicit unitary realization of a quantum repeater for qubits.

2) Entanglement-based quantum repeater

A usual way to implement the quantum repeater is using entangled photons pair and entanglement swapping operations. Since the decoherence of qubits in the quantum channel, which degrades the quality of entanglement between two particles, the entanglement degree is deduced gradually so that various errors are occurred on the entangled qubit, subsequently, the information may be lost. Accordingly, most quantum cryptographic schemes which employed entanglement require that two distant parties share highly

entangled photon pairs. Generally, the decoherence can be overcome by exploiting entanglement purification. Therefore, quantum repeaters, based on both the entanglement swapping [**?**] and entanglement purification [**?**], hold the promise to solve the problem of photon loss and detector noise as well as that of decoherence in a long-distance quantum communication.

In principle, an entanglement-based quantum repeater works as follows. Suppose that Alice and Bob need to share a maximally entangled state, but they are far apart. Alice can prepare an entangled state and send one-half to Bob. However, the further Alice and Bob are apart, the further the quantum system has to travel, and the fidelity F of the total state will decrease due to decoherence effects. Assume that the fidelity behaves exponentially, i.e.,

$$F \propto \exp(-L\gamma), \tag{7.2.21}$$

where L is the distance between Alice and Bob, and γ is the characteristic rate of deterioration for the traveling quantum system. Alice and Bob can use purification protocols to extract maximal entanglement, but such protocols break down below a minimum fidelity $F_{\min}$. The maximum distance of unaided quantum communication therefore has an upper bound. To overcome this limitation, divide the long channel into N smaller segments and create less distant entangled pairs across each segment. The number of segments N is thereby chosen in such a way that it is possible to create entangled pairs with sufficiently high initial fidelity $F > F_{\min}$ over the distance of such a segment and purification is possible. In this case, the fidelity decreases with a factor

$$\alpha = \exp(-L\gamma/N), \tag{7.2.22}$$

which is an exponential improvement. When the decrease in the fidelity is due to the attenuation of an optical beam in a fiber, the probability that a photon emitted by Alice reached Bob, without repeaters, is a^N. Therefore, Alice must send a^{-N} photons to Bob, in order to share one maximally entangled photon pair on average. Using quantum repeaters, every leg needs only $1/\alpha$ photons, and the total number of photons in all the legs is $1/(N\alpha)$. Thus, the quantum repeater transforms an exponential overhead into polynomial overhead. Fig.7.3 shows how a two-leg communication system with

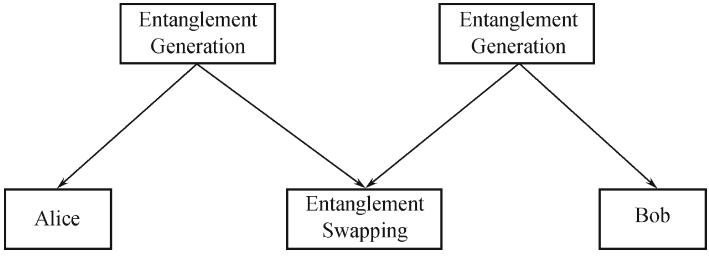

Fig. 7.3. A two-leg quantum repeater based on entanglement swapping

one quantum repeater is used to share maximal entanglement between Alice and Bob.

7.3 Single Photon Detection

As an important technique for detecting weak light, the single photon detection technique has been widely applied in many fields, such as physics, astronomy, chemistry, biology, medicine, and communication. The emergence of photonics applications requiring single photon detection has been driving significant advances in photon detectors with single photon sensitivity. The exploitation of quantum properties of photons for quantum cryptography and other quantum information processing techniques is critically dependent on single photon detection. The discrete-variable quantum private communication is implemented usually to used single photon signals to transmit information. Thus, single photon detectors with some key techniques such as coincidence measurement and count are necessary. To satisfy the requirements of quantum communication, the single photon detectors should have following properties:

- stable performance;
- high detection efficiency (as close to 100%);
- broadband (100 nm to 2000 nm);
- low dark count rate, that is no false counts and no after-pulsing;
- a good timing resolution;
- fast recovery.

Unfortunately, it turns out that it is impossible to meet all mentioned restricts above at the same time. This section introduces several typical methods and their principles for detecting single photon.

7.3.1 Photomultiplier Tubes

Photomultiplier tubes (PMTs), members of the class of vacuum tubes, are extremely sensitive detectors of light in the ultraviolet, visible, and near-infrared ranges of the spectrum. These detectors multiply the signal produced by incident light by as many as 100 million times, enabling single photons to be detected individually. PMTs are constructed from a glass vacuum tube, which consists of a photocathode, several dynodes, and an anode. Incident photons strike the photocathode material, which is present as a thin deposit on the entry window of the device, with electrons being produced as a consequence of the photoelectric effect. These electrons are directed by the focusing electrode toward the electron multiplier, where electrons are multiplied by the process of secondary emission. Fig.7.4 shows the schematic construction of a photomultiplier tube [**?**].

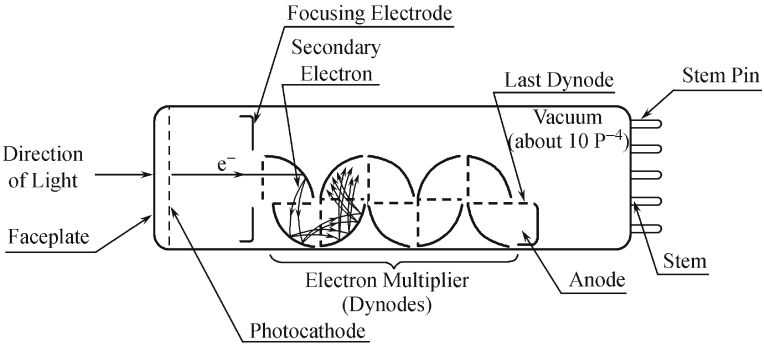

Fig. 7.4. Schematic construction of a photomultiplier tube

The electron multiplier consists of a number of electrodes, called dynodes. Each dynode is held at a more positive voltage than the previous one. The electrons leave the photocathode, having the energy of the incoming photon (minus the work function of the photocathode). As the electrons move toward the first dynode, they are accelerated by the electric field and arrive with much greater energy. Upon striking the first dynode, lower energy electrons are emitted, and these electrons in turn are accelerated toward the second dynode. The geometry of the dynode chain is such that a cascade occurs with an ever-increasing number of electrons being produced at each stage. Finally, the electrons reach the anode, where the accumulation of charge results in a sharp current pulse indicating the arrival of a photon at the photocathode.

PMTs typically utilize 1000 to 2000 volts to accelerate electrons within the chain of dynodes. The most negative voltage is connected to the cathode, and the most positive voltage is connected to the anode. Negative high-voltage supplies with the positive terminal grounded are preferred, because this configuration enables the photocurrent to be measured at the low voltage side of the circuit for amplification by subsequent electronic circuits operating at low voltage. While powered, photomultipliers must be shielded from ambient light to prevent their destruction through over-excitation.

The combination of high gain, low noise, high frequency response, and large area of collection has earned photomultipliers an essential place in nuclear and particle physics, astronomy, medical diagnostics and high-end image scanners known as drum scanners. On the other hand, photomultipliers are subject to damage from overexposure, bulky and requires a stable high-voltage power supply. Moreover, Photomultipliers for the infrared region suffer the additional disadvantage of having a low quantum efficiency and high dark current. Hence they are rarely used at telecommunication.

7.3.2 Single Photon Avalanche Diode

Semiconductor devices, particularly avalanche photodiodes, are alternatives to photomultipliers. Single photon avalanche diodes (SPADs) are based on a p-n junction reversed bias at a voltage higher than breakdown voltage. Its physical construction is plotted in Fig.7.5.

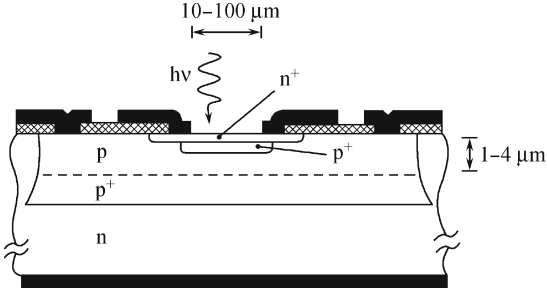

Fig. 7.5. Physical construction of single photon avalanche diode

At this bias, the electric field is so high that a single charge carrier injected in the depletion layer can trigger a self-sustaining avalanche. The current rises swiftly (sub nanosecond rise-time) to a macroscopic steady level, in the milliampere range. If the primary carrier is photo-generated, the leading edge of the avalanche pulse marks (with picosecond time jitter) the arrival time of the detected photon. The current continues to flow until the avalanche is quenched by lowering the bias voltage down to or below breakdown voltage: the lower electric field is not able any more to accelerate the carriers to impact-ionize with lattice atoms, therefore current ceases. In order to detect another photon, the bias voltage must be raised again above breakdown.

Clearly, these operations require a suitable circuit [**?**], which has to sense the leading edge of the avalanche current, generate a standard output pulse synchronous with the avalanche build-up, quench the avalanche by lowering the bias down to the breakdown voltage, restore the photodiode to the operative level. This circuit is usually referred to as a quenching circuit. Several typical quenching circuits are introduced as follows.

1) Passive quenching circuit

The simplest quenching circuit is commonly called Passive Quenching Circuit. It composes of a single resistor R_s in series to SPAD shown in Fig.7.6. In this figure, C_d is the junction capacitance typically 1 pF, and C_s is the stray capacitance to ground of the diode terminal connected to the load resistor R_L, typically a few picofarads. The diode resistance R_d is given by the series of space-charge resistance of the avalanche junction and of the ohmic resistance of the neutral semiconductor crossed by the current. The R_d value depends on the semiconductor device structure: it is lower than 500 Ω for the types

with a wide area and thick depletion layer and from a few hundred Ω to some kΩ for the devices with a small area and a thin junction. This experimental set-up has been employed since the early studies on the avalanche breakdown in junctions. The avalanche current self-quenches simply because it develops a voltage drop across a high-value ballast load R_L (about 100 kΩ or more). After the quenching of the avalanche current, SPAD bias slowly recovers to V_A, and therefore the detector is ready to be ignited again. Avalanche triggering corresponds to closing the switch in the diode equivalent circuit with an avalanche triggering voltage V.

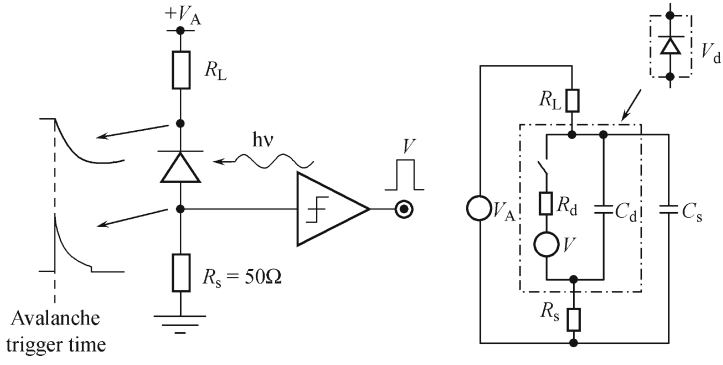

Fig. 7.6. Schematic of the passive quenching circuit

Fig.7.7 shows the typically waveforms of diode current I_d and diode voltage V_d. The diode voltage exponentially recovers toward the bias voltage (refer to the curve b in Fig.7.7) with time constant T_r, so that it takes about $5T_r$ to recover the correct excess voltage within 1%. Given the typical values of load R_L and of the total capacitance $C_s + C_d$, T_r is typically in the μs range. The maximum count rate varies from several hundred kHz to a few MHz.

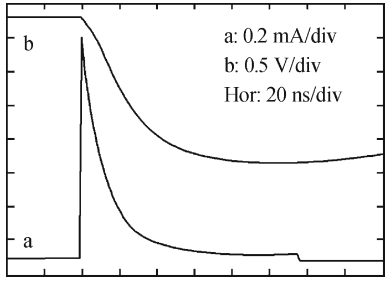

Fig. 7.7. Schematic passive quenching circuit

2) Active quenching circuit

To avoid disadvantages due to slow recovery from avalanche pulses, a new approach was suggested. The basic idea was simply to sense the rise of the avalanche pulse and feed back on SPAD, forcing the quenching and reset transitions in short times, with a controlled bias-voltage source. The basic active quenching circuit configuration is shown in Fig.7.8.

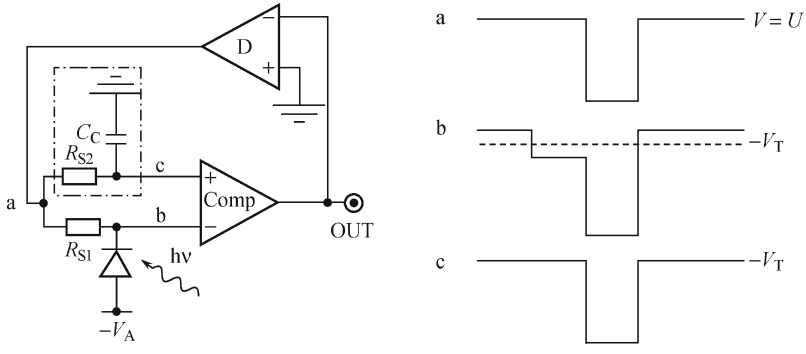

Fig. 7.8. Active quenching circuit

This configuration has the basic advantage of being suitable for various kinds of SPADs with any breakdown voltage because one of the device terminals is free, connected to ground, and is available for applying any required direct current (DC) bias voltage. The quenching pulse is applied to the same terminal and with the same polarity of the avalanche pulse; thus it locks the comparator in the triggered state unless suitable circuit means are provided to avoid it. A monostable circuit that limits the duration of the quenching pulse is a simple solution. By carefully designing, such a circuit produces clean rectangular pulses with fast transitions affected by minimal overshoots and ringings, typically limited from 1% to 3% of the pulse amplitude. However, the pulse amplitudes range from a few volts to tens of volts, this means overshoots from tens to hundreds of millivolts applied to the input. Since the circuit must be sensitive to pulses smaller than 50 mV, the overshoots on the reset transition can retrigger the comparator and drive the circuit into oscillation. The overshoots could be minimized by devising for the second generation active quenching circuit. A comparator with differential input is employed and the quenching pulse is applied to both terminals (common-mode signal), whereas the avalanche pulse is applied to one side only (differential signal). If the waveforms on the two input sides are identical, the action of the quenching pulse on the comparator is canceled. To equalize the shape of the pulse transitions, one can improve the input symmetry by adding a capacitor in parallel to the second terminal, emulating the detector capacitance.

3) Gated quenching circuit

Gated mode control including the electric pulse generation and its synchronization with the arriving the photon can reduce the quantum bit error rate from the thermal noise. Furthermore, gated operation can also be effective in avoiding the dark-count rate enhancement that is due to trapping effects in SPAD. As outlined in Fig.7.9, gated circuit configuration can have controlled input with either DC or alternating current (AC) coupling.

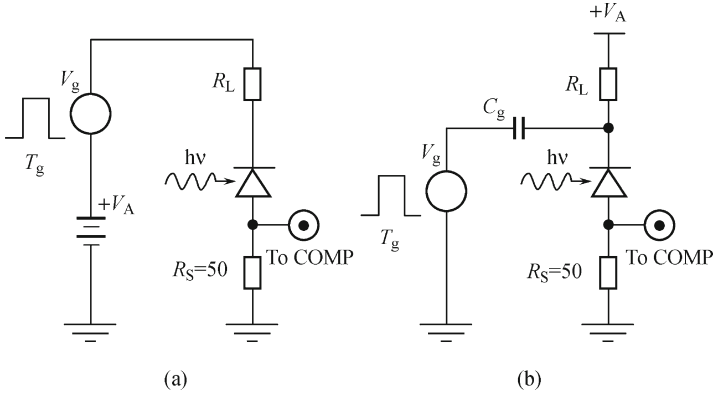

Fig. 7.9. Gated quenching circuit

A constant reverse bias is necessary to be high but under the breakdown voltage. In this case, a gate pulse with small amplitude can trigger an avalanche breakdown during sensing a signal with the fastest speed. The bias should be below the punch-through voltage from the theoretical consideration. The punch-through voltage is defined as voltage under which the depletion area has extended through the multiplication region and reaches the absorption layer. The bias should be below this level since the main noise existed in the absorption layer. The second role of the bias is to clear those trapped carriers in avalanche process by the defects in the semiconductor material. These trapped carriers can keep a relatively long time at low temperature, and the bias will accelerate the releasing of the trapped carriers. Therefore, both the bias and the bias time should be carefully considered that should be longer than the life time of the trapped carrier. In fact, it is not easy to produce an electric pulse below nanosecond time. The gate pulse is designed as few ns, and a square pulse is ideal to perform. In practice, the avalanche is triggered by the leading edge of the pulse. The steepness of the front edge of gate pulse and its time jitter which is synchronized with the arriving of the photon will decide the performance of the single photon detector. Gated mode operation is commonly used in quantum cryptography based on faint laser pulses where the arrival-times of the photons are well known. For 2-photon schemes, it is most often combined with one passive

quenched detector, generating the trigger signal for the gated detector.

The trade-off between dark count rate and photon detection rate is most fundamental. Increasing the avalanche probability by operating at larger excess bias ΔV increases the probability for both photo-excited and dark carriers to generate detectible avalanches; therefore, both dark count rate and photon detection rate increase. Moreover, if electric field-mediated dark carrier generation is significant at operating conditions of interest, the dark count rate will exhibit a faster increase with ΔV than photon detection rate. For applications required high counting rates ($\gg$ 1 MHz), a primary limitation is an effect known as after-pulsing. Avalanche events can create large instantaneous currents, and even with relatively fast quenching, the number of electrical carriers flowing through SPAD multiplication region is large. A small fraction of these carriers is trapped at defects within the multiplication region and are detrapped at a later time with an exponentially decaying behavior described by a detrapping time constant τ_d that is often on the scale of microseconds. If a carrier is detrapped after SPAD has been re-armed, this carrier can cause a dark count referred to as an after-pulsing. After-pulsing can be mitigated by imposing a sufficiently long "hold-off" time before rearming SPAD, but this approach limits the photon counting rate. For many single photon applications, the dark count rate and photon detection rate performance are satisfactory, and the counting rate limitation imposed by after-pulsing is the most crucial issue to be tackled.

Due to physical properties, most detectors are only efficient in a limited wavelength window. Fig.7.10 shows the quantum efficiency obtained for different materials.

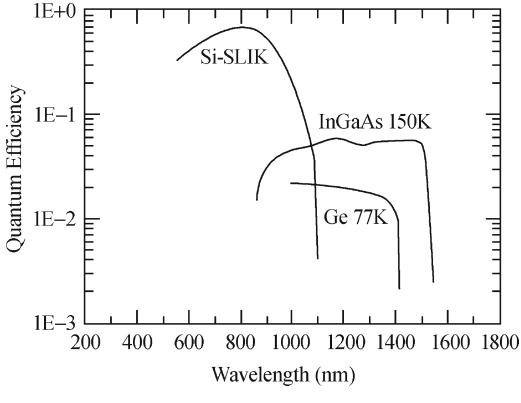

Fig. 7.10. Quantum efficiency as a function of wavelength for Silicon, Germanium, and InGaAs/InP APDs

Usually, three different semiconductor materials may be used: either Silicon, Germanium or Indium Gallium Arsenide (InGaAs), depending on the wavelengths. A lot of work has been done to characterize Silicon SPADs

for single photon counting. Commercial single photon counting modules are available, featuring quantum efficiencies of 70% at a wavelength of 700 nm, a time jitter of around 300 ps and maximum count rates larger than 5 MHz. When working at around 1300 nm, one has to take advantage of SPADs made from Germanium or InGaAs/InP semiconductor materials. In the 1550 nm, the only option is InGaAs/InP SPADs. No industrial effort has been done to optimize SPADs operating at telecommunication wavelength for photon counting, and their performance is still far behind the Silicon SPADs. Today, the quantum efficiency of InGaAs SPAD is only 25% at a wavelength of 1550 nm, and dark count rate is 10^{-5} per ns for gated on time. The performance of the single photon detector should be improved by the avalanche photodiode (APD) especially designed and manufactured for single photon detection.

7.3.3 Frequency Up-conversion

The idea of using the frequency up-conversion to facilitate a measurement in a bandwidth with better detection characteristics is not new. However, it is only with recent technological advances that this approach is being revisited to study the single photon detection regime for telecom wavelengths. As mentioned above, the InGaAs SPADs suffer from relatively low quantum efficiency, high dark counts and the need for cryogenic cooling. The efficiency limits the bit rate and achievable distance by the key distribution protocol. So by up-converting an infrared photon to a visible one, Si SPADs can be used, which have much lower noise and higher efficiency for visible wavelengths. The nonlinear process of frequency up-conversion can enable superior detectors of infrared photons. In the telecom band, there are now several groups investigating this approach using commercially available single photon counting modules, based on Si SPADs with periodically Poled Lithium Niobate (PPLN) crystals and either continuous or pulsed pump sources. To achieve high efficiency frequency up-conversion, an intense escort laser pulse, a very weak input laser, and a bulk crystal of PPLN was utilized. The resulting system up-converts one photon from the input beam and one photon from the escort beam into a single output photon. Due to energy conservation, the output frequency ω_o is the sum of the input frequency ω_{in} and the escort frequency ω_e, i.e., $\omega_o = \omega_{in} + \omega_e$. The relations that describe the nonlinear field evolution in a periodically poled nonlinear medium were given by Myers in 1995,

$$\frac{\mathrm{d}E_{in}}{\mathrm{d}z} = \mathrm{i}\frac{\omega_{in}\mathrm{d}_Q}{n_{in}c}E_o E_e^* \exp(\mathrm{i}\Delta k_Q z), \tag{7.3.1}$$

$$\frac{\mathrm{d}E_e}{\mathrm{d}z} = \mathrm{i}\frac{\omega_e\mathrm{d}_Q}{n_e c}E_o E_{in}^* \exp\left(\mathrm{i}\Delta k_Q z\right), \tag{7.3.2}$$

$$\frac{\mathrm{d}E_o}{\mathrm{d}z} = \mathrm{i}\frac{\omega_o \mathrm{d}_Q}{n_o c} E_{in} E_e \exp\left(-\mathrm{i}\Delta k_Q z\right), \tag{7.3.3}$$

where E_{in}, E_e, and E_o are the electric field strengths of the input, escort, output beams, respectively; n_{in}, n_e and n_o are the indices of refraction at the three frequencies; d_Q is the effective nonlinear coefficient; z is the longitudinal position within the crystal; and Δk_Q describes the phase mismatch with assumed to be zero for perfect phase-matching. Since the escort beam is not significantly depleted from the up-conversion of the input beam, one may let $\dfrac{dE_e}{dz} = 0$. Then equations can be reduced to two. Solving these equations under the initial condition $E_o(z = 0) = 0$ gives a sinusoidal oscillation output field amplitude, which can then be converted to a probability of up-conversion $P_o(z)$,

$$P_o(z) \propto \sin^2\left(A\sqrt{I_\varepsilon} z\right), \tag{7.3.4}$$

where A is a constant. For the spatial period L_c, the input light will be completely up-converted to the output frequency, and then down-converted back to the original input frequency before leaving the crystal. Hence for a given crystal with length L, by choosing the escort intensity to give $L_c = 2L$, one can achieve very high conversion efficiency.

Lately, a simple scheme for a compact and tunable single photon detector based on frequency up-conversion with high count rates and timing resolution at telecommunication wavelength has been presented [**?**]. The detection scheme is illustrated in Fig.7.11. Improvements in the fabrication of the PPLN, the filtering, as well as an optimization of the Si APDs, this scheme has seen overall detection efficiencies greater than 10% obtained.

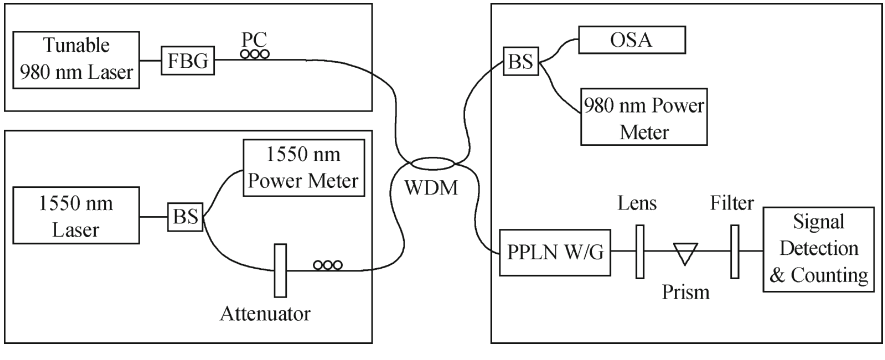

Fig. 7.11. A single photon detection scheme based on frequency up conversion

7.3.4 Quantum Dots Single photon Detector

As described in Section 7.1.3, the quantum dot can be used to implement a single photon source. Here we demonstrate another potential application of quantum dots for the detection of single, visible or near-infra red photons. The device structure consists of a modulation doped field effect transistor (FET) containing a layer of self-organized quantum dots separated from the conducting channel by a thin barrier layer. The capture of a single photo-excited carrier by a quantum dot produces a detectable change in the source-drain resistance of the transistor. This effect makes the device sensitive to individual photons in the incident light. The device is fundamentally different from other types of single photon detector such as PMT or APD, which rely upon an avalanche multiplication process to produce the gain required to measure a single photon. Fig.7.12 shows a schematic of the device structure.

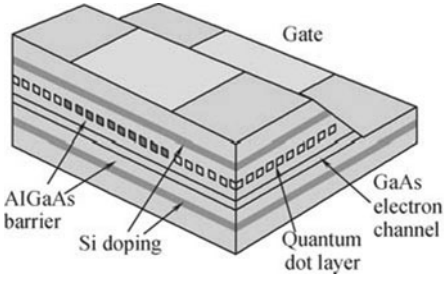

Fig. 7.12. Schematic structure of a detector based on quantum dot

Since the conduction band level in the quantum dots lies to lower energy than that in GaAs, each dot traps several excess electrons. The negative charge trapped in the dots raises the local electron potential and repels electrons in the near quantum well layer. As a consequence the energy of the conduction and valance band edges in the quantum well layer show strong spatial variations. Maxima form in the potential in the quantum well adjacent to each dot, where the excess electron density falls to zero. The presence of these electron-less regions in the two dimensional electron gas (2DEG) adjacent to each quantum dot, results in a relatively low electron mobility. The 2DEG density is initially set to a value for which the source-drain conductivity is low. Under these conditions, the channel current is extremely sensitive to the charge trapped in the dots. Thus capture of even a single photo-excited charge can produce a detectable change in the source-drain conductance. Absorption of a photon inside the semiconductor produces an electron-hole pair. One of these carriers can be captured by the quantum dot, thereby altering the height of the potential island in the adjacent 2DEG layer. For the example shown, the photo-excited hole will be attracted to the negatively charged quantum dot. Capture of a hole by the dot will reduce

its negative potential and increase the local electron density in the 2DEG layer, thereby increasing the 2DEG conductance. Thus if the active area of the device is sufficiently small, it could be possible to detect single photons.

Fig.7.13 shows experimental data taken at 4 K by Shields in 2000 [**?**]. The curve plots the change in source-drain conductance with time under very weak illumination by a LED. Prior to illumination, the gate is biased at 0.76 V, so as to recharge dots under the gate region with electrons, resulting in a low source-drain conductance initially. The steps observed are the response to the single photons.

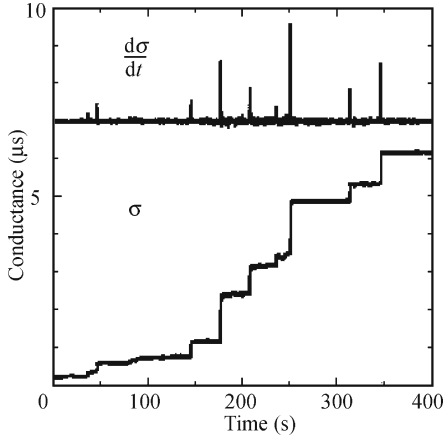

Fig. 7.13. Testing result of a detector based on quantum dot

The photon count rates measured here are limited by the lock-in detection system used to make the measurements. However, as the device is based upon a short gate FET, its intrinsic response time could be designed to be very short, allowing higher count rates to be detected. The quantum efficiency of the device can also be greatly increased by using a doped semiconductor, rather than the metal, layer on the front surface, and by increasing the thickness of the absorbing layer. If these challenges can be overcome, the quantum dot field effect transistor could provide a cheap, robust, and low voltage solution for single photon detection.

7.3.5 Superconducting Single photon Detector

Recently, a new class of ultrafast single photon detectors for counting both visible and infrared photons is presented. Superconducting devices are the natural choice for fast and ultrasensitive optical detection, because of their quantum nature and low-noise, cryogenic operation environment. The superconducting energy gap is two to three orders of magnitude lower than in a

semiconductor, thus, the photon absorption in a superconducting detector creates an avalanche electron charge two to three orders of magnitude higher for the same photon energy. This extends the range of detectable energies well into the infrared for photon detectors. In addition, the energy relaxation time constants of excited electrons in superconductors are in the picosecond range for both the low temperature and high temperature superconductors, assuring the gigahertz repetition rate for superconducting photon counters.

Single photon absorption, the subsequent quasiparticle avalanche, and the creation of a hotspot are very local, nanoscale events in superconducting films which are wide and/or thick compared to the quasiparticle diffusion length. Thus neither of these phenomena is going to produce an observable, macroscopic effect. However, if the superconducting single photon detector (SSPD) consists of a stripe with both its thickness and width comparable to few nanometers scale hotspot, the photon absorption results in a major perturbation and leads to a resistive barrier across the stripe. Since it is extremely difficult to fabricate few nanometers wide stripes, typically only the thickness of SSPD is comparable with the hotspot size. In this case, the device is maintained at a significantly low temperature, and needs to be biased with the current I_b close to the stripe's critical current I. The collective action of the hotspot formation and I_b redistribution results in the appearance of the macroscopic resistive barrier across the SSPD stripe. As illustrated in Fig.7.14 [**?**], after absorption of a photon, a hotspot region where superconductivity is suppressed or even destroyed is formalized. During the initial thermalization, the hotspot grows in size as hot electrons diffuse out of the hotspot core. The supercurrent, which biases the device, is expelled from the resistive hotspot volume and is concentrated in the "sidewalks" near the edges of the film. If the current density after this redistribution exceeds the critical value outside the hotspot, phase-slip centers are created

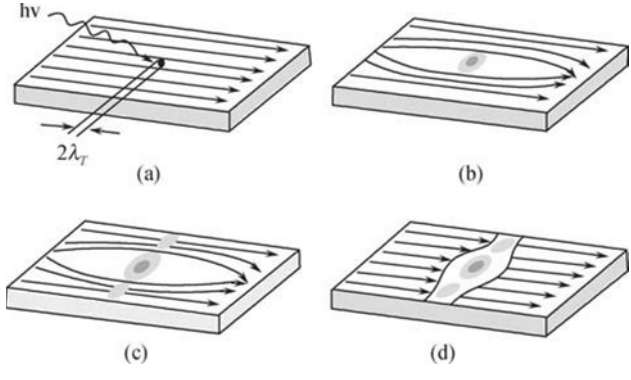

Fig. 7.14. Schematics of the supercurrent-assisted hotspot formation mechanism

in the sidewalks, the superconductivity is destroyed, and the resistive barrier is formed across the entire width of the device, which, in turn, gives rise to a

voltage signal with the amplitude proportional to I_b. After its growth phase, the hotspot decreases due to the relaxation and cooling of excited electrons and their out-diffusion. Thus, after 30 ps long quasiparticle relaxation time, the hotspot collapses, superconductivity is restored, and the detector is ready to register another photon.

In 2006, researchers in Russia developed an advanced SSPD structure with an optical microcavity optimized for absorption of 1550 nm photons. The design of an advanced SSPD structure consists of a quarter-wave dielectric layer, combined with a metallic mirror. And measurements demonstrate that implementation of the one-mirror resonant cavity allows to increase quantum efficiency of the detector at the resonant wavelength by factor of 3-to-4 compared to that of the detector without microcavity. Besides, they have fabricated and tested a fiber-based single photon receiver, designed for applications in practical quantum private communication systems. This integrated two-channel, single photon receiver based on fiber-coupled SSPDs is shown in Fig.7.15 [**?**]. Two SSPDs were placed at the bottom flange of a cryogenic insert. For fiber-coupling of SSPDs, photoresist rings were used fabricated on top of the detector by a photolithography process. The cross section through the coupling mechanical support for the fiber-detector consisting of the photoresist ring and two bridge-like aluminum holders. The estimated coupling efficiency of the fiber-detector setup is about 30%. This direct fiber-coupling implemented in SSPDs doesn't significantly reduce the time resolution of the iobium nitride (NbN) detectors. The real time counting rate of the receiver is about 1 GHz. The measured jitter was 35 ps. The value was somewhat longer than the best 18 ps, obtained in the non-fiber NbN detectors. The completed

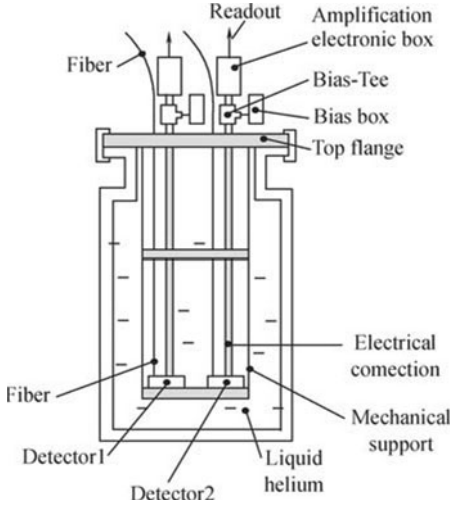

Fig. 7.15. Schematics of the two-channel single photon detector operating in a helium transport Dewar

receivers, inserted into a liquid-helium transport dewar, reached 1% system QE for 1550 nm photons.

There are also other recently developed superconducting detectors, including superconducting tunnel-junction detectors (STJDs), and tungsten-based superconducting transition-edge sensors (STESs). It is interesting to compare NbN SSPD with its superconducting counterparts. The traditional superconducting radiation detectors, such as STJDs and STESs, exhibit a very slow (kHz range) photoresponse speed, and their time jitter in the photon-counting mode is difficult to determine. The fundamental reason for the slow speed of these detectors is that they are based on superconductors with very low temperature (below 1 K), which is dictated by the desire to reach the lowest possible intrinsic noise levels and noise equivalent power (NEP), but also results in the very long quasiparticle relaxation time in these materials. Thus, STJDs and STESs are not suitable for the high-speed quantum private communication. They do, however, hold promise for other quantum information applications. The STJDs can easily be integrated into multiple-element SPDs, while STESs show not only excellent values of NEP, but also exhibit excellent energy resolution in the near-infrared (NIR) range. The latter makes them very attractive for characterization of truly single photon quantum sources, as well as candidates for photon number resolving detectors for the linear optical quantum computation.

7.4 Encoding with Discrete Variable Qubits

In a communication system, in order to transmit information from one communicator to others, the information should be encoded. In the classic communication, binary bits "0" and "1" are basic elements for encoding information. Correspondingly, qubits are always used to encode the quantum information as well as classic information. This section introduces how to encode information into the single photon signal using discrete variables qubits.

7.4.1 Polarization Modulation

The most well know realization of qubit is using orthogonal states of polarization. Identify 0° (horizontal) and 90° (vertical) polarized photons as the basis states $|0\rangle$ and $|\pi/2\rangle$, which may be implemented with a quantum signal passing through a polarizer angled 0° or 90°. By tuning the angle of polarizer into 45° or 135°, one gets the superposition states,

$$|\pi/4\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |\pi/2\rangle), \tag{7.4.1}$$

$$|3\pi/4\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |\pi/2\rangle). \tag{7.4.2}$$

The four states $|0\rangle$, $|\pi/2\rangle$, $|\pi/4\rangle$, $|3\pi/4\rangle$ are used in the BB84 QKD protocol, which is first presented by Bennett and his coworkers in 1984 [**?**], and then demonstrated experimentally in 1992 [**?**]. They realized a system where Alice and Bob exchanged faint laser pulses containing less than one photon on average over 30 cm in air.

As an example, Fig.7.16 shows schematic diagram of the QKD system in the polarization modulation. At Alice's side, laser pulses are generated by four laser diodes, and the polarization states of pulses are set by polarizers which are oriented to 0°, 45°, 90°, and 135°, respectively, according to the corresponding BB84 QKD protocol. For a given qubit, a single diode is triggered. Then the pulses are attenuated into a single photon level by a set of filters before they are combined into a non-polarizing beam splitter and sent to quantum channel. At Bob's side, polarization controllers recover the polarization state of photons to their original state at Alice. The 3-dB coupler randomly chooses the detection base and the polarization beam splitter helps to determine the key value. Finally, the photons are detected by single photon detectors. To illustrate it clearly, let us follow a photon polarized at 45°. If Bob chooses the output of beamsplitters corresponding to the vertical-horizontal basis, it will experience a random outcome. On the other hand, if it chooses the diagonal basis, its state will be rotated to 90°. The polarizing beamsplitters will then reflect it with unit probability, leading to a deterministic outcome.

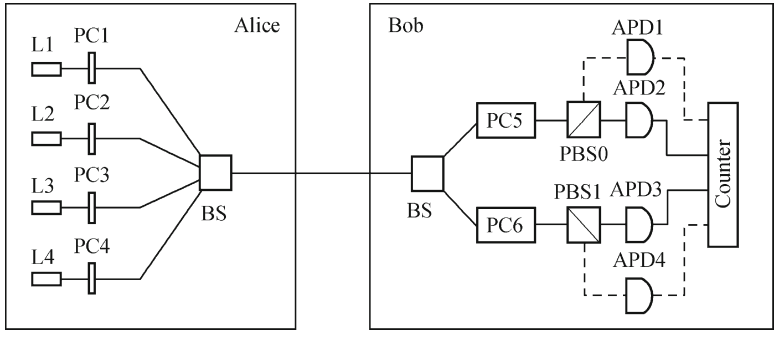

Fig. 7.16. Schematic diagram of a QKD system in polarization modulation

7.4.2 Phase Modulation

Another way of realizing discrete-variable qubits is to modulate the phase of photons which was first mentioned by Bennett. Fig.7.17 shows a schematic diagram of phase modulation. It consists of two symmetric couplers, the equivalent of beamsplitters, connected to each other, with one phase modu-

lator in each arm. Laser pulses are produced by laser diode (LD), and then sent into the coupler after they are attenuated into single photon level on average. The coupler divides one pulse into two equivalent pulses, phases of which are modulated by adding φ_A and φ_B, respectively. After they go into the second coupler, interference will occur giving the result.

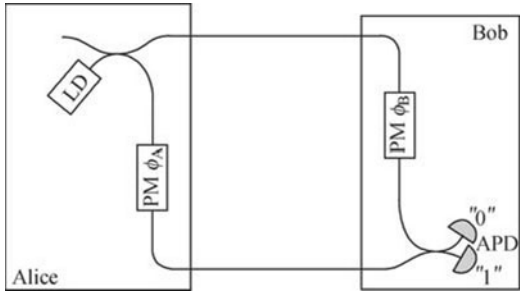

Fig. 7.17. Schematic diagram of a QKD system in phase modulation

Before considering the application of phase modulation qubits in the quantum private communication, let us briefly recall some basic principles of interference with two continuous and classical light beams, which have the same intensity and polarization. Assume that two light beams are

$$E_1 = A\mathrm{e}^{-\mathrm{i}\varphi_1}, \quad E_2 = A\mathrm{e}^{-\mathrm{i}\varphi_2}. \tag{7.4.3}$$

Then, the superposition is

$$E = A(\mathrm{e}^{-\mathrm{i}\varphi_1} + \mathrm{e}^{-\mathrm{i}\varphi_2}) = 2A\mathrm{e}^{-\frac{\mathrm{i}}{2}(\varphi_1+\varphi_2)} \cos\frac{(\varphi_1 - \varphi_2)}{2}, \tag{7.4.4}$$

and the intensity is

$$I = 4A^2 \cos^2\frac{(\varphi_1 - \varphi_2)}{2}. \tag{7.4.5}$$

Taking into account the $\pi/2$ phase shift experienced upon reflection at a beamsplitters, the effect of the phase modulators φ_A and φ_B, and the path length difference ΔL, the final phase difference in the output port labeled "0" is given by

$$\Delta\varphi = \varphi_1 - \varphi_2 = \varphi_A - \varphi_B + k\Delta L, \tag{7.4.6}$$

where k is the wave number. When $\Delta\varphi = \dfrac{\pi}{2} + n\pi$, n is an integer, the intensity registered in port "0" reaches a minimum and all the light exits in port "1". When $\Delta\varphi = n\pi$, the situation is reversed. Although we discussed the interference based on classical light, it works exactly the same when a single photon is pumped. The output probability from one port can be changed by varying the single photon's phase.

As an example, the implementation of the BB84 protocol using a phase modulation is analyzed. In this scheme, Alice's setup consists of the source,

first coupler, and first phase modulator, while Bob takes the second modulator and coupler, as well as two detectors. Alice applies one of four possible phase shifts (0, $\pi/2$, π, $3\pi/2$) to modulate a qubit. Bob can perform a basis choice by randomly applying a phase shift of 0 or $\pi/2$. When they use compatible bases, they obtain deterministic results; when the bases are incompatible, the photon chooses randomly which port it takes at Bob's coupler.

All the discussion above is based on that the coherence length of light used is larger than the path mismatch. However, this condition is hardly satisfied when the quantum channel is longer than tens of kilometers. Hence the double Mach-Zehnder implementation and pug-play system are presented, which are demonstrated in the following sections.

7.4.3 Frequency Modulation

The discrete-variable qubits can also be encoded via the frequency modulation, in theory, using a superposition of frequency states, which could be easily realized in atomic physics where different energy levels are used. However, the superposition of two basic states is difficult to achieve with photons. Until now, there is still no good experiment demonstrating this kind of modulations.

7.5 QKD with Single Photon Signal

Main components for implementing a quantum private communication system which bases on single photon signal have been presented in the previous sections. Now, we move on to describe the basic principles and physical implementations of the integrated system for the quantum private communication using these components. As described in previous chapters, a private communication is employed to guarantee the confidentiality and authentication of transmitted message. While the confidentiality and authentication are associated with the keys. Accordingly, this section demonstrates how to physically implement the well-known QKD scheme whose basic principles have been described in Chapter 4.

The QKD invented firstly by Bennett and Brassard in 1984, is a method for creating shared, assuredly secret, cryptographic key data over unsecured optical links. Its security is guaranteed by the fundamental quantum property of light rather than by physical barriers to interception or by computational complexity. The indivisibility of single photons defeats simple beam splitter attacks. More sophisticated attacks that attempt to read and replace (also called intercept and resend) the photons with identical copies are thwarted by suitable quantum laws such as Heisenberg Uncertainty Principle, quantum no-cloning theorem, or correlation of entanglement. Many works have

demonstrated the feasibility of experimental implementations of QKD using the faint laser pulse transmitted through free space or through optical fiber. Generally, there are two kinds of ways for the technical implementation on the QKD system, i.e., two-way QKD and one-way QKD. This section demonstrates these implementations for QKD classed by various types of set-ups.

7.5.1 QKD in Optical Fiber

In the case of transmission through optical fiber, information has been encoded in either the polarization states of photons or in the relative phase between two amplitude packets produced by splitting each light pulse and delaying one portion before sending it onto the transmission line. Since installed telecom fiber generally does not preserve the polarization state and has optical properties that can vary in time, both the polarization and phase encoding schemes require compensation for optical path fluctuations in order to permit reliable decoding of the information.

1) Two-way QKD

An approach invented by Martinelli in 1989 permits automatic, passive compensation for the polarization-transforming effect of the fiber [**?**]. In this invention, the emitted light from a laser transmits down a fiber, then it passes through a 45° Faraday rotator. After that, the light reflects from a mirror, passes through the Faraday rotator a second time, and returns through the fiber. With such an arrangement, the polarization state of the light returning to the input end of the fiber is always orthogonal to the polarization state of the input light, independent of the polarization transformation induced by the fiber. This effect is referred to as Faraday orthoconjugation. Fig.7.18 shows evolution of polarization state of a light pulse represented on Poincaré sphere over a round trip propagation along an optical fiber terminated by a mirror-Faraday rotator.

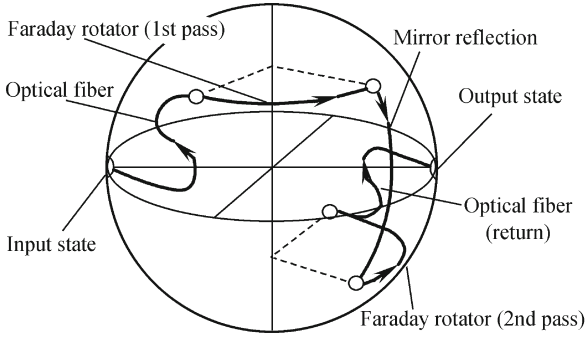

Fig. 7.18. Evolution of polarization state of a light pulse on Poincaré sphere

The input polarization state is moved forward by the total birefringence of the fiber. It must be noted that the path on the Poincaré sphere represents the equivalent birefringence of the fiber length, not the actual evolution of the state of polarization (SOP) along the circuit. The Faraday rotator rotates the azimuth of the light SOP coming from the fiber by 45° and rotates again the light reflected from the mirror by the same amount and in the same direction. After the two passes across the Faraday rotator and the reflection at the mirror, the SOP of the light launched into the fiber is orthogonal with respect to the output SOP. The birefringence of the fiber now acts on the optical beam to give an output SOP that is orthogonal with the input one. This relation holds for every input SOP and independently from the magnitude and the axes' orientation of the reciprocal birefringence, linear or circular, present along the optical circuit. This autocompensation effect will correct for time-varying changes in the optical path provided that the variations are slow compared to the time required for light to make a round trip through the fiber.

As an example, we describe the setup presented in 2002 by Gisin and his coworkers. This is an auto-compensating plug-play system [**?**], where the key is encoded in the phase between two pulses traveling from Bob to Alice and back as shown in Fig.7.19. A strong laser pulse at 1550 nm emitted at Bob is separated at a first 50/50 beamsplitter (BS). The two pulses impinge on the input ports of a polarization beamsplitter (PBS), after having travelled through a short arm and a long arm, including a phase modulator PM_B and a 50 ns delay line (DL), respectively. All fibers and optical elements at Bob are polarization maintaining. The linear polarization is turned by 90° in the short arm, therefore the two pulses exit Bob's setup by the same port of PBS. The pulses travel down to Alice, are reflected on a Faraday mirror, attenuated and come back orthogonally polarized. In turn, both pulses now take the other path at Bob and arrive at the same time at BS where they interfere. Then, they are detected either in SPD1, or after passing through the circulator in SPD2, where SPD denotes a single photon detector. Since the two pulses

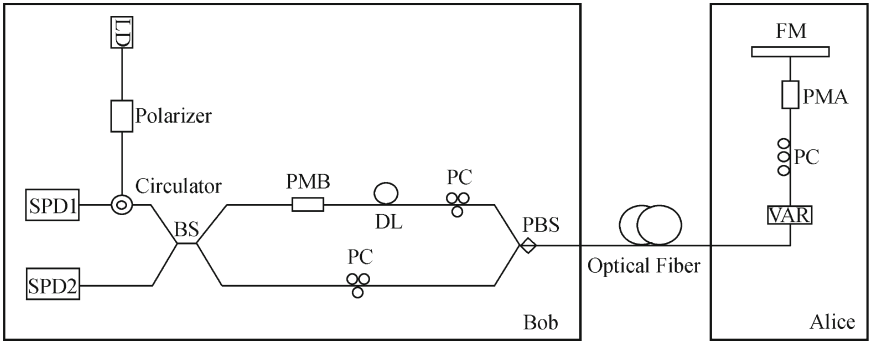

Fig. 7.19. Schematic of the plug-play prototype

take the same path, inside Bob in reversed order, this interferometer is auto-compensated. To implement the BB84 protocol, Alice applies a phase shift of 0 or π and π/2 or 3π/2 on the second pulse with PM_A. Bob chooses the measurement basis by applying a 0 or π/2 shift on the first pulse on its way back.

Because of the intrinsically bidirectional nature of this system, great attention must be paid to Rayleigh backscattering. Although it completely solves the problem of Rayleigh backscattering by adding a delay line in Alice's setup and storing these pulse trains, this scheme has the disadvantage of reducing the effective repetition frequency. Another drawback is that this configuration is more sensitive to Trojan horse strategies.

2) One-way QKD

In the absence of the quantum repeater which could regenerate a modulated photon, photon loss in the fiber limits the maximum distance over which quantum cryptography may be applied. As the fiber length increases, the signal rate falls to a value approaching that of the intrinsic error rate of the receiver's equipment. Eventually, this results in the quantum bit error rate exceeding the threshold for privacy amplification, preventing a secure key from being formed. The fact that the pulses travel along a round trip implies that losses are doubled, yielding a reduced counting rate. Hence, another design based on two Mach-Zehnder (MZ) interferometers was first proposed by Bennett in which both paths are multiplexed onto a single fiber. Alice and Bob have identical, unequal-arm MZ interferometers with a short path and a long path, with one output port of Alice's interferometer coupled to one of the input ports of Bob's. The difference of the light travel times between the long and short paths, ΔT, is much larger than the coherence time of the light source, so there can be no interference within each small interferometer. However, interference can occur within the coupled system. A photon injected into one of the input ports of Alice's interferometer therefore has a 50% probability of entering Bob's interferometer, in a wave packet that is a coherent superposition of two pieces that are separated in time by ΔT, corresponding to one amplitude for it to have taken the short path, and a delayed amplitude which took the long path. On entering Bob's interferometer each component of the wave packet is again split into a short component and a long component, so that at each output port there are three time windows in which the photon may arrive. The first of these prompt corresponds to the short-short propagation amplitude, which is followed after a delay of ΔT by the central component comprising the short-long and long-short amplitudes. Finally, after a further time ΔT, the delayed time window corresponds to the long-long amplitude.

In 2000, Hughes and other researchers at Los Alamos National Laboratory constructed an optical fiber version of this time-multiplexed interferometer in which each of Alice's and Bob's interferometers are built from two 50/50 fiber couplers [**?**]. The output fiber legs from the first coupler convey the

photons to the input legs of the second coupler via a long fiber path or a short path (ΔT is about 5 ns). One of the output legs of Alice's interferometer is connected by a 48 km long underground optical fiber network path to one of the input legs of Bob's interferometer. Fig.7.20 shows the schematic representation of this set-up. Photons emerge from Alice's interferometer are conveyed through fiber jumpers to the underground fiber network and back to Bob's interferometer. The total travel time over the underground link is about 225 μs, with 22.9 dB of attenuation owing to the fiber's 0.3 dB/km attenuation and seven connections along the path. Finally, photons emerge from the output legs of Bob's interferometer into fiber pigtailed, cooled InGaAs APD detectors.

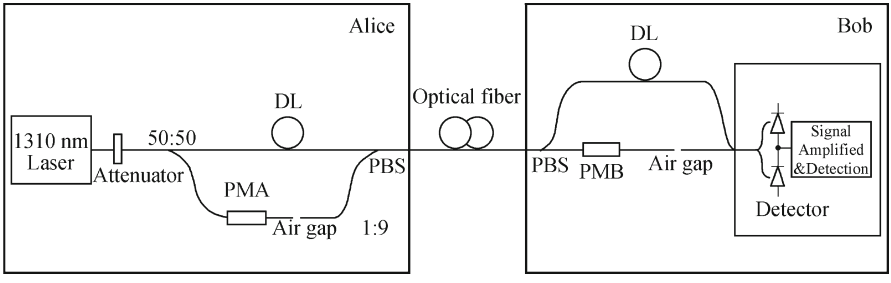

Fig. 7.20. Schematic representation of 48 km quantum cryptography experiment

The main difficulty associated with this kind of schemes is that the imbalance between Alice's and Bob's interferometers must be kept stable within a fraction of the wavelength of the photons during a key exchange to maintain correct phase relations. This implies that interferometers must lie in containers whose temperature is stabilized. In addition, for long key exchanges an active system is necessary to compensate the drift.

7.5.2 QKD in Free Space

In the case of transmission through free space, the polarization states of photon have been used to conveniently encode information, since they do not change significantly in transit. It may of course sound difficult to detect single photons against background light, but the first experiment demonstrated the possibility of free space QKD in 1991 [**?**]. Before quantum repeaters become available and allow to overcome the distance limitation of fiber based QKD, free space systems seem to offer the only possibility for QKD over distances of thousands kilometers. The systems developed for free space applications are actually very similar to the one for optical fiber. The main difference is that the emitter and receiver are connected to telescopes pointing at each other, instead of an optical fiber. The contribution of background light to errors

can be maintained at a reasonable level by using a combination of timing discrimination, spectral filtering, and spatial filtering.

Here we describe a free space quantum cryptography system presented in 1998 [?]. The system is simply based on the B92 protocol operating at a variety of average photon numbers per pulse as low as $\mu < 0.1$. Fig.7.21 shows overview of the experiment setup.

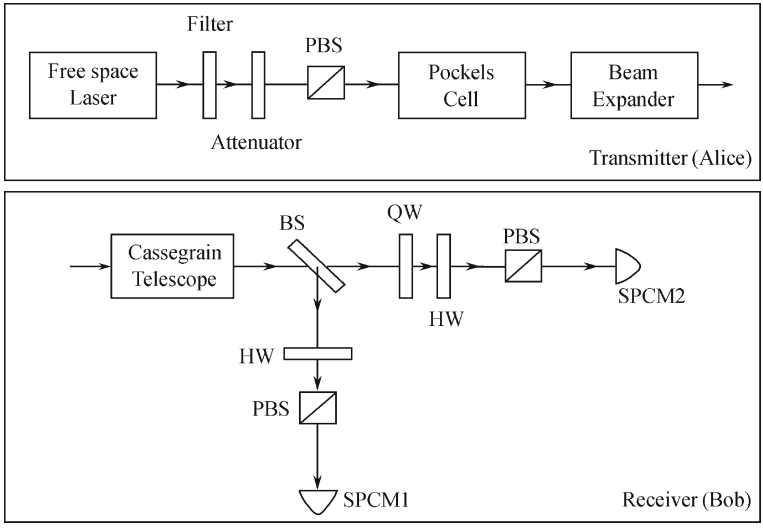

Fig. 7.21. Schematic of QKD experiment configuration in free space

In this setup, the transmitter in the experiment includes a pulsed laser source which is centered at 772 nm, a 2.5 nm bandwidth filter, a variable attenuator, a polarizing beam splitter (PBS), a pockels cell and a beam expander. When QKD system starts, the laser source produces light pulses at a rate previously agreed on. Each pulse is launched into PBS through the filter after being attenuated to an average of less than one photon with the pulse width is approximately 1ns. Then the photon is polarized by PBS in the 0 direction. The pockels cell is controlled under the voltage generated by a white noise source to choose either passing the light unchanged or changing it to $\pi/4$ direction. The receiver in the experiment consists of a 8.9 cm cassegrain telescope, a 50/50 beam splitter, a bunch of retarder, two PBS and two single photon counting module (SPCM). When the transmitting signal comes, the 50/50 BS randomly directs arriving photons into either of two distinct optical paths. The upper path contained a quarter-wave retarder and a half-wave retarder followed by a PBS to receive the 0 direction polarization photons; the lower path contained a half-wave retarder followed by a PBS to receive $\pi/4$ direction polarization photons. Since the splitting of incoming photons to the two analyzers by the beamsplitter is truly random, no other random number sequence for basis choosing is required on the receiver side.

This QKD system was operated over 950 m free space under nighttime conditions with both transmitter and receiver located in the same place to simplify the experiment, which is achieved by reflecting the emitted beam by a mirror at the halfway of the transmission line. When the repletion rate is 20 kHz with an average photon number 0.1 per pulse, the bit rate in agreement is about 50 Hz and the bit error rate is about 1.5%.

Since influence of turbulence in the the free space is mainly happened in the lowest 2 km of the atmosphere, this experiment shows that a QKD system between ground and satellite is possible on nighttime orbits. When the satellite is passing upon a ground station, they could generate thousands of raw key bits which could later be used to produce a shorter safety key stream by error correction and privacy amplification. Actually, this experiment has activated some further implementations of the QKD system in the free space. Currently, the space-based quantum private communication has become possible. This notion will be discussed in Chapter 9.

7.6 QKD with Entangled Photon Pairs

The EPR protocol was first proposed by Ekert in 1991 [**?**]. Since this protocol employs the well-known EPR entanglement pair, it is called the EPR protocol. However, it has been proven that the BB84 protocol and EPR protocol are equal cryptographically [**?**]. Thus, the EPR protocol can be regarded as a physical implementation of the BB84 protocol using two-particle EPR entangled pair. As the BB84 protocol and B92 protocol, there are also four stages in the EPR protocol. These stages are the quantum coding, quantum transmission, eavesdropping detection, and key distillation as described in Chapter 4.

To implement the BB84 protocol using entangled photon pairs, i.e., the EPR protocol, entangled photon pairs should be prepared before the cryptographic protocol is performed. Theoretically, Alice prepares n identical EPR pairs $|\Phi^+\rangle$, and then she keeps one particle and sends another to Bob via a quantum channel. According to physical properties of entanglement states, even if two particles are away from each other the correlation between two particles is still remained until one particle is measured. After these operations Alice and Bob share respectively one particle for each entangled pair. In experiment, the parametric down-conversion technique can be employed. As described in Section 7.1.5, when a laser pump beam is incident upon a nonlinear crystal, pairs of photons that satisfy the type II phase-matching conditions, which is described in Eq.(7.1.14), are emitted. The emitted fluorescence photons with ordinary and extraordinary polarization are entangled. For convenience, generated two photons are always called signal photon and idler photon. They can be employed for the the EPR protocol.

An preliminary experiment for the EPR protocol based on two-photon

interferometry was presented in 1991 [**?**]. The scheme of the apparatus is shown in Fig.7.22. In this setup, a parametric down-conversion source is pumped by a monochromatic short-wavelength laser of frequency $2\omega_0$ with $\lambda_0 = 441.6$ nm. Signal and idler photons are emitted in a broadband cone behind the crystal with pairs satisfying energy and momentum conservation, i.e., satisfying Eq.(7.1.14). Photon pairs are selected by placing apertures in the down-converted cone satisfying the phase-matching conditions in the crystal. Signal and idler photons are launched into separate fiber-optic cables and propagate to remote Mach-Zehnder interferometers. Each interferometer contains a short and longer path with the difference in transit time over the two paths denoted ΔT (1 ns in the experiment). Signal photon detectors labeled S_1 and S_0 and idler detectors labeled I_1 and I_0 view the four Mach-Zehnder outputs.

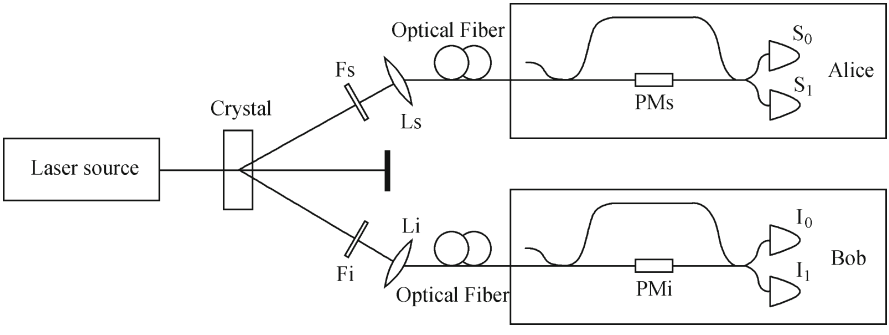

Fig. 7.22. Scheme of QKD using entangled photon pairs

Two legitimate users Alice and Bob of the two distant interferometers, set up the local parameters randomly and independently for each incoming photon. Alice chooses randomly between $\phi_s = 0$ and $\phi_s = \pi/2$, and Bob chooses randomly between $\phi_i = 0$ and $\phi_i = -\pi/2$, where subscripts s and i refer to the signal and idle photons, respectively. This corresponds to the coding stage in the common QKD scheme. According to the correlation of the EPR pair, Alice's encoded qubit is transmitted instantaneously into Bob's photon once Alice measure her photon. Thus the second stage, i.e., the quantum transmission of the encoded qubit, is finished instantaneously with the first stage.

Let ϕ_s and ϕ_i are phase shifts of the signal mode and idler mode, the sum of these parameters result in a nonlocal character of correlation between the photocounts in the two distant interferometers. If $\phi_s + \phi_i = 0$ there is a perfect correlation between photocounts in the two distant interferometers, otherwise, no correlation exists between these photocounts. This property is utilized to detect the eavesdropping.

After having finished the above stages, Alice and Bob reveal publicly the setting of their local parameters, but not which detector registered a pho-

ton. They then agree to discard all instances in which $\phi_s + \phi_i \neq 0$, as well as instances in which one or both detectors failed to register a photon due to imperfect quantum efficiency. The remaining instances ought to refer to perfectly correlated photoncounts, $\phi_s + \phi_i = 0$. To verify that this is so, Alice and Bob publicly compare the results of the photocounts on a sufficiently large random subset of the undiscarded instances. If they find that the tested subset is indeed perfectly correlated, they can infer that the remaining untested subset is also perfectly correlated. This finishes the third stage, i.e., the eavesdropping detection stage. These remaining subsets are employed to distribute a raw key. With the key distillation techniques, i.e., the key reconciliation and privacy amplification, the final key is obtained.

In the presented experiment, one beam is propagated over 170 m through a multi-mode optical fiber before the interferometer, but here the measured correlation coefficient was low, partly due to poor time resolution in the detectors. The bit error rate reaches 5×10^{-2}, and the communication loss is as low as 0.17 dB. Clearly, these parameters are not practical since it is a preliminary experiment. Subsequently, many experiments based on the entangled photon pair have been performed, and now this technique has entered gradually the practical era.

7.7 Secret Sharing with Single photon Signal

The secret sharing is an important component in the cryptology and private communication [**?**], it is useful especially in the distributed network and multiparty computation. The secret sharing scheme is referred to method for distributing a secret amongst a group of participants, each of which is allocated a share of the secret. The secret can be reconstructed only when the shares are combined together; individual shares are of no use on their own. More formally, in a secret sharing scheme there is one dealer and n players. The dealer gives a secret to the players, but only when specific conditions are fulfilled. The dealer accomplishes this by giving each player a share in such a way that any group of t (for threshold) or more players can together reconstruct the secret but no group of fewer than t players can. Such a system is called a (t, n)-threshold scheme. In Shannon information theory, a secret sharing scheme should satisfies

$$\begin{cases} H(S|s_1, s_2, \ldots, s_t) = 0, \\ H(S|s_1, s_2, \ldots, s_k) = H(S), \end{cases} \tag{7.7.1}$$

where S denote the secret, s_i denotes a share of the secret S, $i = 1, 2, \ldots, n$ and $1 \leq k \leq t - 1$.

The quantum secret sharing is a special kind of secret sharing which is implemented using quantum laws, e.g., using properties of the Greenberger-Horne-Zeilinger (GHZ) state [**?**]. By far, generally theories for the quantum

secret sharing have been presented in Refs.[32 – 34]. Usually, the quantum secret sharing is regarded as an expansion of the "traditional" QKD to more than two parties. As an example, an (3,3)-quantum secret sharing scheme designed using properties of the GHZ state [**?**] is briefly introduced in the follows. In this scenario, a sender, usually called Trent, distributes a secret key to two other parties, Alice and Bob, in a way that neither Alice nor Bob alone have any information about the key, but that together they have full information. Moreover, an eavesdropper trying to get some information about the key creates errors in the transmission data and thus reveals him presence. The motivation for secret sharing is to guarantee that Alice and Bob must cooperate in order to do some task, one might think for instance of accessing classified information.

Properties of the GHZ state has been described in Section 3.5.2. Making use of these properties of the GHZ state, the (3,3)-quantum secret sharing scheme executes the following steps.

Step1: GHZ particles distribution. Trent prepares a sequence of GHZ triplet states and then sends two particles of each GHZ state to Alice and Bob, respectively, so that each participant holds one particle for a GHZ triplet state.

Step2: Random measurement. The participants construct two measurement bases $\{|x+\rangle, |x-\rangle\}$ and $\{|y+\rangle, |y-\rangle\}$ which are along x direction or y direction, respectively. Making use of these measurement bases, Trent, Alice, and Bob randomly measure their GHZ particles using one of these measurement bases. Then, Alice and Bob tell Trent their adopted measurement bases but not the measurement results, i.e., bits values.

Step 3: Comparison operations. Trent compares their measurement bases. When their measurement bases for the same GHZ triplet state are along the same direction, e.g., the x direction, participants keep the measurement results, since in this case the results are correlated according to Table 3.2. Otherwise, they discard the measurement results.

Step 4: Eavesdropping detection. Making use of the correlation illustrated in Table 3.2, the participants check the eavesdropping. The way is similar to that used in the two-party QKD scheme.

Step 5: Now the participants, i.e., Trent, Alice, and Bob, enter the error-correction and privacy amplification procedures, which have been described in Chapter 4.

Clearly, the (3,3)-quantum secret sharing is very similar to the two-party QKD scheme which have been described in previous. Thus the security can be analyzed using the same way as that in the QKD scheme.

This scheme has been implemented experimentally based on energy-time entanglement shown in Fig.7.23 [**?**]. In this experiment, 600 ps full width at half maximum (FWHM) laser pulses with 655 nm wavelength at a repetition frequency of 80 MHz are emitted from a pulsed diode laser (DL). After passing a polarizing beamsplitter (PBS) serving as optical isolator, the pump is focused into a single mode fiber and guided into a fiber-optical Michelson

interferometer (MI) made of a 3 dB fiber coupler and chemically deposited silver end mirrors. The path-length difference corresponds to a difference of travel time of about 1.2 ns, splitting the pump pulse into two well separated pulses. To change the phase difference, the fiber of the long arm by means of a piezo-electric actuator is elongated. Three polarization controllers are employed to control the evolution of the polarization state within the different parts of the interferometer. Finally, the horizontally polarized light leaving the interferometer by the second output fiber is focused into a $4 \times 3 \times 12$ mm $KNBO_3$ crystal, cut and oriented in order to ensure colinear, degenerate phasematching, hence creating photon pairs at 1310 nm wavelength. Behind the crystal, the red pump light is absorbed by a filter, and the photon pairs are focused into a fiber coupler, separating them in half of the cases. The average pump power before the crystal is about 1 mW, and the energy per pulse is about 6 pJ. To characterize the performance of the source, the coupler's output fibers are connected to single-photon counters operated in Geiger-mode, i.e., APD (denoted using symbol "D" in the figure). The down-converted photons are finally guided into fiber optical Michelson interferometers, located at Alice's and Bob's, respectively. The interferometers, consisting of a 3 dB fiber coupler and Faraday mirrors.

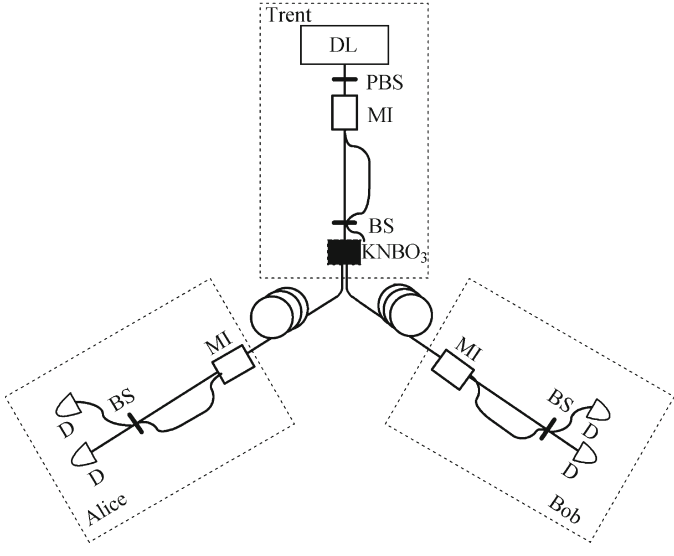

Fig. 7.23. Experimental principle setup for quantum secret sharing using energy-time entangled states

With the setup presented in Fig.7.23, a pseudo-GHZ state is prepared. The state may be denoted as

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|l_t\rangle, |s_a\rangle |s_b\rangle + \mathrm{e}^{\mathrm{i}(\alpha+\beta+\gamma)} |s_t\rangle, |l_a\rangle |l_b\rangle \right), \tag{7.7.2}$$

where α, β, γ are phases in the different interferometers, the subscripts t, a, b are referred to the participants Trent, Alice and Bob, respectively, and l, s imply the long and short arms, respectively. After the pseudo-GHZ state has been prepared, remainder operations, which should follow steps in the involved (3,3)-quantum secret sharing scheme, are similar to the QKD scheme.

References

[1] Tittel W, Weihs G (2001) Photonic entanglement for fundamental tests and quantum communication. Quantum Information and Computation, 1(2): 3 – 56

[2] Brassard G, Lütkenhaus N, Mor T, et al (2000) Limitations on Practical Quantum Cryptography. Physical Review Letters, 85(6): 1330 – 1333

[3] Malko A, Baier M H, Karlsson K F, et al (2006) Optimization of the efficiency of single photon sources based on quantum dots under optical excitation. Applied Physics Letters, 88: 1 – 4

[4] Zwiller V, Blom H, Jonsson P, et al (2001) Single quantum dots emit single photons at a time: Antibunching experiments. Applied Physics Letters, 78(17): 2476 – 2479

[5] Chen S, Chen Y A, Strassel T, et al (2006) Deterministic and storable single photon source based on a quantum memory. Physical Review Letters, 97(17): 3004 – 3007

[6] Kurtsiefer C, Mayer S, Zarda P, et al (2000) Stable Solid-State Source of Single Photons. Physical Review Letters, 85(2): 290 – 293

[7] Kim J, Benson O, Kan H, et al (1999) A single photon turnstile device. Nature, 397: 500 – 503

[8] McCusker K T, Peters N A, VanDevender A P, et al (2008) A deterministic single photon source. Conference on Lasers and Electro-Optics (CLEO), California, paper JTuA117

[9] Zeng G H, Keitel C H (2002) Inhibiting decoherence via ancilla processes. Physical Review A, 66: 1 – 6

[10] Walls D F, Milburn G J (1995) Quantum Optics. NewYork: Springer-Verlag

[11] Shor P W (1995) Scheme for reducing decoherence in quantum computer memory. Physical Review A, 52: 2493 – 2508

[12] Genoni M G, Paris M G A (2005) Optimal quantum repeaters for qubits and qudits. Physical Review A, 71(5):1 – 5

[13] Zukowski M, Zeilinger A, Horne M A, et al (1993) "Event-ready-detectors" Bell experiment via entanglement swapping. Physical Review Letters, 71 (26): 4287 – 4290

[14] Bennett C H, Bernstein H J, Popescu S, et al (1996) Concentrating partial entanglement by local operations. Physical Review A, 53(4): 2046 – 2052

[15] Flyckt S O, Marmonier C (2002) Photomultiplier Tubes: Principles and Applications. Photonis, Brive

[16] Cova S, Ghioni M, Lacaita A, et al (1996) Avalanche photodiodes and quenching circuits for single photon detection. Applied Optics, 35(12): 1956 – 1976

[17] Thew R T, Zbinden C H, Gisin N (2008) Tunable up-conversion photon detector. Applied Physics Letters, 93(7): 1104 – 1107

[18] Shields A J, O'Sullivan M P, Farrer I, et al (2001) Single photon detection with a quantum dot transistor. Special Edition of Japanese Journal of Applied Physics, 40(3)B: 2058 – 2064

[19] Sobolewski R, Verevkin A, Gol'tsman G N, et al (2003) Ultrafast superconducting single photon optical detectors and their applications. IEEE Transactions on Applied Supercondutivity, 13(2): 1151 – 1157

[20] Slysz W, Wjgrzecki M, Bar J, et al (2006) Fiber-coupled single photon detectors based on NbN superconducting nanostructures for practical quantum cryptography and photon-correlation studies. Applied Physics Letters, 88(26): 1113 – 1116

[21] Bennett C H, Brassard G (1984) An update on quantum cryptography. Advances in Cryptology: Proceedings of Cryptology, 84: 475 – 480

[22] Bennett C H, Bessette F, Brassard G, et al (1992) Experimental quantum cryptography. Journal of Cryptology, 5: 3 – 28

[23] Martinelli M A (1989) A universal compensator for polarization changes induced by birefringence on a retracing beam. Optics Communications, 72: 341 – 344

[24] Stucki D, Gisin N, Guinnard O, et al (2002) Quantum key distribution over 67 km with a plug & play system. New Journal of Physics, 4(41): 41.1 – 41.8

[25] Hughes R J, Morgan G L, Peterson C G (2000) Quantum key distribution over a 48 km optical fibre network. Journal of Modern Optics, 47(2): 533 – 547

[26] Buttler W T, Hughes, R J, Kwiat, P G, et al (1998) Quantum key distribution over 1 km, Physical Review Letters, 81: 3283 – 3286

[27] Ekert A K (1991) Quantum cryptography bases on Bell's theorem. Physical Review Letters, 67: 661 – 664

[28] Bennett C H, Brassard G, Mermin N D (1992) Quantum cryptography without Bell's theorem. Physical Review Letters, 68: 557 – 559

[29] Ekert A K, Rarity J G, Tapster P R, et al (1991) Practical quantum cryptography based on two-photon interferometer. Physical Review Letters, 69: 1293 – 1295

[30] Shamir A (1979) How to share a secret. Communications of the ACM, 22 (11): 612 – 613

[31] Hillery M, Buzek V, Berthiaume A (1999) Quantum secret sharing. Physical Review A, 59: 1829 – 1834

[32] Cleve R, Gottesman D, Lo H K (1999) How to share a quantum secret. Physical Review Letters, 83: 648 – 651

[33] Gottesman D (2000) Theory of quantum secret sharing. Physical Review A, 61: 1 – 15

[34] Tyc T, Sanders B C (2002) How to share a continuous-variable quantum secret by optical interferometry. Physical Review A, 65: 1 – 9

[35] Tittel W, Zbinden H, Gisin N (2001) Experimental demonstration of quantum secret sharing. Physical Review A, 63: 1 – 9

8 Private Communication Using Continuous Variable Signal

This chapter introduces how to implement the quantum private communication using continuous variable signals. Key components for the private communication system including continuous variable signal sources, quantum modulation, quantum signal transmission and detection are described. Then, typical ways for protecting confidentiality and authentication with the coherent state and squeezed state are presented.

The previous chapter has presented a way of implementing the quantum private communication using single photon signals. In principle, the single photon signal is an excellent quantum signal for the quantum private communication system, especially for the quantum key distribution (QKD). However, difficulties of generating a single photon signal limit its technical implementations and practical applications. This motivates investigations on using few-photon quantum signals for private communications. Two typical quantum signals which are suitable for this scenario are the coherent state and squeezed state. Such a kind of quantum signals is weak comparing to the classic optical signal used in the optical telecommunication, but it is more powerful than the single photon signal. Therefore, they may be called weak quantum signals which are different from the dim (or faint) laser pulse quantum signal described in Chapter 7. As presented in Chapter 2, the coherent state and squeezed state are often described using quadrature variables, i.e., the quadrature "position" X and "momentum" P. These quadrature variables are associated with physical variables, which satisfy the uncertainty principle, for the coherent state and squeezed state. Since spectra of the variables X and P are continuous, they are continuous variables according to the definition in Section 1.6. Accordingly, the coherent state and squeezed state signals are often called continuous variable signals. This chapter introduces how to implement the quantum private communication with continuous variable signals.

The arrangement of this chapter is similar to Chapter 7. Firstly, the continuous variable signals including the coherent state and squeezed state are described following Chapter 2, and key components for the private communication system are discussed. Then, typical ways for protecting confidentiality and authentication with the continuous variable signals are presented.

8.1 Continuous Variable Signal

Before addressing characteristics of the quantum private communication system, key components including continuous variable signal sources, quantum modulation, quantum signal transmission, and quantum signal detection should be described. Of these components, the first issue is associated with properties of continuous variable signals. To carry encoded information, two kinds of quantum signals are often employed in this scenario. One is the coherent state signal and the other is the squeezed state signal.

8.1.1 Coherent State Signal

In quantum mechanics a coherent state is a specific quantum state of the quantum harmonic oscillator whose dynamics most closely resemble the oscillating behavior of a classical harmonic oscillator system. A coherent state has an indefinite number of photons which allows it to have a more precisely defined phase than a number state where the phase is completely random. The product of the uncertainty in amplitude and phase for a coherent state is the minimum constrained by the uncertainty principle [**?**, **?**].

Theoretically, the coherent state can be generated with a so-called unitary displacement operator defined by

$$\hat{D}(\alpha) = \mathrm{e}^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}, \tag{8.1.1}$$

where α is an arbitrary complex number and α^* is its conjugate. Using the operator theory presented in Chapter 2, one has

$$\mathrm{e}^{A+B} = \mathrm{e}^{A}\mathrm{e}^{B}\mathrm{e}^{\frac{-[A,B]}{2}},$$

with the condition,

$$[A,[A,B]] = [B,[A,B]] = 0.$$

Consequently, one may rewrite the operator as

$$\hat{D}(\alpha) = \mathrm{e}^{\frac{-|\alpha|^2}{2}}\mathrm{e}^{\alpha\hat{a}^\dagger}e^{-\alpha^*\hat{a}},$$

where Eq.(2.3.43) is exploited in derivation. With simple calculation one finds that the operator $\hat{D}(\alpha)$ has following properties,

$$\begin{cases} \hat{D}^\dagger(\alpha) = \hat{D}^{-1}(\alpha) = D(-\alpha), \\ \hat{D}^\dagger(\alpha)\hat{a}\hat{D}(\alpha) = \hat{a} + \alpha, \\ \hat{D}^\dagger(\alpha)\hat{a}^\dagger\hat{D}(\alpha) = \hat{a}^\dagger + \alpha^*, \\ \hat{D}(\alpha+\beta) = \hat{D}(\alpha)\hat{D}(\beta)\mathrm{e}^{-\mathrm{iIm}\{\alpha\beta^*\}}, \end{cases} \tag{8.1.2}$$

where i denotes the imaginary unit, β is an arbitrary complex number, $\mathrm{Im}\{C\}$ denotes the imaginary part of the complex number C, $\hat{a}$ and $\hat{a}^\dagger$ are annihilation operator and creation operator, respectively. Then, the coherent state $|\alpha\rangle$ is generated by operating with $\hat{D}(\alpha)$ on the vacuum state $|0\rangle$,

$$|\alpha\rangle = \hat{D}(\alpha)|0\rangle. \tag{8.1.3}$$

Simple calculation gives

$$\hat{D}^\dagger(\alpha)\hat{a}|\alpha\rangle = D^\dagger(\alpha)\hat{a}\hat{D}(\alpha)|0\rangle = (\hat{a}+\alpha)|0\rangle = \alpha|0\rangle. \tag{8.1.4}$$

Multiplying both sides by $\hat{D}(\alpha)$ yields an eigenvalue equation,

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle. \tag{8.1.5}$$

Thus, the coherent state is also defined as an eigenstate of the annihilation operator $\hat{a}$. Since $\hat{a}$ is non-Hermitian operator its eigenvalue α is complex. As mentioned in above, the coherent state contains an indefinite number of photons. This may be apparent by expanding the coherent state expressed in Eq.(8.1.3) in the number-state basis, i.e., the Fock states basis [**?**],

$$\begin{aligned}
|\alpha\rangle &= \exp[\alpha\hat{a}^\dagger - \alpha^*\hat{a}]|0\rangle \\
&= \mathrm{e}^{\frac{-|\alpha|^2}{2}}\mathrm{e}^{\alpha\hat{a}^\dagger}\mathrm{e}^{-\alpha^*\hat{a}}|0\rangle \\
&= \mathrm{e}^{\frac{-|\alpha|^2}{2}}\mathrm{e}^{\alpha\hat{a}^\dagger}|0\rangle \\
&= \mathrm{e}^{\frac{-|\alpha|^2}{2}}\sum_{n=0}^{\infty}\frac{\alpha^n(\hat{a}^\dagger)^n}{n!}|0\rangle.
\end{aligned}$$

Using the relationship for the Fock state,

$$(\hat{a}^\dagger)^n|0\rangle = \sqrt{n!}|n\rangle,$$

the coherent state is expressed as

$$|\alpha\rangle = \mathrm{e}^{\frac{-|\alpha|^2}{2}}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle. \tag{8.1.6}$$

The probability distribution of photons in a coherent state satisfies the Poisson distribution,

$$P(n) = |\langle n|\alpha\rangle|^2 = \frac{|\alpha|^{2n}\mathrm{e}^{-|\alpha|^2}}{n!},$$

where $|\alpha|^2$ is the mean number of photons since $\langle n\rangle = \langle\alpha|\hat{a}^\dagger\hat{a}|\alpha\rangle = |\alpha|^2$.

The scalar product of two coherent states is $\langle\beta|\alpha\rangle = \langle 0|\hat{D}^{\dagger}(\beta)\hat{D}(\alpha)|0\rangle$. Using Eq.(8.1.6) one obtains

$$\langle\beta|\alpha\rangle = \exp\left[-\frac{1}{2}(|\alpha|^2 + |\beta|^2) + \alpha\beta^*\right]. \tag{8.1.7}$$

The absolute magnitude of the scalar product is

$$|\langle\beta|\alpha\rangle|^2 = \exp\left[-(|\alpha - \beta|)^2\right]. \tag{8.1.8}$$

This implies that two coherent states are approximately orthogonal within the limitation $|\alpha - \beta| \gg 1$. Accordingly, all coherent states form a continuum state space.

Combining Eq.(8.1.6) gives

$$\frac{1}{\pi}\int_{\infty} |\alpha\rangle\langle\alpha| \mathrm{d}^2\alpha = \frac{1}{\pi}\int_{\infty} \mathrm{e}^{-|\alpha|^2} \sum_{m=0}^{\infty} \frac{\alpha^m}{\sqrt{m!}} \sum_{n=0}^{\infty} \frac{(\alpha^*)^n}{\sqrt{n!}} |m\rangle\langle n| \mathrm{d}^2\alpha.$$

With the following well-known relationship,

$$\frac{1}{\pi}\int_{\infty} \alpha^m \alpha^* n \mathrm{e}^{-[\beta|\alpha|^2]} \mathrm{d}^2\alpha = \frac{m!}{\beta^{m+1}}\delta_{mn} \qquad \alpha \in \mathbb{C},$$

one obtains

$$\frac{1}{\pi}\int_{\infty} |\alpha\rangle\langle\alpha| \mathrm{d}^2\alpha = \sum_{n=0}^{\infty} |n\rangle\langle n| = I. \tag{8.1.9}$$

This expression forms the completeness relationship of the coherent state space.

As described in Chapter 2, a field is always described using quadrature variables X and P. Introducing two operators X and P defined in Eq.(2.3.42) which correspond to variables of the quadrature position and quadrature momentum, respectively, the coherent state $|\alpha\rangle$ satisfies $\langle X\rangle = \mathrm{Re}\{\alpha\}$ and $\langle\hat{P}\rangle = \mathrm{Im}\{\alpha\}$, where $\mathrm{Re}\{\alpha\}$ and $\mathrm{Im}\{\alpha\}$ denote the real part and imaginary part of α. According to the definition of variances, one has

$$\begin{aligned}\langle\Delta X^2\rangle &= \langle X^2\rangle - (\langle X\rangle)^2 \\ &= \langle\alpha|\left(\frac{\hat{a}^{\dagger} + \hat{a}}{2}\right)^2|\alpha\rangle - \left(\langle\alpha|\frac{\hat{a}^{\dagger} + \hat{a}}{2}|\alpha\rangle\right)^2.\end{aligned}$$

Making use of the commutation relation in Eq.(2.3.43) gives

$$\langle\Delta X^2\rangle = \frac{1}{4}. \tag{8.1.10}$$

Similarly, one may obtain $\langle\Delta P^2\rangle = 1/4$. Consequently, the corresponding uncertainty principle is

$$\langle\Delta X^2\rangle\langle\Delta P^2\rangle = 1/16, \tag{8.1.11}$$

and $\langle \Delta X^2 \rangle = \langle \Delta P^2 \rangle$. This means the coherent state $|\alpha\rangle$ has the mean complex amplitude α and it is a minimum uncertainty state for two quadrature variables X and P.

A coherent state is often represented intuitionally using an "error circle" in a complex amplitude plane plotted in Fig.8.1 with labels X and P. In this figure, $P(x)$ and $P(p)$ denote distributions for x and p, respectively. The center of the error circle lies at $\langle X + \mathrm{i}P \rangle$ and the radius $\langle \Delta X^2 \rangle = \langle \Delta P^2 \rangle = 1/4$ accounts for uncertainties in X and P. Subsequently, a coherent state is often denoted using $|x + \mathrm{i}p\rangle$ with Eqs.(8.1.10) and (8.1.11).

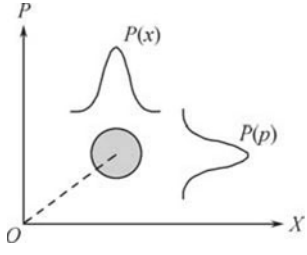

Fig. 8.1. Uncertainty for a coherent state in phase space

In the classic optics, the optical light is thought of as an electromagnetic wave radiating from a source. Often, coherent laser light is thought of as light that is emitted by many such sources that are in phase [**?**]. Actually, the picture of one photon being in-phase with another is not valid in quantum theory. Laser radiation is produced in a resonant cavity where the resonant frequency of the cavity is the same as the frequency associated with the atomic transitions providing energy flow into the field. As energy in the resonant mode builds up, the probability for stimulated emission, in that mode only, increases. That is a positive feedback loop in which the amplitude in the resonant mode increases exponentially until some nonlinear effects limit it. As a counter-example, a light bulb radiates light in a continuum of modes, and there is nothing that selects any one mode over the others. The emission process is highly random in space and time (e.g., thermal light). In a laser, however, light is emitted in a resonant mode, and that mode is highly coherent. Thus, laser light is idealized as a coherent state. The coherent states have a physical significance in that the field generated by a highly stabilized laser operation well above a threshold is a coherent state. Thus a coherent state is very easy to implement physically in experiment. As an example, the well-known distributed feed back (DFB) laser outputs directly coherent state.

In practice, the so-called Gaussian-shaped coherent state is needed in many scenarios. A coherent state is said to be Gaussian state if its Wigner function is a Gaussian function. The Wigner function is a generating function for all spatial autocorrelation functions of a given quantum-mechanical wavefunction $\psi(x)$. Mathematically, the Wigner function is a special type of

quasi-probability distribution. The Wigner distribution $P(x,p)$ is defined as

$$P(x,p)=\frac{1}{\pi\hbar}\int_{-\infty}^{+\infty}\psi^*(x+y)\psi(x-y)e^{2\mathrm{i}py/\hbar}dy. \tag{8.1.12}$$

Making use of the Winger function, one may obtain a Gaussian distribution in the basis of eigenstate of X and P as follows,

$$\begin{cases}\langle X|\alpha\rangle=\dfrac{1}{\sqrt[4]{2\pi\langle\Delta X^2\rangle}}\exp\left\{-\dfrac{(x-\langle X\rangle)^2+\mathrm{i}\langle X\rangle\langle P\rangle}{4\langle\Delta X^2\rangle}+\dfrac{\mathrm{i}\langle P\rangle x}{2\langle\Delta X^2\rangle}\right\},\\ \langle P|\alpha\rangle=\dfrac{1}{\sqrt[4]{2\pi\langle\Delta P^2\rangle}}\exp\left\{-\dfrac{(p-\langle P\rangle)^2+\mathrm{i}\langle X\rangle\langle P\rangle}{4\langle\Delta P^2\rangle}+\dfrac{\mathrm{i}\langle X\rangle p}{2\langle\Delta P^2\rangle}\right\}.\end{cases}$$

8.1.2 Squeezed State Signal

A squeezed coherent state, briefly called squeezed state, is any state of the Hilbert space such that the uncertainty principle is satisfied. Generally, a coherent state is a particular state with equal noise in both quadratures X and P. While a squeezed state may have less noise in one quadrature than the other with two quadratures still satisfying the requirement of a minimum uncertainty principle. There is obviously a whole family of minimum uncertainty states defined by

$$\langle\Delta X^2\rangle\langle\Delta P^2\rangle=1/16. \tag{8.1.13}$$

If one plots ΔX against ΔP the minimum uncertainty state lies on a hyperbola shown in Fig.8.2(a), only points lying to the right of this hyperbola correspond to physical states. The coherent state is a special case of a more general class of states which may have reduced uncertainty in one quadrature at the expense of increased uncertainty in the other ($\Delta X<1/4<\Delta P$). These states correspond to the shaded region in Fig.8.2(b).

Theoretically, squeezed states can be generated using a unitary squeeze operator [**?**],

$$S(\zeta)=\exp\left(\frac{1}{2}(\zeta^*\hat{a}^2-\zeta\hat{a}^{\dagger 2})\right), \tag{8.1.14}$$

where $\zeta=r\mathrm{e}^{2\mathrm{i}\phi}$ and the squeeze operator obeys the following relations,

$$S^\dagger(\zeta)=S^{-1}(\zeta)=S(-\zeta), \tag{8.1.15}$$

and has the following transformation properties,

$$\begin{cases}S^\dagger(\zeta)\hat{a}S(\zeta)=\hat{a}\cosh r-\hat{a}^\dagger\mathrm{e}^{-2\mathrm{i}\phi}\sinh r,\\ S^\dagger(\zeta)\hat{a}^\dagger S(\zeta)=\hat{a}^\dagger\cosh r-\hat{a}\mathrm{e}^{2\mathrm{i}\phi}\sinh r,\\ S^\dagger(\zeta)(X+\mathrm{i}P)S(\zeta)=X\mathrm{e}^{-r}+\mathrm{i}P\mathrm{e}^{r}.\end{cases} \tag{8.1.16}$$

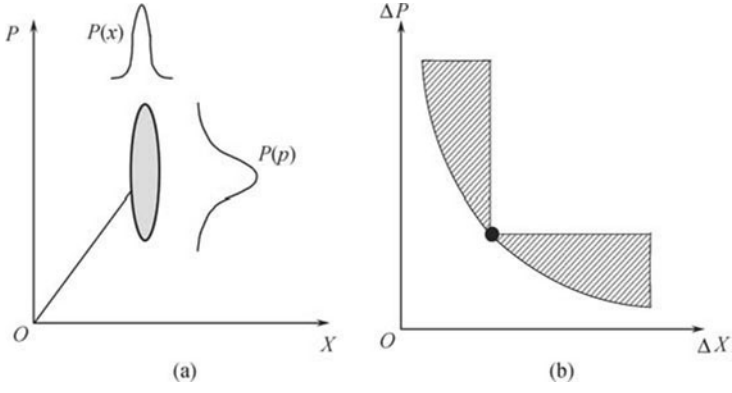

Fig. 8.2. Schematic of squeezed state

a) Squeezed state plotted in phase space. b) Plot of ΔX versus ΔP for minimum uncertainty state.

The squeeze operator attenuates one component of the complex amplitude and amplifies the other component. The degree of attenuation and amplification is determined by $r = |\zeta|$ called squeezing factor. Physically, the squeezed state $|\alpha, \zeta\rangle$ may be obtained by first squeezing the vacuum and then displacing it, i.e.,

$$|\alpha, \zeta\rangle = D(\alpha)S(\zeta)|0\rangle. \tag{8.1.17}$$

Using quadrature variables X and P, a squeezed state has the following expectation values and variances,

$$\begin{cases} \langle X + \mathrm{i}P\rangle = \alpha, \\ \Delta X = \dfrac{1}{2}\mathrm{e}^{-r}, \\ \Delta P = \dfrac{1}{2}\mathrm{e}^{r}. \end{cases} \tag{8.1.18}$$

Eq.(8.1.18) implies that the squeezed state has unequal uncertainties for X and P as seen in the error ellipse shown in Fig.8.2. The principal axes of the ellipse lie along X and P axes, and the principal radii are ΔX and ΔP. Similarly, a squeezed state may be denoted $|x + \mathrm{i}p\rangle$ with constraint of Eq.(8.1.11) and $\Delta X \neq 1/4$.

Generally, there are several typical approaches for generating the squeezed state. One is the so-called quadrature amplitude squeezed state and the other is the photon number squeezed state. They can be prepared in free space and in fiber.

In 1985, squeezed states of the electromagnetic field have been generated using nondegenerated four-wave mixing with Na atoms in an optical cavity [**?**]. The optical noise in the cavity, comprised of primarily vacuum fluctuations and a small component of spontaneous emission from pumped Na atoms,

is amplified in one quadrature of the optical field and deamplified in the other quadrature. A schematic diagram of the experimental configuration is shown in Fig.8.3. Here, a continuous wave single-mode ring dye laser pumps a beam of Na atoms at the pump-cavity (PM1 and PM2) resonance frequency. The pumped Na atoms generate four-wave-mixing gain in the squeezing cavity (SM1 and SM2). A local oscillator beam is split off by BS1. The squeezed cavity noise is detected with a balanced homodyne detector which will be introduced in Section 8.3.3.

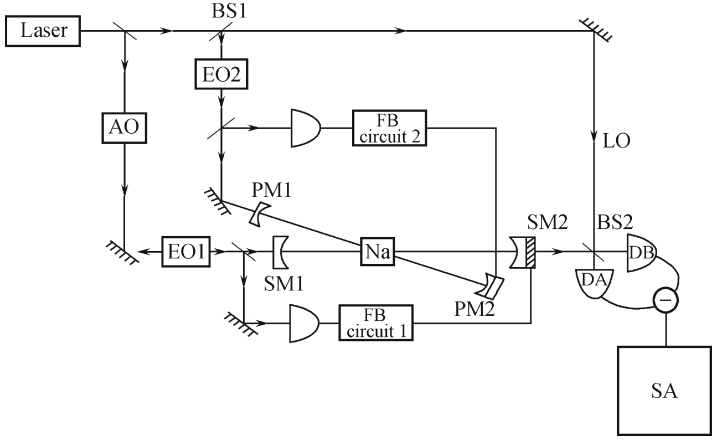

Fig. 8.3. A schematic diagram of the experimental configuration for squeezed state by four-wave mixing

In 2002, the first demonstration on bright EPR beams with quantum correlations between the quadrature phase and amplitude of the spatially separated signal and idler beams have been generated experimentally [**?**]. This experiment used a continuous wave nondegenerate optical parametric amplifier injected by seed waves with degenerate frequency but orthogonal polarization. The correlation degree is directly inferred from the measured quadrature-phase squeezing of the output vacuum squeezed-state light field formed from superposition of the original signal and idler modes. The theoretical calculation and experimental measurements provide a reliable method to confirm the quadrature phase-squeezing level below the vacuum level 5.4 dB.

In 1991, Rosenbluh's group experimentally demonstrated the squeezing of optical solitons in fiber, resulting in a photon-current noise power 1.7 dB below the shot-noise limit over a broadband of frequencies [**?**]. The squeezing is accomplished using the Kerr nonlinearity of a polarization-preserving single-mode optical fiber at liquid-nitrogen temperature. The experimental schematic is shown in Fig.8.4. In this experiment, 200 fs, 1550 nm light pulses are injected from the right APM laser and are controlled in energy by a polarizer P and wave plate WP. They are launched into both the ends of

the PM fiber through BS2. A portion of the emerging pulse is picked off by beam splitter BS1 to form the local oscillator. The mean-square fluctuations in each quadrature of the squeezed vacuum pulse are measured via balanced homodyne detection.

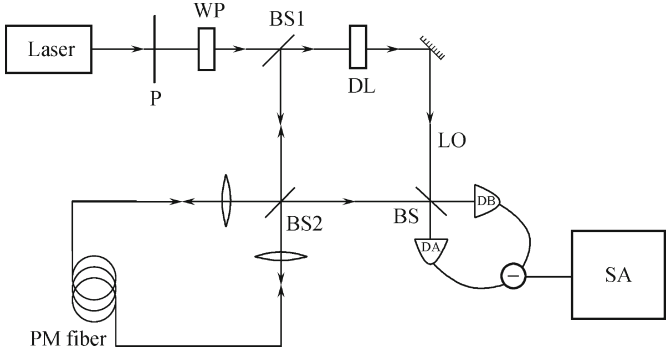

Fig. 8.4. A schematic diagram of experimental configuration for squeezed state using Kerr nonlinearity

Fig.8.5 demonstrates an approach for generation of the photon number squeezed state in fiber. Direct photon-number squeezing was demonstrated in 1998 for the first time, in a nonlinear fiber-optic interferometer. Launching 126 fs solitons into a highly asymmetric sagnac loop, the maximum photocurrent noise reduction was 3.9 dB below shot noise. The loop is a model system for squeezing generated by the interference of two pulses after nonlinear propagation through a fiber.

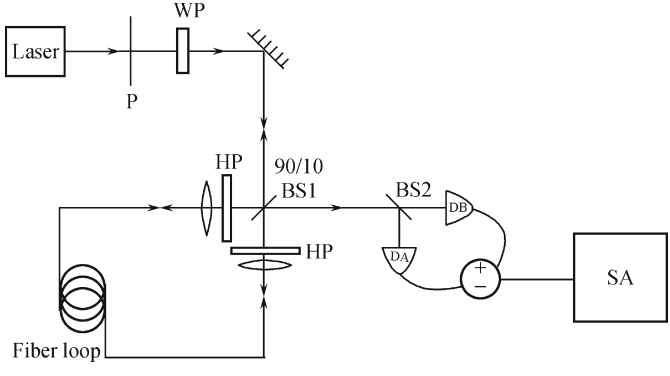

Fig. 8.5. A schematic diagram of the experimental configuration for squeezed state by asymmetric Sagnac loop

8.2 Continuous Variable Signal Transmission

The previous sections have described how to generate the coherent state and squeezed state quantum signal, and characteristics of these states are presented. This section describes transmission characteristics of continuous variable signals. Similar to the transmission of single photon signals, two situations for the transmission of continuous variable quantum signals are also involved. One is the direct transmission which is suitable for short distance quantum communications such as the local area network (LAN) or metropolitan area network (WAN). Another is the long-distance transmission where the quantum repeater is necessary.

The transmission mechanism of quantum signals in channels has been described in Section 7.2. It shows that the decoherence changes the state of the transmitted quantum signal and deteriorates on the transmission length. Subsequently, errors are generated on the carried information in the quantum signal.

The refraction phenomenon can be regarded as a kind of interactions between the transmitted light signal and its environments. Therefore, influences of the refraction on quantum signals are described in the follows. As described in Chapter 2, when the Hamiltonian operator is determined for a quantum system, any physical variable of this system can be calculated. Thus we first try to obtain the Hamiltonian operator of quantum signals in a media. This can be done using the well-known Lagrange approach with the Fermat principle. Consider that a light transmits in a media with refractive index $N(x, z)$. In this case, the Lagrange quantity is expressed by

$$L = N(x, z)\sqrt{1 + x^2}. \tag{8.2.1}$$

The Fermat principle is mathematically expressed by

$$\delta \int_{z_0}^{z_1} L(x, \dot{x}; z) = 0, \tag{8.2.2}$$

where $\dot{x}$ denote the differentiation. Define a variable p as follows,

$$p = \frac{\partial L}{\partial \dot{x}} = N\dot{x}(1 + \dot{x})^{\frac{1}{2}} = N(x, z)\sin\theta, \tag{8.2.3}$$

where $N(x, z)\sin\theta$ denotes the X-direction cosine of light at a position (x, z). Using the Legendre transformation, one obtains the classic Hamiltonian of the involved light system,

$$H_c = -(N^2 - p^2)^{\frac{1}{2}}. \tag{8.2.4}$$

When the light is transmitted in a fiber, the parallel axis approximates is suitable for the considered situation, thus one has

$$p^2 \ll N^2. \tag{8.2.5}$$

In addition, $N(x,y,z) = N_0(1-\tilde{N}(x,z))$ with $\tilde{N}(x,z) \ll 1$. Then, the classic Hamiltonian is rewritten as

$$H_c = -N_0 + N_0\tilde{N}(x,z) + \frac{p^2}{2N_0}. \tag{8.2.6}$$

For the kind of fibers with square-law refractive index, $\tilde{N}(x,y,z) = \eta x^2$. In this case, the classic Hamiltonian is expressed by

$$H_c = -N_0 + N_0\eta x^2 + \frac{p^2}{2N_0}. \tag{8.2.7}$$

By analogy with the classic Hamiltonian expressed in Eq.(8.2.7), the Hamiltonian operator (briefly, Hamiltonian) for the quantum signal light is expressed by

$$H = \frac{\hat{p}^2}{2N_0} + N_0\eta\hat{x}^2 - N_0, \tag{8.2.8}$$

where $\hat{x}$ and $\hat{p}$ denote the position operator and momentum operator, respectively. Define two quadratures X and P,

$$\begin{cases} X = 2\left(\dfrac{2\eta N_0^2}{\Delta^2}\right)^{\frac{1}{4}}\hat{x} = \sqrt{\dfrac{2\pi\omega_c N_0}{\lambda}}\hat{x}, \\ P = \left(2\eta N_0^2\Delta^2\right)^{\frac{1}{4}}\hat{p} = \sqrt{\omega_c N_0\Delta}\hat{p}. \end{cases} \tag{8.2.9}$$

One may easily check that $[X,P] = \mathrm{i}$. Subsequently, the Hamiltonian is rewritten as

$$H = k\omega_c(X^2 + P^2) - N_0, \tag{8.2.10}$$

where $k = 2\pi/\lambda$, $\omega_c = (2\eta)^{\frac{1}{2}}$.

After having obtained the Hamiltonian, transmission properties of the quantum signal can be acquired using the Schrödinger equation or the master equation. At the parallel axis approximates the stationary Schrödinger equation in 2-dimension reads as

$$\frac{\mathrm{i}\lambda}{2\pi}\frac{\partial\tilde{\psi}}{\partial z} = \left[-N_0 + N_0\tilde{N}(x,z) - \frac{\lambda^2}{4\pi^2 N_0}\frac{\partial^2}{\partial x^2}\right]\tilde{\psi}. \tag{8.2.11}$$

Let $\tilde{\psi}(x,z) = \psi(x,z)\exp(2\pi\mathrm{i}\frac{N_0}{\lambda}z)$, Eq.(8.2.11) is simplified as

$$\frac{\mathrm{i}\lambda}{2\pi}\frac{\partial\psi}{\partial z} = \left[N_0\tilde{N}(x,z) - \frac{\lambda^2}{8\pi^2 N_0}\frac{\partial^2}{\partial x^2}\right]\psi. \tag{8.2.12}$$

In the kind of fibers with square-law refractive index, the stationary Schrödinger equation reads as

$$\frac{\mathrm{i}\lambda}{2\pi}\frac{\partial\psi}{\partial z} = \left[N_0\eta x^2 - \frac{\lambda^2}{8\pi^2 N_0}\frac{\partial^2}{\partial x^2}\right]\psi. \tag{8.2.13}$$

Let $\xi = (8\pi^2\eta N_0^2/\lambda^2)^{\frac{1}{4}}x, \zeta = (2\pi/\lambda)z$, Eq.(8.2.13) is rewritten as

$$\mathrm{i}\frac{\partial\psi(\xi,\zeta)}{\partial\zeta} = \frac{\lambda\omega_c}{4\pi}\left(\xi^2 - \frac{\partial^2}{\partial\xi^2}\right)\psi(\xi,\zeta). \tag{8.2.14}$$

Let $\psi(\xi,\zeta) = \phi_n(\xi)\exp(-\mathrm{i}\Delta\omega\zeta)$, an eigenequation is obtained, and its solutions for the eigenstate and eigenvalue are given, respectively, by

$$\phi_n(\xi) = P_n H_n(\xi)\exp\left(-\frac{\xi^2}{2}\right), \tag{8.2.15}$$

and

$$\omega_n = \omega_c\left(n + \frac{1}{2}\right), \quad n = 0, 1, 2, \ldots, \tag{8.2.16}$$

where $P_n = \left(\sqrt{\pi}2^n n!\right)^{-\frac{1}{2}}$ and $H_n(\xi)$ is the Hermite polynomial. For convenience, the Dirac symbol which is often employed in the quantum information processing is adopted, then the eigenstate is denoted by

$$|n\rangle = \phi_n(\xi), \tag{8.2.17}$$

and subsequently the state $\psi(\xi,\zeta)$ is denoted by

$$|\xi,\zeta\rangle = \psi(\xi,\zeta) = |n\rangle\exp(-\mathrm{i}\Delta\omega_n\zeta). \tag{8.2.18}$$

Let $U(\zeta_0,\zeta)$ be the transmission operator, using the Hamiltonian one gets,

$$U(\zeta_0,\zeta) = \exp\left[-\mathrm{i}H(\zeta-\zeta_0)\right]. \tag{8.2.19}$$

Then the state of the quantum signal at the position (ξ,ζ) is given by

$$|\xi,\zeta\rangle = U(\zeta_0,\zeta)|\xi_0,\zeta_0\rangle = \exp\{-\mathrm{i}\Delta\omega_n(\zeta-\zeta_0)\}|n,\zeta_0\rangle. \tag{8.2.20}$$

Clearly, this is an oscillating solution since the decoherence is not included. Easily, the state of single photon signal is easily given by

$$|\xi,\zeta\rangle_s = \left(2\sqrt{\pi}\right)^{-\frac{1}{2}}H_1(\xi)\exp\left(-\frac{\xi^2}{2}\right)\exp\{-\mathrm{i}\Delta\omega_c(\zeta-\zeta_0)\}|\zeta_0\rangle, \tag{8.2.21}$$

and the coherent state is acquired using Eq.(8.1.6).

Transmission characteristics of continuous variable signals in optical fiber and in free space is similar to situations of the single photon signal. Subsequently, they have same transmission characteristics in a same physical channel, e.g., the fiber. This has been presented in detail in Chapter 7, it does not here repeat again. However, it is worth stressing the transmission of the polarization-based encoding system. Currently, the standard optical single-mode fiber is the most popular choice for fiber communication. It can connect two arbitrary points, and can easily be extended to form networks.

Moreover, it is deployed in most developed urban areas. The main disadvantage of optical fiber is its birefringence which will be described in Section 9.2. The strong polarization dispersion made it hard to implement the polarization-based encoding system. Also it has strong spectral dispersion, which affects the high speed (10 GHz) QKD systems heavily [**?**] as the pulses are broadened and overlap with each other. For this reason, the loss in fibers (0.21 dB/km at 1550 nm) results in limitations on the longest distance that a fiber-based QKD system can reach. The free space, however, is ideal for the polarization-based encoding system. There is negligible dispersion on the polarization and the frequency. However, the alignment of optical beams can be challenging for long distances, particularly due to the atmospheric turbulence. Notice that open-air QKD requires a direct line of sight between Alice and Bob (unless some forms of mirrors are used). Buildings and mountains are serious obstacles for the open-air QKD systems. The greatest motivation for the open-air QKD scheme is the hope for ground-to-satellite and satellite-to-satellite quantum communication. As there is negligible optical absorption in the outer space, one may be able to achieve an inter-continental quantum communication with the QKD in free-space. This will be described in the next chapter.

8.3 Continuous Variable Signal Detection

As described in Chapter 7, both the optical signal and the carried quantum state (qubit) must be detected in the quantum private communication so that receivers can decode the transmitted information. Due to differences of the single photon and continuous variable signals, these signals must be detected in different ways. This section introduces several detection ways for continuous variable signals, including direct intensity measurement, coherent detection and standard homodyne detection. Finally, influences of imperfectness on the homodyne detection are analyzed.

8.3.1 Direct Intensity Measurement

As it is well-known that the intensity measurement of optical signal is always employed in the classical telecommunication system. Actually, this measurement approach is suitable for both the classic communication and quantum communication. Fig.8.6 shows a schematic diagram of the direct intensity measurement of a light beam. The main devices in this diagram are the photodetector, preamplify, oscilloscope, and spectrum analyzer. In this way, the direct current (DC) component of the photon detector output is monitored by an oscilloscope or a power meter. The output voltage is proportional to the optical power of the light, which can also be measured by a power meter. The

alternating current (AC) component is measured by a spectrum analyzer.

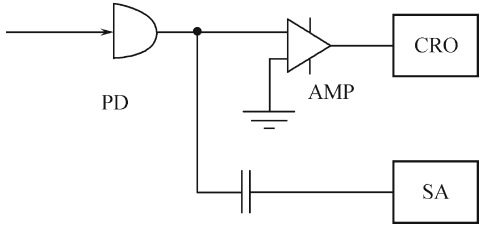

Fig. 8.6. Schematic of direct intensity measurement

PD: photodetector; AMP: preamplify; CRO: oscilloscope; SA: spectrum analyzer

The photodetector is a main device in this detection system. Most photodetectors work with the photoelectric effect which was discovered by Herz in 1887 [**?**] and has become important for quantum mechanics since Einstein's works in 1905 [**?**]. In principle, the radiation ionizes a piece of photosensitive materials and produces freely moving electrons. The photosensitive part of the detector is a p-i-n structure, a sandwich of the p (positively) doped, i (intrinsic), and n (negatively) doped semiconductor materials. Commonly, Si or InGaAs are used where Si detects light out to a one-micrometer wavelength and InGaAs operates in the range 1.0 to 1.1 micrometers. A bias voltage (about 10 volts) is applied to drain majority carders (electrons in n and holes in p) out of the intrinsic zone. In this depletion region an unstable situation is created for minority carders. As soon as electron-hole pairs are presented in the intrinsic zone, the bias voltage produces a current that is proportional to the number of carders. As the avalanche photodiode, the light excites electron-hole pairs in the depletion zone. This process may be highly efficient because the applied voltage is low in contrast to the avalanche photodiode so that no avalanche is yielded. The current response of the detector is linear in the intensity of the detected light. On the other hand, thermal fluctuations cause Nyquist noise in the photocurrent. In addition, thermal effects create naturally electron-hole pairs in the depletion zone, producing the so-called dark current. Because of this electronic noise, linear-response photodiodes do not reach the single photon resolution. They are suitable for relatively high intensities, e.g., greater than about 100 photons per microsecond.

In the quantum scenario, the direct intensity measurement is the simplest optical measurement. Suppose that the quantum efficiency of the photodiode is η. The detected photocurrent is proportional to the number of photons incident on the surface of the photodiode,

$$i_c = \eta e \langle \hat{n} \rangle = \eta e \langle \hat{a}^\dagger \hat{a} \rangle, \tag{8.3.1}$$

where e is the charge of an electron, and $\hat{n}$ is the photon number operator which is defined by $\hat{n} = \hat{a}^\dagger \hat{a}$ [**?**]. A spectrum analyzer is employed to measure

the variance of the photocurrent which is proportional to the variance of the photon number $\langle \Delta \hat{n}^2 \rangle$,

$$V_{i_c} = \eta^2 e^2 \langle \Delta \hat{n}^2 \rangle. \tag{8.3.2}$$

Since noises result in fluctuations on the intensity and frequency of the employed optical signal, one should consider imperfectness and noise in realistic photodetection. A convenient model to understand these experimental effects is provided by imagining a fictitious beam splitter placed in front of an ideal detector which will be discussed in the later.

8.3.2 Coherent Detection

To measure the continuous variable signal, a local oscillator signal is helpful as that in the radio and microwave communication. This leads the so-called coherent detection. Exactly, the coherent detection consists of combining optical signal coherently with a continuous-wave optical field, i.e., the local oscillator signal, before it enters into the photodetector. The detection system is shown in Fig.8.7.

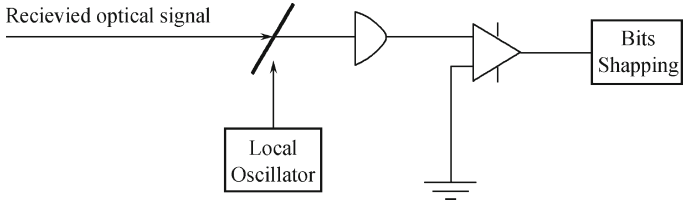

Fig. 8.7. Schematic illustration of a coherent detection scheme

In the coherent measurement, the key point is how to mix the signal field and the local oscillator field so that the performance is improved. A description for classical optics has been presented in Ref.[**?**]. The difference between the classical way and quantum way relies on how to treat with the noise of the optics field. According to the quantum optics theory, the annihilation operator of output field $\hat{a}_o$ is a linear combination of the annihilation operator of the signal field and local oscillator field, i.e.,

$$\hat{a}_o = T\hat{a}_s + R\hat{a}_{LO}, \tag{8.3.3}$$

where T and R are the transmission index and reflection index of beamsplitter, respectively, they satisfy $|T|^2 + |R|^2 = 1$ and $\arg(R) - \arg(T) = \pi/2$. Suppose a 50:50 beamsplitter, the operator for detection photon number

$\hat{n}_o = \hat{a}_o^\dagger \hat{a}_o$ is

$$\begin{aligned}\hat{n}_o &= \frac{1}{2}(\hat{a}_s^\dagger - \mathrm{i}\hat{a}_{LO}^\dagger)(\hat{a}_s + \mathrm{i}\hat{a}_{LO}) \\ &= \frac{1}{2}[\hat{n}_s + \hat{n}_{LO} + \hat{a}_s^\dagger \hat{a}_{LO} \mathrm{e}^{\mathrm{i}\frac{\pi}{2}} + (\hat{a}_{LO}\mathrm{e}^{\mathrm{i}\frac{\pi}{2}})^\dagger \hat{a}_s)].\end{aligned} \tag{8.3.4}$$

Without loss of the generality, the local oscillator is usually treated as a classical field, then the annihilation operator of the local oscillator field is replaced by a complex vector, i.e., $\hat{a}_{LO} = |\alpha| e^{\mathrm{i}\phi_{LO}}$. Subsequently, Eq.(**??**) is rewritten as,

$$\hat{n}_o = \frac{1}{2}(\hat{n}_s + \hat{n}_{LO} + X_s \cos\theta + P_s \sin\theta), \tag{8.3.5}$$

where $\theta = \phi_{LO} + \pi/2$. Eq.(8.3.5) implies that the quadrature amplitude is hidden in the local oscillator field when the local oscillator field is much stronger than the signal field. Making use of Eqs.(8.3.1) and (8.3.5) one may obtain the detected photocurrent, i.e., $i \propto \langle \hat{n}_o \rangle$.

8.3.3 Homodyne Detection

Since the continuous variable quantum communication is actually a special kind of coherent optical communication which has been investigated in classic optical communications, a so-called homodyne detection, which is employed to obtain a phase sensitive measurement, has to be adopted. In this case, a local oscillator signal is necessary for retrieving the carried information by the transmitted signal. In principle, the local oscillator should have same wavelength as the signal field. The local oscillator is as a reference light field and contains a photon number n_{LO} which is typically about 10^6 photons/pulse. While the quantum signal contains photons at quantum level, i.e., $n_{sig} \leq 1$ photon/pulse.

In the homodyne detection, the signal interferes with a coherent laser beam, i.e., the local oscillator, at a well-balanced 50:50 beam splitter (BS). The local oscillator provides the phase reference 0 for the quadrature measurement. Principle of the homodyne detection is shown in Fig.8.8.

As usual, let the signal and local oscillator have a fixed phase relation, which is adopted in most experiments since both fields are ultimately generated by a common laser. The local oscillator should be intense with respect to the signal for providing a precise phase reference. Usually, the local oscillator should be powerful enough so that it may be treated as a classical field. In this case, its quantum fluctuations are neglected. After the optical mixing of the signal with the local oscillator, each emerging beam is directed to a photon detector (usually a linear-response photodiode). The photocurrents $i_1(t)$ and $i_2(t)$ are measured, and then electronically processed, and finally subtracted from each other. The difference current $i\_(t)$ is the quantity of interest

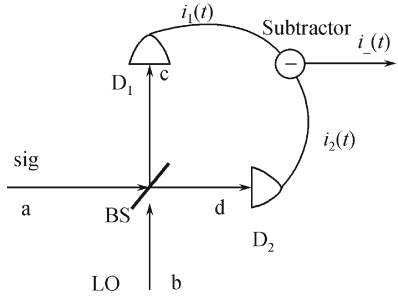

Fig. 8.8. Balanced homodyne detector

BS 50:50 beam splitter; D1,D2: PIN photoelectric detector; sig: signal optical field; LO: local oscillator optical field.

because it contains the interference term of the local oscillator and the signal. For simplicity, assume that the measured photocurrents $i_1(t)$ and $i_2(t)$ are proportional to the photon numbers $\hat{n}_c$ and $\hat{n}_d$ of beams striking each detector. According to the relationship between four ports of 50:50 beamsplitter one obtains

$$\begin{cases} \hat{a}_c = \dfrac{1}{\sqrt{2}}(\hat{a}_s + \mathrm{i}\hat{a}_{LO}), \\ \hat{a}_d = \dfrac{1}{\sqrt{2}}(\mathrm{i}\hat{a}_s + \hat{a}_{LO}). \end{cases} \tag{8.3.6}$$

Then the differential current is

$$\begin{aligned} i\_(t) &= i_1(t) - i_2(t) \propto \langle \hat{n}_c \rangle - \langle \hat{n}_d \rangle, \\ &= \langle \hat{a}_s^\dagger \hat{a}_{LO} \mathrm{e}^{\mathrm{i}\frac{\pi}{2}} + (\hat{a}_{LO}\mathrm{e}^{\mathrm{i}\frac{\pi}{2}})^\dagger \hat{a}_s \rangle. \end{aligned} \tag{8.3.7}$$

Since the local oscillator field is treated as a classical field, one has $\hat{a}_{LO} = |\alpha|\mathrm{e}^{\mathrm{i}\phi_{LO}}$. This gives

$$i\_(t) \propto |\alpha_{LO}| \langle X \cos\theta + P \sin\theta \rangle. \tag{8.3.8}$$

Eq.(8.3.8) demonstrates that a balance homodyne detection may measure two quadrature components X or P, e.g., phase shifter or phase modulator, with adjusting the differential phase between the signal field and local oscillator.

In above a rather crude way is presented for the homodyne detection, sophisticated theories for the homodyne detection may be referred to Refs. [12 – 14]. The above mode shows that the homodyne detector is an amplifier. The local oscillator amplifies the signal by the mutual optical mixing. In addition, the homodyne detector is regarded as an interferometer that even can be measurably imbalanced by a single photon in the signal mode since the reference field is very intense. The amplification has an important technical advantage. The so-amplified signal is well above the electronic noise floor of the photodiodes. The signal amplitude is enhanced so that even the noisy

linear-response photodiodes can detect the quantum features of the signal. In this way, the balanced homodyne detector takes advantage of the high efficiency of photodiodes and at the same time can determine signals with single photon resolution!

Above all, the light field is supposed to be a single mode regardless of signal or local oscillator. However, the experimental operation in the homodyne detection requires matching states of polarization of the local oscillator to the signal received. Although the polarization state of the local oscillator may be fixed easily, the polarization state of the signal field randomly changes because of undetermined factors such as birefringence, polarization dependent loss, polarization mode dispersion, etc. An alternative way is to realize a polarization diversity and balanced homodyne detection scheme [**?**] as in Fig.8.9. The diversity architecture can mitigate significantly the limitations imposed by phase and polarization fluctuations.

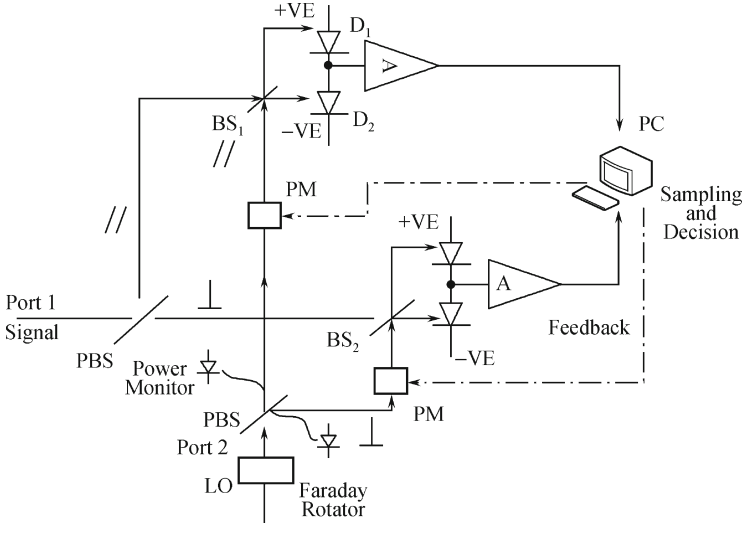

Fig. 8.9. Polarization diversity homodyne detection

PBS: polarization Beam splitter; BS1, BS2: Beam Splitter; D1, D2: PIN photoelectric detector; A: amplifier; Port 1: signal optical field; Port2: local oscillator.

In Fig.8.9, two orthogonal polarization components of the received signal are detected separately and then combined after an appropriate phase compensation. In detail, the signal is equally split into a pair of orthogonal polarization states through polarization beam splitter (PBS). Simultaneously, the local oscillator is equally spilt with PBS, too. Two pairs of local oscillator and signal independently are mixed in BS1 and BS2, respectively. Quadrature position or momentum of the coherent state is detected using the homodyne detection. After A/D sampling, these quadrature values of

two branches are sent to a computer for evaluating polarization fluctuation and combine according to the optimum algorithm. The advantage of using polarization diversity is to allow simultaneously track phase drift of a pair of orthogonal polarization. In this scheme, effects induced by polarization fluctuation and phase drift are mitigated, and system can be continuously operated in a convenient way.

8.3.4 Imperfect Homodyne Detection

A photon detection is usually not completely efficient in practice due to the imperfectness of employed devices, for example, the employed photodetections are always imperfect. In order to understand influence of the imperfectness on the homodyne detection, a simple model for losses in direct photon detection is exemplified in this subsection.

Imagine a fictitious beam splitters to be placed in front of two ideal detectors in the measurement setup which is shown in Fig.8.10. Annihilation

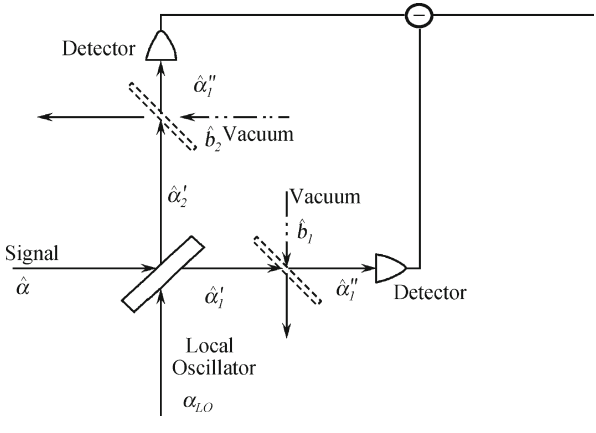

Fig. 8.10. Schematic diagram of imperfect homodyne detection

operators of detected fields are obtained according to unbalance beam splitter model,

$$\begin{cases} \hat{a}_1'' = \eta^{\frac{1}{2}}\hat{a}_1' + (1-\eta)^{\frac{1}{2}}\hat{b}_1, \\ \hat{a}_2'' = \eta^{\frac{1}{2}}\hat{a}_2' + (1-\eta)^{\frac{1}{2}}\hat{b}_2, \end{cases} \tag{8.3.9}$$

where $\hat{b}_1$ and $\hat{b}_2$ denote annihilation operators of vacuums entering second ports of fictitious beam splitters. From Fig.8.10 one may easily obtain

$$i\_(t) \propto \langle (\hat{a}_2'')^\dagger \hat{a}_2'' - (\hat{a}_1'')^\dagger \hat{a}_1'' \rangle. \tag{8.3.10}$$

Combining Eqs.(8.3.9) and (8.3.10) gives the photon-number difference,

$$i\_(t) \propto \langle \eta((\hat{a}_2')^\dagger \hat{a}_2' - (\hat{a}_1')^\dagger \hat{a}_1') + (1-\eta)(\hat{b}_2^\dagger \hat{b}_2 - \hat{b}_1^\dagger \hat{b}_1)\rangle + \langle [\eta(1-\eta)]^{\frac{1}{2}}((\hat{a}_2')^\dagger \hat{b}_2 + \hat{b}_2^\dagger \hat{a}_2' - (\hat{a}_1')^\dagger \hat{b}_1 - \hat{b}_1^\dagger \hat{a}_1')\rangle. \quad (8.3.11)$$

Annihilation operators $\hat{a}_1'$ and $\hat{a}_2'$ given by Eq.(8.3.6) describe fields emerging from the 50:50 beam splitter where the sign is optically mixed with the local oscillator, which is a rather intense coherent field compared with the signal. Consider a classic local oscillator field and only leading terms in Eq.(8.3.11) with respect to α_{LO}, one obtains

$$i\_(t) \propto \langle \eta^{\frac{1}{2}} \alpha_{LO}^* (\eta^{\frac{1}{2}} \hat{a} + (1-\eta)^{\frac{1}{2}} \hat{b}) + (1-\eta)^{\frac{1}{2}} \alpha_{LO}((1-\eta)^{\frac{1}{2}} \hat{a}^\dagger + \eta^{\frac{1}{2}} \hat{b}^\dagger)\rangle, \quad (8.3.12)$$

where $\hat{b} = 2^{-\frac{1}{2}}(\hat{b}_2 - \hat{b}_1)$. This operator corresponds to an optical mixing of the fictitious vacuum-noise modes $\hat{b}_1$ and $\hat{b}_2$, and it obeys the bosonic commutation relation,

$$[\hat{b}, \hat{b}^\dagger] = 1.$$

Because the interference of a vacuum with another vacuum still yields a vacuum, the fluctuation mode $\hat{b}$ is regarded as a bosonic mode, being in the vacuum state as well. Eq.(8.3.12) has a simple interpretation: similar to direct photon counting, a fictitious vacuum field has to be added to the intensity-reduced signal in homodyne detection. This interpretation means that one may replace the arrangement of two fictitious beam splitters in front of the photodetectors, which is shown in Fig.8.10, by just one effective beam splitter in front of an ideal homodyne detector shown in Fig.8.11.

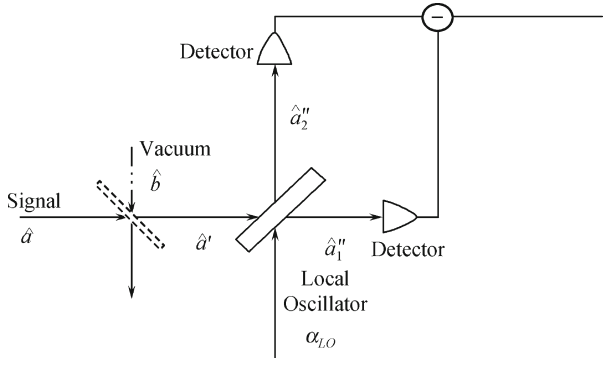

Fig. 8.11. Effective balanced homodyne detection scheme with one fictitious beam splitter

The effective beam splitter demonstrates another kind of losses as well, in particular the mode mismatch. Consequently, quantum effects of both detection losses and mode mismatch comprised in an effective η may be predicted according to the tot with the above ways.

8.4 Encoding with Continuous Variable Qubits

In the quantum communication, information is encoded using qubits alike that in the classic communication where the information is encoded using classic bits, e.g., binary bits "0" and "1" [**?**]. Then the encoded qubits are modulated physically into the quantum signal so that the encoded information is transmitted from senders to receivers. To implement the quantum private communication with continuous variable signals, the security requires the prepared qubits obeying the well-known Heisenberg Uncertainty Principle so that the encoded qubits are undistinguished. As described in above, the coherent state and squeezed state are often characterized using quadrature components X and P, and these quadrature components obey the uncertainty principle since their commutation relationship. Accordingly, they are often employed for the quantum private communication, especially the QKD scheme. Thus, a message including meaningful random string or meaningless random string may be encoded using quadrature components X, P of the coherent state or squeezed state. In addition, the polarization component of the coherent state and squeezed state have similar attributes to quadrature position and momentum, subsequently, they are also employed for encoding operations. This section presents several physical ways for encoding qubits.

8.4.1 Continuous Variable Qubits

For clearly, the continuous variable qubit is described briefly before discussing the encoding process. Let Ω be a random variable. As defined in Chapter 1, if Ω consists of finite discrete symbols, e.g., $\omega_1, \omega_2, \ldots, \omega_n$ with probabilities $p_1, p_2, \ldots, p_n$, the random variable Ω is called a discrete variable. Similarly, if a variable Ξ consists of continuous values $\xi \in [a, b]$ with a probability distribution $p(\xi)$, the random variable Ξ is called a continuous variable in the interval $[a, b]$.

In the quantum communication, information is encoded using qubit or qubit string, and then is modulated physically into a quantum signal, e.g., single photon signal or weak quantum signals, for a communication processing. There are two qubit forms, i.e., discrete variable qubit and continuous variable qubit. Physically, a discrete variable qubit is referred to a discrete quantum state in a finite Hilbert space $\mathscr{H}_n$. For example, in the 2-dimension Herbert space an arbitrary qubit is denoted $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$. Clearly, the possible value is discrete, i.e., 0 and 1, with probabilities $|\alpha|^2$ and $|\beta|^2$, respectively. Similar to the discrete variable qubit, a continuous variable qubit may be expressed also using the Dirac symbol. However, the continuous variable qubit is associated with a quantum state in an infinite Hilbert space. Let Ξ be a continuous variable, the corresponding continuous variable qubit is denoted $|\Xi\rangle$. One should note here that the variable Ξ consists of

continuous values in an interval, e.g., $[a, b]$, with a probability distribution, e.g., a Gaussian distribution.

For demonstration, the "position" x and "momentum" p are exemplified for continuous variable qubits. The corresponding operators of the variables x and p are $\hat{x}$ and $\hat{p}$, respectively. Their eigenstates satisfy following eigenequations,

$$\begin{cases} \hat{x}|x\rangle = x|x\rangle, \\ \hat{p}|p\rangle = p|p\rangle. \end{cases} \tag{8.4.1}$$

Here states $|x\rangle$ and $|p\rangle$ are continuous variables qubits. These states are orthogonal which are expressed in following forms,

$$\begin{cases} \langle x|x'\rangle = \delta(x - x'), \\ \langle p|p'\rangle = \delta(p - p'), \end{cases} \tag{8.4.2}$$

and the completion are denoted,

$$\begin{cases} \int_{\infty} \mathrm{d}x|x\rangle\langle x| = I, \\ \int_{\infty} \mathrm{d}p|p\rangle\langle p| = I. \end{cases} \tag{8.4.3}$$

Note that there are a few differences on the orthogonality of the continuous variable qubit to the discrete variable qubit. In addition, these quadrature eigenstates are mutually related to each other by a Fourier transformation as following,

$$\begin{cases} |x\rangle = \dfrac{1}{\sqrt{\pi}} \int_{\infty} \mathrm{d}p \mathrm{e}^{-2\mathrm{i}xp}|p\rangle, \\ |p\rangle = \dfrac{1}{\sqrt{\pi}} \int_{\infty} \mathrm{d}x \mathrm{e}^{2\mathrm{i}xp}|x\rangle. \end{cases} \tag{8.4.4}$$

Despite being unphysical and not square integrable, quadrature eigenstates can be very useful in the quantum private communication. These quadrature variables obey the canonical commutation relationship. This relationship helps to encode legitimate messages using quadrature eigenstates since they are undistinguished when information is encoded to $|x\rangle$ and $|p\rangle$, so that an eavesdropper who doesn't know correctly measurement basis cannot decode the legitimate message. In the idealized quantum communication protocols with continuous variables, the qubits $|x\rangle$ and $|p\rangle$ with x and p being real number are always regarded as a pair of non-commute basis vectors which span an infinitely dimension Hilbert space. Subsequently, an arbitrary quantum state in such a Hilbert space is expressed by

$$|\Psi\rangle = \int_{\infty} \mathrm{d}x\psi(x)|x\rangle,$$

or

$$|\Psi\rangle = \int_{\infty} \mathrm{d}p\psi(p)|p\rangle.$$

For instance, a vacuum state infinitely squeezed in position may be expressed by a zero position eigenstate $|x = 0\rangle = \frac{1}{\sqrt{\pi}} \int \mathrm{d}p|p\rangle$. Physical and finitely squeezed states are characterized by the quadrature probability distribution $|\Psi(x)|^2$ of which the width corresponds to the quadrature uncertainties.

8.4.2 Amplitude-Phase Encoding Rule

Suppose a continuous variable quantum signal $|q\rangle$ with its displacements denoted X and P, then this signal may be denoted $|x + \mathrm{i}p\rangle$. Consider that quadrature variables X and P in the quantum signal are pair of conjugate variables, i.e., they satisfy the uncertainty principle, as mentioned in above, they may be employed to encode a continuous variable s (i.e., message) which may be meaningful or meaningless. Not loss the generality, let the involved continuous variable s follows a Guassian distribution $p(s)$. To encode this variable s into the associated quantum signal, the following rule is often adopted,

$$|q\rangle \longrightarrow |x + \mathrm{i}p\rangle. \tag{8.4.5}$$

Exactly, displacements X and P in the quantum signal state, e.g., coherent state or squeeze state, are encoded according to the variable s into X and P, respectively. After finished this process, the message denoted by the variable s is modulated into the quantum signal so that it is transmitted securely from one communicator to others. Subsequently, the quantum signal becomes $|x+\mathrm{i}p\rangle$. Since s follows a Guassian distribution, encoded quadrature variables X and P follow

$$X \sim N(0, \sigma_A^2),$$

and

$$P_1 \sim N(0, \sigma_A^2),$$

where $\lambda \sim N(\mu, \sigma^2)$ denotes that the random variable λ follows a Gaussian probability distribution with an average value μ and variance σ^2.

For clearly, the encoding rule is shown in Fig.8.12 using coherent state as an example. In this figure, the coherent states, such as the one illustrated in the upper left quadrant which has a quantum error illustrated by shadow, are modulated along both axes. Their centers follow a bivariate Gaussian distribution, illustrated by the concentric circles.

The main idea of this rule is that the Heisenberg uncertainty principle prevents one from measuring both quadratures X or P with full accuracy. As an example, consider its application in the QKD scheme. In this scenario, suppose that Alice encodes randomly his variable and yields outputs X_A and

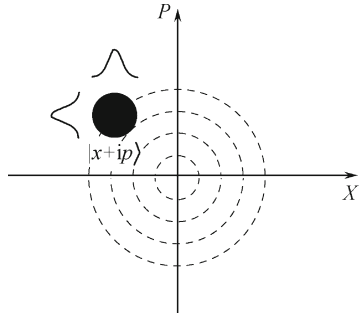

Fig. 8.12. Description of amplitude-phase encoding rule

P_A. After received the quantum signal, the receiver, Bob, randomly chooses one basis to measure either X or P. Denote Bob's measurement results X_B and P_B. When Bob measures X, the value X_B is correlated to X_A, and Alice and Bob discard P_A and keep X_B after reconciliation. Conversely, when Bob measures P, Alice and Bob discard X_A and keep P_B. In principle, the amplitude-phase encoding rule is suitable for the QKD scheme as well as other kinds of schemes for the quantum private communication. However, when it is exploited to encrypt a message, for example, a pre-shared key is necessary.

Quadrature variables X and P are abstract notations for theoretical investigations. Technically, the amplitude and phase of a coherent state or a squeezed state are often employed since they obeys the uncertainty principle and are easy to implement experimentally. An amplitude and phase encoding scheme which change the coherent state $|\alpha\rangle$ to $|\alpha_A e^{i\theta_A}\rangle$ is shown in the following figure.

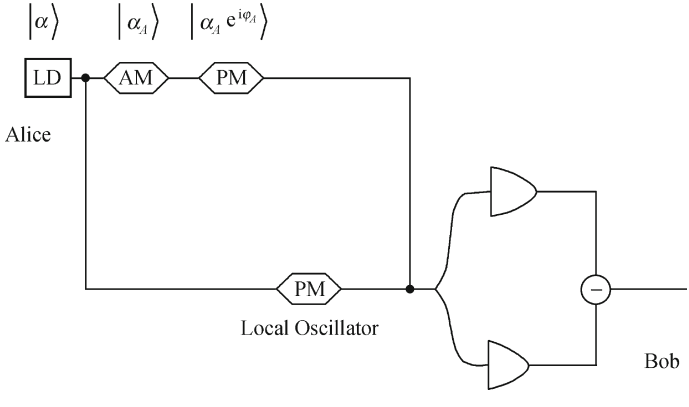

Fig. 8.13. An amplitude and phase encoding scheme

In Fig.8.13, an intense coherent state signal is emitted into a beam splitter

which is unbalanced and only a small fraction of the intensity which include hundreds photons is directed to an amplitude modulator and a phase modulator. The sender called Alice randomly generates a set of continuous signal denoted by random variables α_A and adds to amplitude modulator (AM) to change signal field intensity. The α_A obeys the rayleigh distribution $R(\sigma)$. The phase modulator (PM) changes the phase in $[0, 2\pi]$ randomly and sends a new coherent state $|\alpha_A e^{i\phi_A}\rangle$ to a receiver called Bob.

The amplitude-phase encoding rule has been applied in several QKD schemes. Typical schemes are presented in Refs.[**?**, **?**]. One may refers to these references for further reading.

8.4.3 PSK Encoding Rule

In previous two quadrature variables of a coherent state or squeezed state are encoded so that the message is encoded into different quantum states which cannot be distinguished. However, the datum rate of the private communication, e.g., the QKD system, which uses such encoding rules depends on the bandwidth of AD (analog to digital) and DA (digital to analog) convertor. Therefore, those schemes of the discrete modulation based on continuous carrier become important choice in the quantum private communication system. A typical scheme is the phase shifted key (PSK) scheme. Actually, this encoding rule is simpler and more suitable for high speed scenario.

The PSK scheme uses four nonorthogonal states generated by phase shift between the quantum signal and local oscillator to encode information. In experiment, laser pulses are split by an unsymmetrical beam splitter into two arms of a Mach-Zehnder interferometer shown in Fig.8.13. To encode information into the quantum signal, a random operation is applied on the quantum signal so that the output phase shift ϕ is one of states set $\{0°, 90°, 180°, 270°\}$, i.e., $\phi \in \{0°, 90°, 180°, 270°\}$. To decode the information, the quantum signal and the local oscillator are combined by a 50:50 beam splitter at the receiver's side. Two photodiodes are used to monitor the intensities from two output ports. Finally, two photodiode outputs are subtracted, and the difference of photoelectrons N_ϕ is measured. According to the theory presented in Section 8.3, photoelectrons N_ϕ is given by

$$N_\phi \propto \langle X \cos\phi + P \sin\phi \rangle. \tag{8.4.6}$$

Eq.(8.4.6) yields easily $N_{0°} \propto \langle X \rangle, N_{90°} \propto \langle P \rangle, N_{180°} \propto \langle -X \rangle$ and $N_{270°} \propto \langle -P \rangle$. Since X and P are conjugate variables, the generated four phase-shift states are clearly nonorthogonal.

As an example, consider implementation of the well-known BB84 QKD scheme based on this encoding rule [18 – 20]. In this case, Alice encodes her information using the PSK rule, then the encoded quantum signal and local oscillator are sent to Bob. At Bob's side, he applies a random operation

on the local oscillator with phase shift 0° or 90°. This corresponds to the random choice of the measurement basis in the BB84 protocol. After the combination of the signal and local oscillator with 50:50 beam splitter, the normalized quadrature amplitude of the signal $X = (\hat{a}_{sig} + \hat{a}^{\dagger}_{sig})/2$ may be obtained by $X_\phi = N_\phi/2\sqrt{n_{LO}}$, where a_{sig} is the annihilation operator of the signal. For each pulse, X_ϕ takes a random value due to quantum fluctuations. Theoretically, the probability distribution $P(X_\phi)$ is given by integrating the Wigner distribution over the conjugate variable $X_{\phi+90°}$. When the signal is in a coherent state, $P(X_\phi)$ is given by a Gaussian function with a standard deviation of 1/2. Fig.8.14 shows $P(X_\phi)$ for ϕ=0°, 90°, 180°, and 270° when the average signal photon number is 1. The probability distribution $P(X_{90})$ for ϕ=90° and $P(X_{270})$ for ϕ=270° are the same, so it is impossible to differentiate them. In this case, Bob selects the wrong basis. It is, however, possible to differentiate ϕ=0° from ϕ=180°. To do this, Bob sets up two threshold values m and $-m$ where $-m \leq m$. If the measured quadrature amplitude X_ϕ is larger than m (in this case, one may say that Bob's result is positive), Bob judges that ϕ=0°. If X_ϕ is smaller than $-m$ (Bob's result is negative), Bob judges that $\phi = 180°$. Finally, if X_ϕ is between $-m$ and m (Bob gets an inconclusive result), Bob abandons the judgement. This data procedure called as postselection. Note that because $P(X_{0°})$ overlaps $P(X_{180°})$, Bob's judgement is not always true. This intrinsic bit error rate e_{int} is the probability that ϕ is actually 180° even when Bob's result is positive, or ϕ=0° for Bob's negative result. The larger m is the smaller e_{int} becomes, but at the same time the probability, p_{inc}, that Bob gets inconclusive results becomes larger. After an appropriate number of pulses has been transferred, Bob tells Alice which phase shift he applied for each pulse. Alice, then, tells Bob which phase shifts were correct. The correctly measured data is interpreted as a binary sequence according to the coding scheme (ϕ_A=0° or 90°)=1 and (ϕ_A=180° or

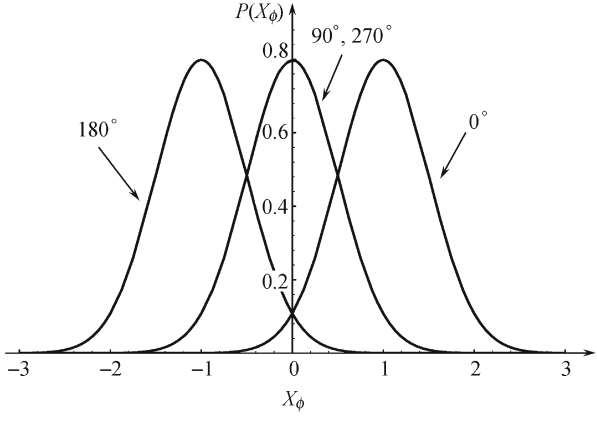

Fig. 8.14. Theoretical probability distributions of the quadrature amplitude for total phase shifts are 0°, 90°, 180°, and 270°

270°)=0 for Alice, and (positive result)=1 and (negative result)=0 for Bob. Finally, Alice and Bob perform error correction and privacy amplification procedures.

8.4.4 Polarization Encoding Rule

Four polarization states, e.g., horizon, vertical, and ±45°, have been employed to realize the BB84 QKD protocol with single photon signal in Chapter 7. This scheme inherently suggests that the qubit is represented in the 2-dimensional Hilbert space. However, a polarized coherent state may be conveniently represented as a two-mode coherent state, or two single-mode coherent states excited in the orthogonal directions [**?**]. The variables which completely determine polarization properties of the classical electromagnetic field are known as Stokes parameters [**?**], and their quantum mechanical analogues, Stokes operators which are Hermitian, are adequate for the quantum mechanical description of light polarization. Three of the four Stokes operators do not commute, yielding the well known uncertainty-like relations among them [**?**, **?**]. In fact, any pair of non commuting quantum continuous variables (quadratures, polarization variables) would be suitable for a continuous variable quantum private communication such as the QKD scheme. The expectation values as well as variances of the Stokes operators may be readily measured using linear optical devices and PIN photodiodes, without the need of a separate local oscillator and single photon detectors [**?**, **?**].

Before describing the polarization encoding rule, it is useful to briefly recall basic notions on polarization of light in classical and quantum optics. In general, any polarization state of light corresponds to a point on the Poincaré sphere shown in Fig.8.15 in the classical optics, which is the parametrization of three Stokes vectors in spherical coordinates.

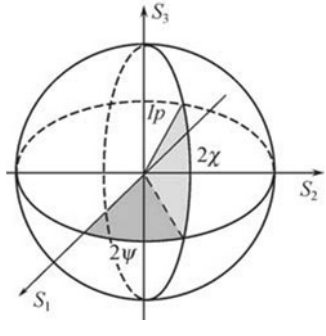

Fig. 8.15. Representations of polarization states of bright coherent on Poincaré sphere

Suppose that a monochromatic plane wave transmits in a linear, homo-

geneous, isotropic medium, its electric field $E(t)$ has the following form,

$$\mathbf{E}(z,t) = a_x\,\mathbf{e}_x + a_y\,\mathbf{e}_y \exp[-\mathrm{i}(\omega t - kz), \tag{8.4.7}$$

where x and y represent the horizon polarization vector and vertical polarization vector. Then, the relationship among Stokes parameters and intensity and polarization ellipse parameters is shown in following expressions,

$$\begin{cases} S_0 = |a_x|^2 + |a_y|^2 = I, \\ S_1 = |a_x|^2 - |a_y|^2 = I \cdot p\cos 2\psi \cos 2\chi = (I_x - I_y)\cdot p, \\ S_2 = a_x a_y^* + a_x^* a_y = I \cdot p \sin 2\psi \cos 2\chi = (I_{+45^\circ} - I_{-45^\circ})\cdot p, \\ S_3 = \mathrm{i}(a_x^* a_y - a_x a_y^*) = I \cdot p \sin 2\chi = (I_r - I_l)\cdot p, \end{cases} \tag{8.4.8}$$

where I is the total intensity of the beam, I_x , I_y $I_{\pm 45^\circ}$, I_r, and I_l are horizon, vertical, $\pm 45°$, right circle, left circle polarization wight of light intensity, respectively, and p is the degree of polarization which take on a range of [0,1]. The factor ψ represents the fact that any polarization ellipse is indistinguishable from one rotated by 180°, while the factor χ indicates that an ellipse is indistinguishable from one with the semi-axis lengths swapped accompanied by a 90° rotation. The Stokes vector spans the space of unpolarized, partially polarized, and fully polarized light. The four Stokes parameters do not form a preferred basis of the space, but rather were chosen because they can be easily measured or calculated as shown in Fig.8.16.

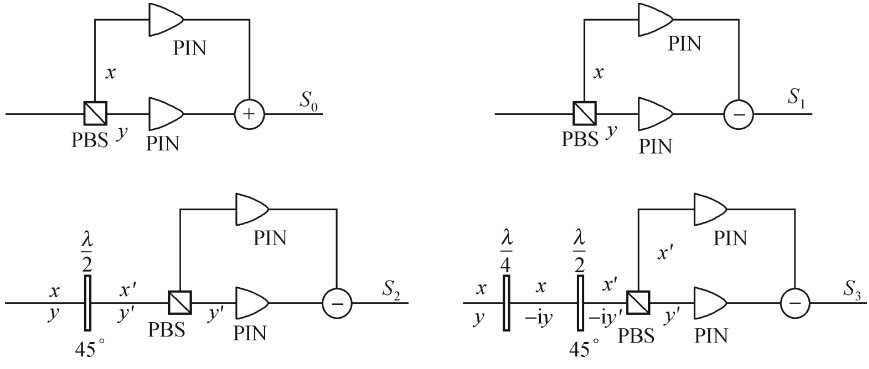

Fig. 8.16. Scheme for measuring Stokes parameters S_0, S_1, S_2, and S_3

In the quantum field, classical amplitudes of light are replaced by bosonic operators. Consider two orthogonal polarization modes of the electromagnetic field with polarizations oriented along the cartesian axis x and y. Then, the photon creation (annihilation) operators associated to each mode may be written as $\hat{a}_x^\dagger$ ($\hat{a}_x$) and $\hat{a}_y^\dagger$ ($\hat{a}_y$). These operators satisfy the usual commutation

relations,

$$\left[\hat{a}_j, \hat{a}_k^\dagger\right] = \delta_{jk}, \qquad j,k = x,y. \tag{8.4.9}$$

The Hermitian Stokes operators are defined as [**?**]

$$\begin{cases} \hat{S}_0 = \hat{a}_x^\dagger \hat{a}_x + \hat{a}_y^\dagger \hat{a}_y = \hat{n}_x + \hat{n}_y, \\ \hat{S}_1 = \hat{a}_x^\dagger \hat{a}_x - \hat{a}_y^\dagger \hat{a}_y = \hat{n}_x - \hat{n}_y, \\ \hat{S}_2 = \hat{a}_x^\dagger \hat{a}_y + \hat{a}_y^\dagger \hat{a}_x, \\ \hat{S}_3 = \mathrm{i}\left(\hat{a}_y^\dagger \hat{a}_x - \hat{a}_x^\dagger \hat{a}_y\right). \end{cases} \tag{8.4.10}$$

Consider the field prepared in the two-mode coherent state,

$$|\psi_{xy}\rangle = |\alpha_x\rangle_x |\alpha_y\rangle_y = \hat{D}_x(\alpha_x)\hat{D}_y(\alpha_y)|0\rangle_x |0\rangle_y, \tag{8.4.11}$$

where modes x and y prepared in two different single-mode coherent states $|\alpha_x\rangle$ and $|\alpha_y\rangle$ with $\hat{a}_j|\alpha_j\rangle = \alpha_j|\alpha_j\rangle$, respectively. The expectation values of the Stokes operators of the field in state $|\psi_{xy}\rangle$ read

$$\begin{cases} \langle \hat{S}_0 \rangle = |\alpha_x|^2 + |\alpha_y|^2, \\ \langle \hat{S}_1 \rangle = |\alpha_x|^2 - |\alpha_y|^2, \\ \langle \hat{S}_2 \rangle = \alpha_x^* \alpha_y + \alpha_y^* \alpha_x, \\ \langle \hat{S}_3 \rangle = \mathrm{i}\left(\alpha_y^* \alpha_x - \alpha_x^* \alpha_y\right). \end{cases} \tag{8.4.12}$$

They are the quantum Stokes parameters describing the polarization of a light beam, the intensity of which is $\langle \hat{S}_0 \rangle$. Here α_x denotes an electric field in the x direction and α_y denotes the amplitude in the y direction. Therefore, the coherent states correspond to fully polarized classical fields. However, the Stokes operators exhibit quantum mechanical fluctuations, e.g., their variances in the two-mode coherent state are

$$V_j \equiv \langle (\Delta \hat{S}_j)^2 \rangle = \langle \hat{S}_j^2 \rangle - \langle \hat{S}_j \rangle^2 = \langle \hat{S}_0 \rangle, \tag{8.4.13}$$

where $j = 0,1,2,3$. Easily, one may prove that the Stokes operators obey the following commutation relations,

$$\left[\hat{S}_j, \hat{S}_k\right] = 2\mathrm{i}\epsilon_{jkl}\hat{S}_l, \tag{8.4.14}$$

where $j,k,l = 1,2,3$. This means that the precision of simultaneous measurements of a pair of Stokes parameters is limited by an uncertainty-like relation. For instance,

$$(V_2 V_3)^{1/2} \geq \left|\langle \hat{S}_1 \rangle\right|. \tag{8.4.15}$$

It is worth remarking that the product of the variances of the Stokes operators is not a constant. However, for $\hat{S}_0$, whose mean value is basically the field intensity, one has

$$\left[\hat{S}_0, \hat{S}_j\right] = 0, \tag{8.4.16}$$

where $j = 1, 2, 3$. The quantum mechanical properties of Stokes operators turn out that they are suitable candidates for the quantum private communication, e.g., the QKD scheme. One most remarkable property of the Stokes operators is that their measurement may be accomplished with well established optical measurement methods. A simple way to measure the expectation value $\langle \hat{S}_j \rangle$ with $j = 1, 2, 3$ is as follows. Making use of Eq.(8.4.12) yields the following expressions,

$$\begin{cases} \langle \hat{S}_1 \rangle = I_x - I_y, \\ \langle \hat{S}_2 \rangle = I_{45^\circ} - I_{-45^\circ}, \\ \langle \hat{S}_3 \rangle = I_{\sigma_+} - I_{\sigma_-}, \end{cases} \tag{8.4.17}$$

then the expectation value $\langle \hat{S}_j \rangle$ could be acquired by measuring differences of the light intensity of various components. As an example, the expectation value $\langle \hat{S}_1 \rangle$ could be gotten by measuring differences of the light intensity of component along the reference axes (xy).

Now the principle of polarization encoding rule may be presented as follows. Alice generates a coherent beam of intensity S_0. A convenient preparation for that beam is a highly polarized two-mode coherent state. According to Eq.(8.4.11), if the beam is strongly polarized in the x direction so that $|\alpha_x|^2 \gg |\alpha_y|^2$, it follows from Eq.(8.4.12) that,

$$\langle \hat{S}_1 \rangle \approx \langle \hat{S}_0 \rangle = |\alpha_x|^2. \tag{8.4.18}$$

Simple calculation gives $\langle \hat{S}_1 \rangle \gg \langle \hat{S}_2 \rangle, \langle \hat{S}_3 \rangle$. Therefore, the uncertainty-like relation in Eq.(8.4.15) may be approximately written as

$$(V_2 V_3)^{1/2} \geq |\alpha_x|^2. \tag{8.4.19}$$

This means that the product of the variances of $\hat{S}_2$ and $\hat{S}_3$ is a constant for a given field intensity $|\alpha_x|^2$. As a consequence, one obtains

$$\left[\hat{S}_2, \hat{S}_3\right] = 2\mathrm{i}|\alpha_x|^2. \tag{8.4.20}$$

Defining quadrature operators $X = (\hat{a}^\dagger + \hat{a})$ and $Y = (\hat{a}^\dagger - \hat{a})\mathrm{i}$, one has $[\hat{X}, \hat{Y}] = 2\mathrm{i}$. It would be then convenient to normalize the Stokes operators as $\hat{s}_j = \hat{S}_j/|\alpha_x|$, so that $[\hat{s}_2, \hat{s}_3] = 2\mathrm{i}$.

In summary, there is a clear correspondence between noise properties of the pair of non-commuting quadrature operators (X, Y) and those of the

pair of normalized Stokes operators $(\hat{s}_2, \hat{s}_3)$. This means that it becomes possible to encode the key elements in the Stokes variables S_2 and S_3, which is the same as that is done in other continuous variables schemes based on the quadratures, e.g., gaussian modulating using the coherent state. The beam generated by Alice crosses an electro-optical modulator and a magneto-optical modulator in sequence, so that small random and independent modulations of the Stokes variables S_2 and S_3 are performed, which follow a Gaussian distribution with zero mean value and a variance V_m. Alice then sends the modulated signal field to Bob, who randomly chooses to measure either S_2 or S_3. As it is usual in quantum cryptography protocols, Alice and Bob establish communication via a public authenticated channel and Bob informs Alice which Stokes variable he has measured. After repeating that process several times, Alice and Bob share a set of Gaussian correlated variables, or key elements. Such raw data must be further processed in order to generate a common secret binary key (a string of bits). After converting the continuous correlated variables in bit strings, the error correction should be performed, and the information available to a potential eavesdropper (Eve) should be minimized via a "sliced reconciliation procedure" [**?**]. Then the bit string should be made secret with the privacy amplification.

A continuous variable QKD with polarization encoding rule has been presented in Ref.[**?**]. An attractive advantage of this scheme is that the local oscillator does not need. The key element is modulated on basis S_2 and basis S_3 randomly by an electro-optical modulator (EOM) and a magneto-optical modulator (MOM) which uses the Faraday effect of a magneto-optically active glass rod (Moltech MOS-04). By controlling the applied modulation voltage on the EOM and the current through the MOM coil, the polarization amplitude in S_3 and S_2 directions can be adjusted continuously. At the receiving station Bob measures either S_2 or S_3 displacement. Two resulting beams are reflected by a low-loss mirror onto silicon PIN photodiodes (Hamamatsu S3883). The signal is recorded by a fast digitizing oscilloscope (Tektronix TDS 420) and transferred to a computer for Bob's data processing. Such a kind of schemes could be used in free-space communication with high efficiency and key-exchange rate. Some similar schemes may refer to Refs.[**?**, **?**].

8.5 QKD with Continuous Variable Signal

In Chapter 4, fundamental principles of QKD has been described, and two standard QKD protocols, i.e., BB84 protocol and B92 protocol have been presented mathematically in cryptographic language. Physical implementation of a QKD scheme is significant in the private communication. By far, there are two ways for implementing QKD schemes. One relies on single photon signals and the other is associated with continuous variable signals. The for-

mer has been introduced in Chapter 7. This section presents implementation of QKD protocols using continuous variable signals.

8.5.1 QKD with Squeezed State

This subsection demonstrates how to implement physically the well-known BB84 protocol using squeezed state signal. This is actually the first principle scheme for QKD implementation using continuous variable quantum signal.

1) Scheme Descriptions

Suppose that two communicators Alice and Bob want to implement the BB84 protocol using squeezed state signal. The following steps are executed.

Step 1: Alice chooses a random string S_g with each element following a Gaussian distribution. Note here each random element in S_g is a continuous variable and following a Gaussian distribution. This is different from the random element used for implementing BB84 protocol with single photon signal in Chapter 7.

Step 2: Alice prepares two quadrature squeezed states $|\psi_1\rangle = |X_A(s) + \mathrm{i}P_A\left(\frac{1}{s}\right)\rangle$ and $|\psi_2\rangle = |X_A\left(\frac{1}{s}\right) + \mathrm{i}P_A(s)\rangle$. Their fluctuations on X and P are squeezed randomly. Therefore, when fluctuations on X of the squeezed state $|\psi_1\rangle$ is squeezed so that $\Delta X^2 = s\sigma_{N0}^2 < 1/4$, fluctuations on P should satisfy $\Delta P^2 = s^{-1}\sigma_{N0}^2 > 1/4$, and vice verse, where σ_{N0}^2 is the quantum vacuum noise power and parameter $s(s < 1)$ is referred to the squeezing factor of X and P in the squeezed state, respectively. To reach a maximal key-rate, the prepared squeezed states are restricted by following conditions: $\langle X_A\rangle$ and $\langle P_A\rangle$ have Gaussian profiles with mean 0 and variances $V_j\sigma_{N0}^2$ with $j = X, P$, respectively, where V_j denotes the modulation variance of signal. Physically, the squeezed state is split into a quantum signal and a local oscillator signal, and then these signals are entered into two arms which have been shown in Fig.8.13. The local oscillator is directly transmitted to the receiver and the quantum signal is entered to the encoding phase in the next step.

Step 3: Using the prepared states $|\psi_j\rangle$ $(j = 1, 2)$, Alice chooses two encoding bases to encode randomly the Gaussian elements x_j and p_j in the random string S_g into the prepared squeezed states $|\psi_j\rangle$ using one of two encoding bases. For example, when the basis X is chosen, Alice creates a displacement on the squeezed quadrature X in the prepared squeezed state $|\psi_1\rangle$ with an amount equalling the value of the Gaussian element x, i.e., $\langle X\rangle = x_1$, where the mean value of x_1 is 0 and the encoding variance of x_1 is $V_x(1)$. Similarly, the squeezed quadrature P of the state $|\psi_1\rangle$ is displaced suitably for the security so that the displaced X and P are indistinguishable. After have performed these encoding operations, statistical distributions of measurement outcomes on X is Gaussian with variance $V_x\sigma_{N0}^2 + s\sigma_{N0}^2$ since each squeezed

state gives an extra contribution of $s\sigma_{N0}^2$ to the variance and variance of $\langle P\rangle$ is $V_p\sigma_{N0}^2 + \frac{1}{s}\sigma_{N0}^2$. To reach the maximal security the distribution of measurement outcomes on X should be indistinguishable whether basis X or P is used by Alice. If this condition is fulfilled, Eve cannot obtain any indication on whether she is measuring a X or P in the squeezed state, whatever the statistics she accumulates. Consequently, a condition is yielded for indistinguishable X and P as follows,

$$V_x(1)\sigma_{N0}^2 + s\sigma_{N0}^2 = V_p(1)\sigma_{N0}^2 + \frac{1}{s}\sigma_{N0}^2 = V\sigma_{N0}^2.$$

Similarly, if the basis P is chosen the squeezed quadrature P in the prepared squeezed state $|\psi_2\rangle$ is displaced with an amount equalling the value of the Gaussian element p_1, i.e., $\langle P\rangle = p_1$, where the mean value of the p_1 is 0 and the encoding variance of p_1 is $V_p(1)$. In this case, one may get the following condition when fluctuations of P was squeezed,

$$V_p(2)\sigma_{N0}^2 + s\sigma_{N0}^2 = V_x(2)\sigma_{N0}^2 + \frac{1}{s}\sigma_{N0}^2 = V\sigma_{N0}^2.$$

Step 4: Alice sends the encoded squeezed state and the local oscillator signal to Bob. Bob measures randomly the received signal using basis X or P. Physically, the measurement is performed using homodyne detectors on the amplitude and phase of the encoded squeezed state.

Step 5: Now communicators Alice and Bob enter the error-correction and privacy amplification procedures, which have been described in Chapter 4.

2) Security Analysis

According to Shannon theory, if the noise is white and Gaussian and the signal-to-noise ratio (SNR) is Σ, the optimum information rate is

$$I_{AB} = 1/2\log_2(1+\Sigma). \tag{8.5.1}$$

Since this optimum can be closely approached only if the signal has a Gaussian statistics, the Gaussian modulation is involved.

From the viewpoint of security, one must assume that Eve has an arbitrary powerful computer, and thus she is able to reach this limit. The information rate is given by

$$\Delta I = I_{AB} - I_{AE}, \tag{8.5.2}$$

where I_{AB} and I_{AE} are referred to information rate between Alice and Bob, and between Alice and Eve. To reach an optimal security, one should assume I_{AE} being the maximum possible value.

Consider the individual attacks in a continuous channel which adds a Gaussian noise of variance σ^2 on each signal. In this case, if Alice uses the squeezed state $|X_A(s) + \mathrm{i}P_A\left(\frac{1}{s}\right)\rangle$, Bob got the optimal SNR on measurement of the basis X, on the other basis P the SNR will degrade. Hence,

information is gathered for the key only when Bob chooses a good basis, i.e., the measurement basis chosen correctly. To compute the private key rate ΔI, the good measurement and the bad measurement should be averaged. Thus, one obtains

$$\begin{aligned}\Delta I &= \frac{1}{2}[(I_{AB}^{G} - I_{AE}^{G}) + (I_{AB}^{B} - I_{AE}^{B})] \\ &= \frac{1}{4}\log_2 \frac{(1+\Sigma_B^G)(1+\Sigma_B^B)}{(1+\Sigma_E^G)(1+\Sigma_E^B)},\end{aligned} \tag{8.5.3}$$

where subscripts G and B refer to the good measurement basis and bad measurement basis, respectively. The I_{AB} in Eq.(8.5.3) is easy to compute for a Gaussian channel. If the protocol is invariant under the exchange of two quadratures X and P, the best strategy for Eve is to keep this property and don't disturb the state under her attacks. Therefore, when the line has a transmission coefficient η with no eavesdropping, the best attack for Eve is to take a fraction $1-\eta$ of the beam at Alice's site, and then send the fraction η to Bob through her own lossless line, e.g., a perfect teleporter. In this case, Eve is totally undetected, and she may get the maximum possible information according to the no-cloning theorem so that I_{AE} reaches the maximum. The average power on Bob's side and Eve's side are given respectively by

$$\begin{cases} P_B = \eta P_A + (1-\eta)N_0, \\ P_E = (1-\eta)P_A + \eta N_0, \end{cases} \tag{8.5.4}$$

where N_0 is the added noise in line, including the noise is induce by cloners or duplicators. Therefore, one gets

$$\begin{aligned} I_{AB}^{G} &= \frac{1}{2}\log_2(1+\Sigma_B^G) \\ &= \frac{1}{2}\log_2\left[\frac{\eta(V_x(1)\sigma_{N0}^2 + s\sigma_{N0}^2) + (1-\eta)\sigma_{N0}^2}{\eta s\sigma_{N0}^2 + (1-\eta)\sigma_{N0}^2}\right] \\ &= \frac{1}{2}\log_2\left(1 + \frac{V-s}{s+\chi}\right), \end{aligned} \tag{8.5.5}$$

$$\begin{aligned} I_{AB}^{B} &= \frac{1}{2}\log_2(1+\Sigma_B^B) \\ &= \frac{1}{2}\log_2\left[\frac{\eta(V_p(1)\sigma_{N0}^2 + \frac{1}{s}\sigma_{N0}^2) + (1-\eta)\sigma_{N0}^2}{\eta\frac{1}{s}\sigma_{N0}^2 + (1-\eta)\sigma_{N0}^2}\right] \\ &= \frac{1}{2}\log_2\left(1 + \frac{V-\frac{1}{s}}{\frac{1}{s}+\chi}\right). \end{aligned} \tag{8.5.6}$$

In the same way,

$$\begin{aligned} I_{AE}^{G} &= \frac{1}{2}\log_2(1+\Sigma_E^G) \\ &= \frac{1}{2}\log_2\left[\frac{(1-\eta)(V_x(1)\sigma_{N0}^2+s\sigma_{N0}^2)+\eta\sigma_{N0}^2}{(1-\eta)s\sigma_{N0}^2+\eta\sigma_{N0}^2}\right] \\ &= \frac{1}{2}\log_2\left(1+\frac{V-s}{s+\chi^{-1}}\right), \end{aligned} \tag{8.5.7}$$

and

$$I_{AE}^{B} = \frac{1}{2}\log_2\left(1+\frac{V-\dfrac{1}{s}}{\dfrac{1}{s}+\chi^{-1}}\right), \tag{8.5.8}$$

where $\chi = \dfrac{1-\eta}{\eta}$ and $V = V_x(1)+s = V_p(1)+1/s$. Subsequently, Eq.(8.5.3) is rewritten as

$$\Delta I = \frac{1}{2}\log_2\left(\frac{V+\chi}{1+V\chi}\right). \tag{8.5.9}$$

Eq.(8.5.9) implies that the key rate doesn't depend on the degree of squeezing. Clearly, when $V+\chi > 2+2V\chi$, the QKD protocol is secure according to the security criterion presented in Chapter 4. A further discussion on Eq.(8.5.9) will be presented in the next subsection for the security analysis of the QKD scheme using coherent states.

3) Implementation Analysis

Realization of this continuous variable protocol based on squeezed states would be very challenging as the generation of squeezed light has been a difficult experimental target for years. Probably, the main limitation in the implementation of this protocol is related to the loss of squeezing effected by attenuation in the transmission medium. This would dramatically decrease the SNR, and makes the protocol less efficient or insecure. In analogy with what is known for BB84, there is a threshold on the squeeze parameter that Alice should reach, below which the protocol would fail. Hence, there is yet no implementation for the continuous variable QKD using squeezed state signal.

8.5.2 QKD with Coherent State

The coherent state is an important source for implementing the quantum private communication especially the QKD scheme. This subsection demonstrates how to implement physically the well-known BB84 protocol using coherent state signal.

1) Scheme Descriptions

Step 1: Alice chooses a random string S_g with each element following a Gaussian distribution.

Step 2: Alice prepares a coherent state $|X + \mathrm{i}P\rangle$. Physically, the coherent state is split into a quantum signal and a local oscillator signal, and then these signals are entered into two arms which have been shown in Fig.8.13. The local oscillator is directly transmitted to the receiver and the quantum signal is entered to the encoding phase in the next step.

Step 3: Alice uses two independent Guassian elements in S_g to encode randomly conjugate variables X and P in complex plane. The detail encoding way is presented in Section 8.4.2. This encoding process generates an encoded coherent state $|X_A + \mathrm{i}P_A\rangle$, where the subscript A denotes Alice's operations.

Step 4: Alice sends the encoded coherent state $|X_A + \mathrm{i}P_A\rangle$ and the local oscillator signal to Bob. Bob measures randomly the received signal using basis X or P. Physically, the measurement is performed using homodyne detectors. After these steps a raw key is created.

Step 5: Finally, communicators Alice and Bob enter the error-correction and the privacy amplification procedures, which have been described in Chapter 4.

2) Security Analysis

For simplicity, consider the security against the individual attacks [**?**]. This strategy assumes that Eve clones two imperfect copies with sending one to Bob and measuring X_A and P_A of the other simultaneously using two homodyne detectors through a 50:50 Beamsplitter. According to the uncertainty principle, the cloning operations and measurement will induce additional noise to Bob even though Eve has unexhaustible resource and powerful ability. Subsequently, the variance at Bob's station is added. Thus, Alice and Bob can detect eavesdroppers through computing SNR.

Let the channel be a Gaussian noisy channel with transmission coefficient η, if the signal power from Alice is $V_A\sigma_{N0}^2 + \sigma_{N0}^2$, the power to noise ratio in Bob's side is given by

$$\begin{aligned} \frac{P_B}{P_{NB}} &= \frac{\eta(V_A+1)\sigma_{N0}^2 + (1-\eta)\sigma_{N0}^2}{\sigma_{N0}^2} \\ &= 1 + \frac{V_A}{1+\chi} \\ &= 1 + \Sigma_B, \end{aligned} \tag{8.5.10}$$

where $V_A\sigma_{N0}^2$ is the modulation variance and σ_{N0}^2 is the intrinsical vacuum quantum noise power,

Similar to the QKD scheme based on squeezed states, the best attack for Eve in this scheme is to take a fraction $1-\eta$ of the beam at Alice's site, and to send the fraction η to Bob through her own lossless line. Consequently, Eve is

then totally undetected, whereas she gets the maximum possible information according to the no-cloning theorem. Hence, the power to noise ratio what Eve has intercepted is

$$\begin{aligned}\frac{P_E}{P_{NE}} &= \frac{(1-\eta)(V_A+1)\sigma_{N0}^2 + \eta\sigma_{N0}^2}{\sigma_{N0}^2} \\ &= 1 + \frac{V_A}{1+\frac{1}{\chi}} \\ &= 1 + \Sigma_E. \end{aligned} \tag{8.5.11}$$

Eq.(8.5.10) suggests that the noise power increase $\chi\sigma_{N0}^2$ compared with that of lossless channel, where σ_{N0}^2 is the vacuum noise variance. Then the minimum added noise on Eve's side is $\chi^{-1}\sigma_{N0}^2$. Combining Eqs.(8.5.1) and (8.5.2), the information rate ΔI is calculated,

$$\Delta I = \tfrac{1}{2}\log_2(1+\Sigma_B) - \tfrac{1}{2}\log_2(1+\Sigma_E). \tag{8.5.12}$$

Both variances of each quadrature of the beam when it leaves Alice's realm is $V\sigma_{N0}^2 = V_A\sigma_{N0}^2 + \sigma_{N0}^2$. Using expressions $1+\Sigma_B = \dfrac{V+\chi}{1+\chi}$ and $1+\Sigma_E = \dfrac{V+1/\chi}{1+1/\chi}$, the above equation is simplified as

$$\Delta I = \frac{1}{2}\log_2\frac{V+\chi}{1+V\chi}. \tag{8.5.13}$$

Eq.(8.5.13) is same as Eq.(8.5.9). This means that the QKD scheme based on squeezed state has same secure bound with one based on coherent state. If $\chi < 1$, ΔI increase as a function of the signal modulation V_A. For large modulation ($\chi V \gg 1$), the asymptotic value of ΔI is

$$\Delta I_{asymp} = -\frac{1}{2}\log_2\chi = \frac{1}{2}\log_2\frac{\eta}{1-\eta}. \tag{8.5.14}$$

While the raw channel rate between Alice and Bob is

$$I_{AB} = \frac{1}{2}\log_2(V/(1+\chi)).$$

Accordingly, the security condition only relies on the SNR,

$$\Delta I > 0 \;\Leftrightarrow\; \Sigma_B > \Sigma_E \;\Leftrightarrow\; \chi < 1 \tag{8.5.15}$$

Since $\chi = (1-\eta)/\eta$ for a line with transmission coefficient η, the condition $\chi < 1$ requires that $\eta > 1/2$. Therefore, an available key can be obtained in principle when the transmission loss is less than 3 dB. Taking into account the standard loss of 0.2 dB/km in optical fibers at 1550 nm, the typical range would be around 10 km. However, implementation of the secure QKD

systems based on continuous variable can also operate beyond the 3 dB loss limitations using "reverse reconciliation" techniques which has been described in Chapter 4 so that the transmission distance may be extended.

3) Experimental Implementation

Experimental implementation of the above protocol has been presented in Ref.[**?**] over a standard single-mode telecom fiber of 25 km in a public telecom network. The experimental setup is shown in Fig.8.17. It operates at 1550 nm and consisting entirely of standard fiber optics and telecommunication components. Alice uses a laser diode, pulsed with a repetition rate of 500 kHz, to generate pulses with a width of 100 ns. Using a highly asymmetric fiber-optic coupler, these pulses are split into a strong phase reference, i.e., the local oscillator, containing typically 10^9 photons per pulse, and a weak signal, i.e., the quantum signal. The signal pulses are displaced in the complex plane, with arbitrary amplitude and phase, randomly chosen from a 2-dimensional Gaussian distribution centered at zero and with an adjustable variance $V_A N_0$. The selected amplitude and phase values are set by computer-driven electro-optics amplitude and phase modulators placed in the signal path. Finally, after part of the signal is removed for synchronization and system characterization purposes, Alice's desired modulation variance is adjusted with a second amplitude modulator and a variable attenuator.

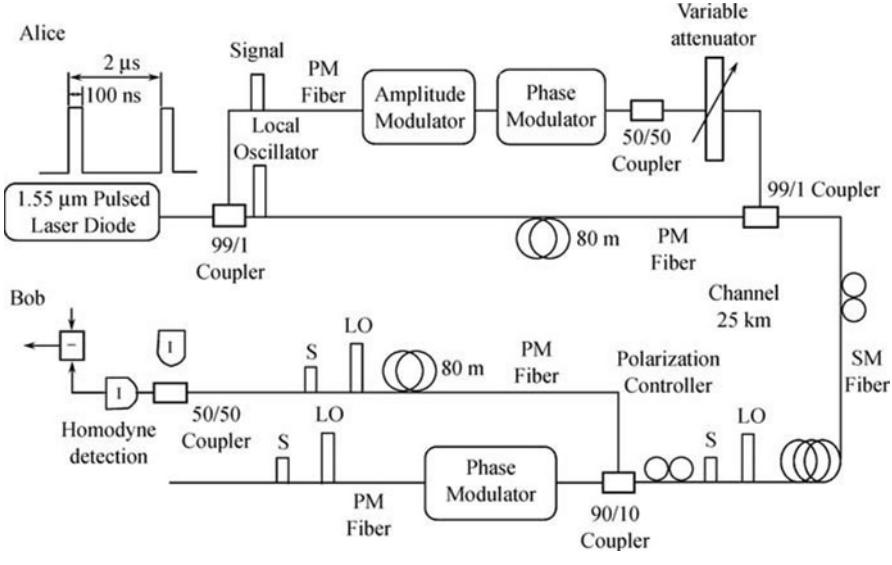

Fig. 8.17. Experimental setup for continuous variable QKD

Bob passively demultiplexes the signal and local oscillator using a 90/10 fiber-optic coupler, subsequently, introducing a 10% loss in the signal. Then, Bob selects the quadrature to be measured by adjusting the measurement

phase with a computer-driven phase modulator placed in the local oscillator path. Another 80 m delay line, placed now in the signal path, results in the signal and local oscillator pulses overlapping at the output beamsplitter of the interferometer. To ensure a good interference contrast, the path difference between the signal and local oscillator has to be adjusted to less than a centimeter. The selected quadrature measurement is then obtained with an all-fiber shot-noise limited time-resolved pulsed homodyne detection system. This measurement consists of the photocurrent substraction of two fast InGaAs photodiodes followed by a low noise charge amplifier and a constant gain amplifying stage.

8.5.3 Private Communication with EPR Correlations

EPR correlation is an important source in quantum information processing. Chapter 7 has presented ways for how to exploit EPR correlation for the quantum private communication with a single photon signal. This subsection further discusses the role of EPR correlation in the quantum private communication. A scheme which is employed to distribute random secret key as well as transmit meaningful message via choosing different input parameters of the nondegenerate optical parametric amplifier (NOPA) has been presented in Ref.[**?**]. The scheme is plotted in Fig.8.18, which executes the following steps.

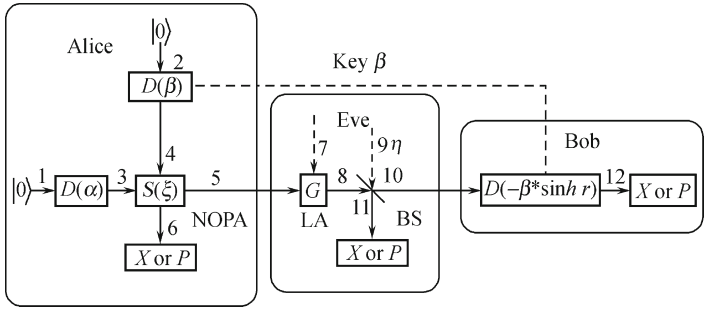

Fig. 8.18. Schematic of quantum private communication scheme based on continuous variable EPR correlations

NOPA: nondegenerate optical parametric amplifier, LA: linear amplifier, BS: beam splitter, $D(\alpha), D(\beta)$: displacement operators, $S(\xi)$: two-mode squeezing operator of NOPA, G: the gain of LA, η: the transmission coefficient of BS. The Arab numbers denote the modes

Step 1: Alice's modulation on two input modes $\hat{a}_1$ and $\hat{a}_2$ with displacement operators $\hat{D}(\alpha = x + \mathrm{i}x)$ and $\hat{D}(\beta = y + \mathrm{i}y)$ respectively yields two new modes $\hat{a}_3 = \hat{D}^{\dagger}(\alpha)\hat{a}_1\hat{D}(\alpha)$ and $\hat{a}_4 = \hat{D}^{\dagger}(\beta)\hat{a}_2\hat{D}(\beta)$, which are the input modes of NOPA. The corresponding output modes of NOPA are $\hat{a}_5 = \hat{S}^{\dagger}(\xi)\hat{a}_3\hat{S}(\xi)$

and $\hat{a}_6 = \hat{S}^{\dagger}(\xi)\hat{a}_4\hat{S}(\xi)$. When a squeeze parameter r is proper, the mode $\hat{a}_5$ correlates with mode $\hat{a}_6$, and this correlation increases with r to be larger. The random numbers x and y are drawn from Gaussian probability distributions $X \sim N(0, \Sigma^2)$ and $Y \sim N(0, \sigma^2)$, respectively.

Step 2: Alice calculates the parameter F_a between $\hat{a}_5$ and $\hat{a}_6$ according to Eq.(2.3.49), and measures either X or P of $\hat{a}_6$ during some time slots. Alice writes down both measurement results and corresponding time slots for detecting Eve after finishing transmission, while the mode $\hat{a}_5$ is sent to Bob.

Step 3: Bob applies $D[-\beta^* \sinh(r)]$ to the received mode $\hat{a}_{10}$. The mode $\hat{a}_{10}$ is the same as $\hat{a}_5$ when the Eve is absent in the quantum channel. After finishing the operation, Bob measures either X or P of the output mode $\hat{a}_{12}$.

Step 4: Alice tells Bob both her measurement results and corresponding time slots through a classical public channel. Bob estimates the parameter F_b according to Eq.(2.3.49) by comparing Alice's measurement results with his own measurement results with the corresponding time slots. If $F_b > F_a$, Eve exists; while $F_b = F_a$, Eve doesn't exist.

Step 5: To distribute meaningless random string of symbols, i.e., quantum key distribution, the parameter y is chosen to be 0 in Step 1, consequently $\beta = 0 = \beta^*$. In terms of the measurement results, Alice and Bob may generate a quantum key. If Alice wants to transmit a meaningful message to Bob, i.e., as a quantum encryption algorithm, the parameters x is regarded as the message which needs to be transmitted to Bob while y acts as the private key shared between Alice and Bob. After finished Step 3, Bob decodes Alice's message while the attacker is detected in Step 4. In the quantum encryption process, the message will be divided into L blocks in order to prevent Eve from obtaining more useful information, above four steps are executed for each block.

In the following a brief remark on the security for the above scheme is presented. The details may be referred to Ref.[**?**]. Since this scheme can be employed to distribute random secret key as well as transmit meaningful message via choosing different input parameters of NOPA, two kinds securities are associated. It is noted that the key distribution and data encryption are different cryptographic objectives and, therefore, have different sets of criteria by which to evaluate performance. In the QKD process, Alice and Bob only concern with the secret information rate

$$\Delta I = I(\alpha, \beta) - I(\alpha, \epsilon),$$

where $I(\alpha, \beta)$ denotes the mutual information between Alice and Bob, and $I(\alpha, \epsilon)$ denotes the mutual information between Alice and Eve. While in the quantum encryption process, Alice and Bob concern with the maximal mutual information $I_{max}(\alpha, \epsilon)$ between Alice and Eve. To analyze the security for the QKD scheme based on continuous variables, one should choose a certain attack strategy such as the Gaussian-cloner attack strategy presented in Ref.[**?**]. Then, under such the kind of attack strategies one calculates the

secret information rate ΔI. If secret information rate satisfies

$$\Delta I > 0,$$

the proposed scheme is security and subsequently a security condition can be naturally yielded. This process has been described in detail in the previous QKD schemes. For the security of the quantum data encryption algorithm, one may analyze the security making use of the Shannon private communication model which has been described in Chapter 5. One should note that the security analysis between the QKD and quantum encryption and decryption algorithms are different. A detail security analysis on such algorithm will be presented in next section for a quantum symmetrical key algorithm based on coherent state.

8.6 Quantum Encryption with Coherent States

As described in Chapter 5, a cryptosystem may be employed to protect confidentiality of the transmitted message in a communication system. In Section 8.5.3, an algorithm which uses NOPA was suggested to encrypt message. This section introduces a new quantum symmetrical key cryptosystem. Similar to the classic symmetrical key algorithm, a pre-shared secret key is necessary in such algorithm. This key may be directly generated using a QKD way or classic key distribution way. Also it may be created using the well-known linear feedback shift-register [35] (LFSR) based on a seed key k_0. In Refs.[36 – 39] a quantum symmetrical key algorithm with LSFR based on a seed key k_0 has been proposed and has been physically implemented using coherent states. This section presents a brief description on this algorithm.

8.6.1 Algorithm Descriptions

Generally, a cryptosystem consists of three parts: key generation, encryption algorithm and decryption algorithm. In the involved algorithm, these phases are described as follows.

1) Key Generation

Suppose that communicators Alice and Bob pre-share a s-bit seed key k_0. When a long key is necessary they extend the seed key k_0 to a M-bit pseudo-random extended-key K using a publicly known s-bit LSFR of maximal length, where $M = (2^s - 1)$. Then the extended-key is blocked into continuous disjointed r-bit blocks and then passed through an invertible r-bit to r-bit deterministic mapping function, referred to as a "mapper". Note that an LFSR is just the way that is used to extend k_0 into K which could be alternated using more complex mathematical ways.

2) Encryption Algorithm

The coherent state is encoded according to its polarization or phase. In both schemes, the fundamental and irreducible measurement uncertainty of coherent states are the key element giving security. In the polarization encoding scheme, the two-mode coherent states employed are

$$\begin{cases} |\Psi_m^{(a)}\rangle = |\alpha\rangle_x \otimes |\alpha\, \mathrm{e}^{\mathrm{i}\theta_m}\rangle_y, \\ |\Psi_m^{(b)}\rangle = |\alpha\rangle_x \otimes |\alpha\, \mathrm{e}^{\mathrm{i}(\theta_m+\pi)}\rangle_y, \end{cases} \tag{8.6.1}$$

where $|\alpha\rangle$ denotes a coherent state, $\theta_m = \pi m/M$, $m \in \{0, 1, 2, \ldots, (M-1)\}$, M is odd, and subscripts x and y indicate two orthogonal polarization mode-functions. Plotting on the Poincaré sphere these $2M$ polarization states form M bases that uniformly span a great circle as shown in Fig.8.19 (a). In the phase encoding scheme, the single-mode coherent states employed are

$$\begin{cases} |\Psi_m^{(a)}\rangle = |\alpha \mathrm{e}^{\mathrm{i}\theta_m}\rangle, \\ |\Psi_m^{(b)}\rangle = |\alpha \mathrm{e}^{\mathrm{i}(\theta_m+\pi)}\rangle, \end{cases} \tag{8.6.2}$$

with $m \in \{0, 1, 2, \ldots, (M-1)\}$. These $2M$ states form M antipodal-phase pairs that uniformly span the phase circle, as shown in Fig. 8.19(b).

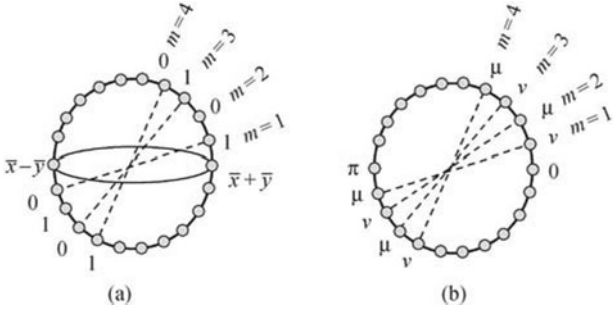

Fig. 8.19. Quantum state plotted in Poincar é sphere for encryption procedures

a) M pairs of orthogonal polarization states uniformly span a great circle of the Poincaré sphere; b) M pairs of antipodal phase states uniformly span a phase circle

Now consider how to encrypt the message, i.e., data bits, in both encryption schemes. In the polarization encoding scheme, if m is even the mapping $(0,1) \rightarrow (|\Psi_m^{(a)}\rangle, |\Psi_m^{(b)}\rangle)$ is used, i.e., encoding the logical bits 0 and 1 to the states $|\Psi_m^{(a)}\rangle$ and $|\Psi_m^{(b)}\rangle$, respectively. While if m is odd the mapping $(0,1) \rightarrow (|\Psi_m^{(b)}\rangle, |\Psi_m^{(a)}\rangle)$ is adopted. Cryptographically, the involved mappings correspond to the encryption procedures. These operations result in the logical bits which map the polarization states on the Poincaré sphere

to be interleaved $0, 1, 0, 1, \ldots$ as shown in Fig.8.19(a). The phase encoding scheme is similarly organized with slight revision on data bits which are defined differentially, i.e., differential-phase-shift keying (DPSK). In detail, if m is even the DPSK mapping is $(0, \pi) \rightarrow (|\Psi_m^{(a)}\rangle, |\Psi_m^{(b)}\rangle)$, and mapping $(0, \pi) \rightarrow (|\Psi_m^{(b)}\rangle, |\Psi_m^{(a)}\rangle)$ is employed for odd m. Labelling the states which correspond to the DPSK phases of "0" and "π" using μ and ν, respectively, then the logical zero is mapped to $|\Psi_m^{(\mu)}\rangle$ ($|\Psi_m^{(\nu)}\rangle$) if the previously transmitted state was from the set $\{|\Psi_m^{(\mu)}\rangle\}$ ($\{|\Psi_m^{(\nu)}\rangle\}$) and logical one is mapped to $|\Psi_m^{(\mu)}\rangle$ ($|\Psi_m^{(\nu)}\rangle$) if the previously transmitted state was from the set $\{|\Psi_m^{(\nu)}\rangle\}$ ($\{|\Psi_m^{(\mu)}\rangle\}$). These results in the mapping of symbols on the phase circle to be interleaved $\mu, \nu, \mu, \nu, ...$, as shown in Fig.8.19(b).

3) Decryption Algorithm

At the receiving end, the intended receiver, Bob, uses the same s-bit secret key and LFSR/mapper to apply unitary transformations to his received quantum states according to the M-bit pseudo-random extended-key K same with the sender Alice. These transformations correspond to polarization-state rotations for the polarization encoding scheme, and phase shifts for the phase encoding scheme. In either case the transmitted M-ry signal set is reduced to a binary signal-set. The resulting states under measurement, depending on the logical bit, are

$$\begin{cases} |\Psi^{(a)}\rangle' = |\eta\alpha\rangle_x \otimes |\eta\alpha\rangle_y, \\ |\Psi^{(b)}\rangle' = |\eta\alpha\rangle_x \otimes |-\eta\alpha\rangle_y, \end{cases} \tag{8.6.3}$$

for the polarization encoding scheme, and

$$\begin{cases} |\Psi^{(a)}\rangle' = |\eta\alpha\rangle, \\ |\Psi^{(b)}\rangle' = |-\eta\alpha\rangle, \end{cases} \tag{8.6.4}$$

for the phase encoding scheme, where η is the channel transmissivity. For both schemes the states are then demodulated and differentially detected. Specifically, a fixed $\pi/4$ polarization rotation on states in polarization encoding scheme results in detected states,

$$\begin{cases} |\widetilde{\Psi}^{(a)}\rangle = |\sqrt{2}\eta\alpha\rangle_x \otimes |0\rangle_y, \\ |\widetilde{\Psi}^{(b)}\rangle = |0\rangle_x \otimes |\sqrt{2}\eta\alpha\rangle_y, \end{cases} \tag{8.6.5}$$

whereas the temporally-asymmetric interferometry in phase encoding implementation results in the detected states,

$$\begin{cases} |\widetilde{\Psi}^{(a)}\rangle = |\eta\alpha\rangle_1 \otimes |0\rangle_2, \\ |\widetilde{\Psi}^{(b)}\rangle = |0\rangle_1 \otimes |\eta\alpha\rangle_2. \end{cases} \tag{8.6.6}$$

An important feature is that Bob does not require high precision in applying decryption transformations to a transmitted bit. While the application of a slightly incorrect polarization/phase transformation result in a larger probability of error for the bit, it does not categorically render a bit to be in error. For small perturbations to the polarization/phase rotation, the majority of the signal energy stays in one of the two detection modes. The same applies to Bob's detector noise; while an ideal detector allows for optimized performance, a noisy detector does not limit Bob's decryption ability beyond an increased probability of the bit error.

4) Security Analysis

For the cryptographic objective of data encryption, whatever be it classical or quantum-noise-protected, some relevant information-theoretic quantities are $H(X|Y^B, K)$, $H(X|Y^E)$, $H(K|Y^E)$, where X, Y^B, Y^E and K are random variables, they denote the n-bit transmitted message (plaintext), Bob's and Eve's n-bit observations of the encrypted plaintext (ciphertext), and the secret key shared by legitimate communicators, respectively. These quantities describe i) the error rate for the legitimate users; ii) the secrecy of data bits when under attack; and iii) the secrecy of the secret key when under attacks. When launched on either data bits or secret keys, cryptographic attacks are normally divided into two categories, i.e., known-plaintext attacks and ciphertext-only attacks. The ciphertext-only attacks correspond to situations where the probability distribution $p(X)$ is uniform, according to the attacker. In other words, all 2^n possible messages are transmitted with equal probability. A known-plaintext attack corresponds to all situations where $p(X)$ is nonuniform including the totally degenerate deterministic case of chosen-plaintext. Some examples for the known-plaintext attacks include knowledge of the native language of the message or perhaps some statistical knowledge on the message content. While there are clearly varying degrees of known-plaintext attacks.

There are two weaknesses in the classical encryption process employing an inefficient one-time pad. One is that the total data uncertainty $H(X)$ given observation Y is bounded by the key uncertainty, i.e., $H(X) \leq H(K)$ since it is easy to measure Y correctly in the classical communication. The other is that the key K may be found by a known-plaintext attack when the eavesdropper (Eve) knows the output-input pairs (Y, X) for certain amounts of data. In the involved quantum algorithm, however, to extract information from even a full copy of the quantum signal without knowing K, Eve has to make a sub-optimal measurement that would yield information on all possible signal sets for the purpose of either estimating X or finding K from a known plaintext attack. While Bob has a better channel/observation than Eve since he know the private key. Thereby, $H(X)$ is not bounded by $H(K)$ because Eve cannot obtain exactly the observation Y which Bob obtained via the optimal quantum measurement utilizing the private key K. In addition, $P(X)$ may be uniform. In contrast to classical cryptography, the scheme

against ciphertext-only attacks, under the individual attacks is proved to be secure.

Physically, the security can be described as follows. In the algorithm described in above, Alice encodes each data bit into two orthogonal mode coherent states in an infinite-dimensional Hilbert space spanned by M pairs of antipodal signals $\{|\Psi_m^j\rangle\}$ with $j = 0, 1$, represented in Eq.(8.6.1). A private key K which is generated via a conventional encryption mechanism driven by a seed key k_0, is used to encode the bit $\{0, 1\}$ to the corresponding pair of $\{|\Psi_m^j\rangle\}$. Bob utilizes a quantum receiver to get information bit by pre-shared the private key. To obtain maximal information on the transmitted message, the attacker has to operate the ciphertext states with an optimal attack strategy, i.e., a suitable measurement in quantum ways. Since the attacker is absent of prior knowledge on the seed or the private key, he cannot obtain exactly the ciphertext states, consequently, $Y^{\mathrm{E}} \neq Y^{\mathrm{B}}$. Let $X_n, Y_n^{\mathrm{E}}, Y_n^{\mathrm{B}}$ be the classical random variables describing the data with length n, Eve's observation, and Bob's observation, respectively. Eve can make any quantum measurement on her copy of the quantum signal to obtain Y_n^{E} with her attacks. In the standard classical cipher, one always has $Y_n^{\mathrm{E}} = Y_n^{\mathrm{B}} = Y_n$, but this relations is impossible in quantum case since the nonorthogonality of the ciphertext states. In practices, Eve measures her copy of the quantum state collapsing to a single bit l_i,

$$l_i = x_i \oplus \tilde{k}_i \tag{8.6.7}$$

where x_i is the data bit at the ith position of the data sequence, and $\tilde{k}_i$ is a fixed function of the private key that determines the basis used for that position chosen by Eve. Each l_i is 0 or 1 according to Eve's observation on the ith two orthogonal coherent state lying on the left or right half-circle.

In Fig.8.20, the small shade circles represent the quantum noise in coherent state. The intrinsic uncertain coherent-state angular with standard deviation $\Delta\theta \simeq 1/|\alpha_0|$ is also shown in Fig.8.20 using dot line, where α_0 is the amplitude of coherent state. The number of pairs of basis included in $\Delta\theta$ is

$$N_\Delta = \frac{\Delta\theta}{\frac{\pi}{M}} = \frac{M}{\pi|\alpha_0|}. \tag{8.6.8}$$

Hence, the bit error rate to Eve is given by

$$P_b^E \simeq 2/(\pi|\alpha_0|). \tag{8.6.9}$$

In fact M pairs of bases are selected with uniform marginal probability for each mode coherent state.

Under the ciphertext-only attack, an estimate of the bit error rate to Eve is simply calculated with the numerical calculations via the optimal binary decision measurement, assuming that the measured state is uniformly distributed within a standard deviation only. The calculation result shows that $P_b^E \to \frac{1}{2}$ when $\mathrm{M} \to \infty$. Therefore, the quantum data encryption algorithm

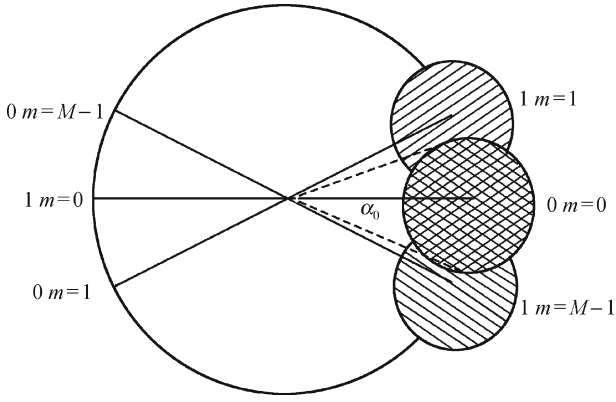

Fig. 8.20. Quantum noise due to the uncertainty of coherent state phase

equals the "one time pad" under ciphertext-only attack when M is very large.

However, if Eve could get value of the phase angular θ_e via the measurement on $\{|\Psi_m^j\rangle\}$ and some pairs of plaintext and ciphertext is acquired by Eve, the corresponding private key elements could be gotten according to Eq. (8.6.7). Thus, under the known-plaintext attack, the security performance of the quantum noise encryption is equal to that of the classical data encryption depending on the Shannon limit, $H(X_n|Y_n) \leq H(K)$.

The security analysis has attracted much attention, further readings may refer to Refs.[36, 40 – 46].

8.6.2 Polarization Encoding Implementation

A high-speed (500 Mbps) quantum-noise-protected data-encryption system over 100 km of telecommunication fiber by the use of coherent states is shown as follows. The system coexisting with classical data traffic utilized Dense wavelength division multiplexing (DWDM) technology. As illustrated in Fig.8.21, a dynamical polarization-controller (DPC) is adjusted to project the light from a 1550.1 nm wavelength DFB laser equally into two polarization modes of Alice's 10 GHz bandwidth fiber-coupled $LiNbO_3$ phase modulator (PM). The modulator introduces a relative phase (0 to 2π radians) between the two polarization modes, driven by the amplified output of a 12-bit digital-to-analog (D-A) board. A software LFSR, which is implemented on a personal computer (PC), yields a private-key K, when combined with the data bit, instructs the generation of one of the two states described in Eqs. (8.6.1) and (8.6.2).

On passing through the 100 km long wavelength division multiplexing (WDM) network, the received light is amplified by a home-built erbium-doped-fiber amplifier (EDFA) with about 30 dB of small-signal gain and a

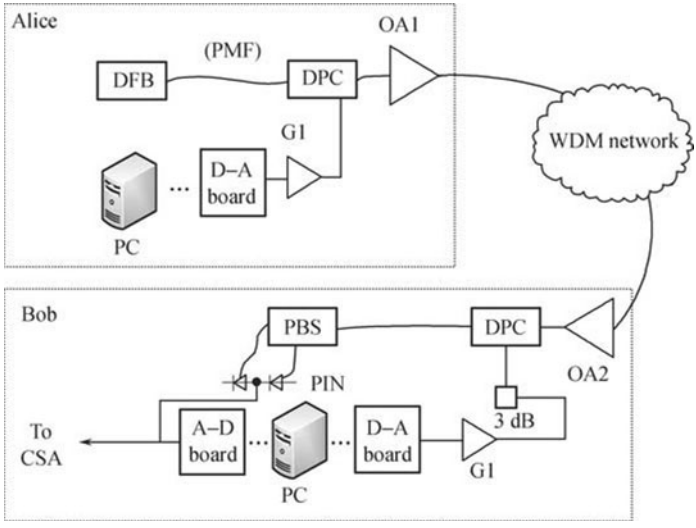

Fig. 8.21. Experiment implementation based on polarization encoding rule

G1, RF power amplifier; OA1, low-noise EDFA followed by a Bragg-grating filter; DPC, dynamical polarization controller

noise figure very close to the quantum limit (NF $\simeq$ 3 dB). Before passing through Bob's PM, the received light is sent through a second DPC to compensate fluctuations of the polarization state that occurs in the 100 km long fiber line. While these rotations fluctuate with a bandwidth on the order of kilohertz, the magnitude of fluctuations drops quickly with frequency, allowing the use of a manual polarization controller to track out such unwanted polarization rotations. In practical implementations Bob's measurements could be used to drive an automated feedback control on DCP.

The relative phase shift (polarization rotation) introduced by Bob's modulator is determined by the private key K generated through a software LFSR in Bob's PC and applied via the amplified output of a second D-A board. After this phase shift has been applied, the relative phase between the two polarization modes is 0 or π, corresponding to a 0 or 1 according to the private key: if K is even then $(0, \pi) \rightarrow (0, 1)$ and if K is odd then $(0, \pi) \rightarrow (1, 0)$. With use of a fiber-coupled polarization beam splitter (FPBS) oriented at $\pi/4$ radians with respect to the modulator's principal axes, the state under measurement is direct-detected by using two 1 GHz bandwidth InGaAs PIN photodiodes operating at the room temperature, one for each of the two polarization modes. The resulting photocurrents are amplified by a 40 dB gain amplifier, sampled by an analog-to-digital (A-D) board, and stored for analysis. The overall sensitivity of Bob's preamplified receiver is measured to be 660 photons/bit for an 10^{-9} error probability.

8.6.3 Phase Encoding Implementation

Although the polarization encoding scheme is technically possible, the polarization alignment required at Bob's side makes it much less attractive than a phase encoding scheme, which is polarization-insensitive, thus has higher speed and transfer longer. As illustrated in Fig.8.22, −25 dBm of power from a 1550.9 nm wavelength DFB laser is projected into Alice's 10 GHz bandwidth fiber-coupled PM. Driven by the amplified output of a 12 bit D-A board, the modulator introduces a relative phase (0 to 2π radians) between temporally neighboring symbols. A 4.4 kb software LFSR, which is implemented on a PC, yields a private key K, when combined with the data bit, instructs the generation of one of the two states described in Eqs.(8.6.3) and (8.6.4) at an 650 Mbps data rate. Before leaving the transmitter, the encrypted signal is amplified with an EDFA (OA1) to a saturated output power of 2 dBm.

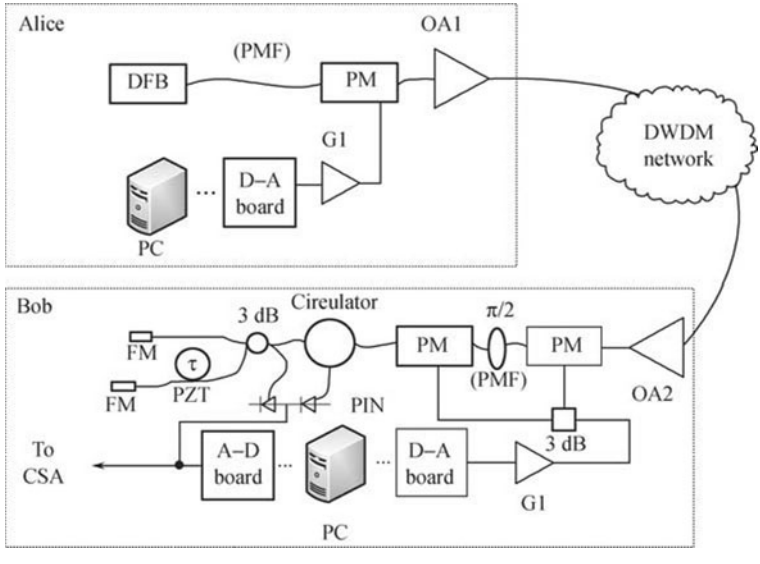

Fig. 8.22. Experiment implementation based on phase encoding rule

G1, RF power amplifier; OA1,OA2, low-noise EDFA followed by a 25GHz-passband Bragg-grating filter; PMF, polarization-maintaining fiber; Circ., optical circulator.

After having been passed through an 200 km long WDM line, the received light, i.e., quantum signal, is amplified by another EDFA (OA2) with about 30 dB of small-signal gain and a noise figure very close to the quantum limit (NF $\simeq$ 3 dB). The light then passes through a pair of 10 GHz bandwidth polarization-maintaining-fiber-coupled PMs oriented orthogonally with respect to each other so that the $\hat{x}$ ($\hat{y}$) polarization mode of the first modulator projects onto the $\hat{y}$ ($\hat{x}$) mode of the second modulator. The effect of such concatenation is to apply an optical phase modulation that is independent

of the polarization state of the incoming light. The relative phase shift introduced by Bob's modulator pair is determined by the private key K generated through a software LFSR in Bob's PC and applied via the amplified output of a second D-A board. After this phase shift has been applied, the relative phase between temporally neighboring states is 0 or π (differential phase-shift keying), differentially corresponding to bit 0 or 1.

The decrypted signal then passes through a fiber-coupled optical circulator and into a temporally asymmetric Michelson interferometer with one bit-period round-trip path-length delay between two arms. Use of Faraday mirrors (FM) in the Michelson interferometer ensures good polarization-state overlap at the output, yielding high visibility interference. Light from two outputs of the interferometer is directly detected by using two room temperature 1 GHz bandwidth InGaAs PIN photodiodes set up in a difference photocurrent configuration. The resulting photocurrent is split into two parts, one is sampled by an A-D board and stored for analysis and the other puts into a communication signal analyzer (CSA) to observe eye patterns. It is note here that the employed detectors are direct intensity measurement which has been described in Section 8.3.1. This is the same as that in the classic optical telecommunication but is different from the detection employed in QKD schemes with continuous variable signals.

8.7 Quantum Identification with Coherent States

The fundamentals of quantum authentication has been described in Chapter 6, here a quantum identity authentication system between two communicators using coherent state is demonstrated [**?**].

Let Alice and Bob are two communicators, and employ coherent state of light as the quantum signal. Suppose that Alice and Bob pre-share a private key k which consists of binary bits, i.e., $k = (k_1, k_2, k_3)$, where $k_1 = (k_1^1, k_1^2, \ldots, k_l^l)$, $k_2 = (k_2^1, k_2^2, \ldots, k_2^m)$, and $k_3 = (k_3^1, k_3^2, \ldots, k_3^n)$. The lengths l, m and n are chosen according to $m/l = r$ and $n/l = s$ with r and s are integers. The protocol executes as following steps.

Step 1: The strings k_2 and k_3 are divided equally into l groups with r and s bits in each group, respectively. Then, create p_i and q_i according to following ways,

$$p_i = a_{i_r} 2^{r-1} + a_{i_{r-1}} 2^{r-2} + \ldots + a_{i_0}, \tag{8.7.1}$$

$$q_i = b_{i_s} 2^{s-1} + b_{i_{s-1}} 2^{s-2} + \ldots + b_{i_0}, \tag{8.7.2}$$

where a_{i_j} $(j = 0, 1, \ldots r)$ and b_{i_k} $(k = 0, 1, \ldots, s)$ are elements of ith group in k_2 and k_3, respectively, and $i = 1, 2, \ldots, l$. Using obtained p_i and q_i yields, $\Phi_{p_i} = 2\pi p_i / 2^r$ and $\Theta_{q_i} = \pi q_i / 2^s$, respectively.

Step 2: Prepare a coherent state, and then encode k_1 into polarization states of the coherent state, then, a string of encoded polarization states $|\Psi(\Phi_{p_i} = k_1^i \pi, \Theta_{q_i} = k_1^i \pi)\rangle$ is obtained.

Step 3: Construct a rotation operator $R_i = R(\Phi_{p_i}, \Theta_{q_i})$ by employing Φ_{p_i} and Θ_{q_i} as rotation angles. Then applying the operator R_i on the polarization state $|\Psi(k_1^i\pi, k_1^i\pi)\rangle$, one obtains $|\Psi(k_1^i\pi + \Phi_{p_i}, k_1^i\pi + \Theta_{q_i})\rangle$ at $p_i + q_i$ being the odd number, and $|\Psi((k_1^i\pi \oplus 1) + \Phi_{p_i}, (k_1^i\pi \oplus 1) + \Theta_{q_i})\rangle$ at $p_i + q_i$ being the even number. Physically, the initial polarization state $|\Psi(k_1^i\pi, k_1^i\pi)\rangle$ is transformed into an arbitrary elliptical polarization state so that obtained polarization states are undistinguished.

Step 4: Applying R^{-1} on the resulted state, then the receiver judges the polarization according to the parity of $p_i + q_i$. If the k_1 can be obtained, the sender's identity is true, otherwise, it is wrong. This step is actually a reverse process of the above step.

To demonstrate the security, a brief remark on the security of the above scheme is presented. The overlap between arbitrary two polarization states $|\Psi(\Phi_j, \Theta_k)\rangle$ and $|\Psi(\Phi_p, \Theta_q)\rangle$ are

$$|\langle\Psi(\Phi_j, \Theta_k)|\Psi(\Phi_p, \Theta_q)\rangle|^2 \approx \exp\left[\frac{(\Phi_j - \Phi_p)^2 + (\Theta_k - \Theta_q)^2}{2 \times \left(\dfrac{1}{\langle n\rangle}\right)}\right]. \quad (8.7.3)$$

Eq.(8.7.3) defines the uncertainty of polarization angle generated by the shot noise associated with the coherent states. $\sigma^2 = \dfrac{1}{\langle n\rangle}$ is the uncertainty associated with light's shot noise. It is stressed here that the parameter σ can't be overcome regardless of one's precision measurement capabilities. Without knowing the precise basis sent, an eavesdropper cannot obtain the sent bits. The number of bases N_σ within σ is

$$N_\sigma = \frac{2^{r+s}\sigma^2}{\pi^2} = \frac{2^{r+s}}{\pi^2\langle n\rangle}. \quad (8.7.4)$$

To warrant the security of the proposed scheme, N_σ should be a considerable number of adjacent bases. However, a larger N_σ will introduce more complexity for the scheme. Thus a proper N_σ is necessary for designing an optimal scheme.

The minimum probability of error for an eavesdropper can be made arbitrarily close to $\dfrac{1}{2}$ for a fixed average number of photons $|\alpha|^2$ with r and s increasing, where α is the amplitude of coherent states. However, the probability of error for the receiver is

$$P_e^{svr} = \frac{1}{2}(1 - \sqrt{1 - \exp(-2T|\alpha|^2)}), \quad (8.7.5)$$

where T is the transmissivity of the channel. For large $|\alpha|^2$, P_e^{svr} may be negligible since it approaches zero. In this situation, the received quantum signal can be recovered excellently by the legitimate receiver.

The above scheme has been experimentally implemented using the set-up illustrated in Fig.8.23. The quantum signal employed in this scheme is a mesoscopic coherent state (MCS) of light, which is created by a DFB laser. The generated quantum signal is modulated by changing the voltage of the polarization encoder (PE) controlled by the string k_1. The horizontal and vertical polarization states are encoded into bit 0 and bit 1, respectively, i.e., $0 \leftrightarrow |\Psi(0,0)\rangle$ and $1 \leftrightarrow |\Psi(\pi,\pi)\rangle$. Alice's controller 1 controls the dynamical polarization controller (DPC) 1, i.e., DPC1 to transform the encoded polarization states into arbitrary elliptical polarization states according to the pre-shared binary strings k_2 and k_3. After the quantum signal reaches Bob's side, the DPC2 transforms the elliptical polarization states into the original polarization states controlling by Bob's controller according to strings k_2 and k_3. There are two components in the output signal of DPC2, i.e., the horizontal or vertical polarization state, they are separated by the polarization beam splitter (PBS). Finally, the optical signal is detected by the PIN photodetectors D1 and D2 and the data are input into the controller 2.

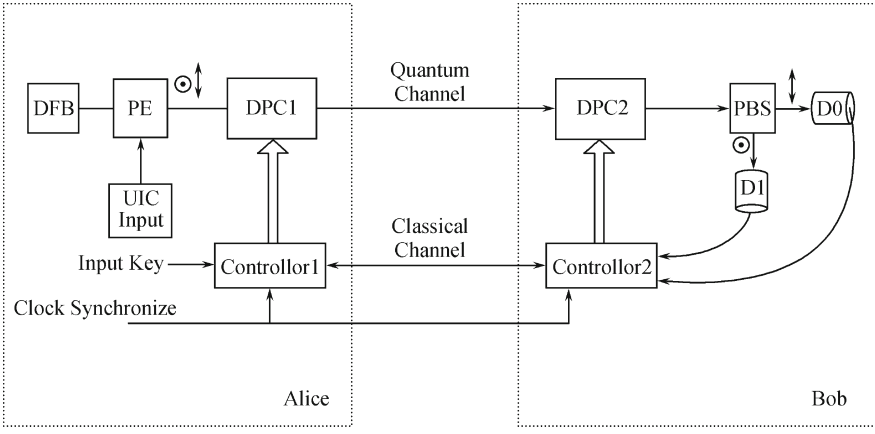

Fig. 8.23. Experimental implementation scheme for quantum identification system with coherent state

References

[1] Glauber R J (1963) Coherent and incoherent states of the radiation field. Physical Review, 131(6): 2766

[2] Walls D F, Milburn G J (1995) Quantum optics. Springer, New York

[3] Gazeau J P (2009) Coherent states in quantum physics. Wiley, New York

[4] Slusher R E, Hollberg L W, Mertz J C, et al (1985) Observation of squeezed states generated by four-wave mixing in an optical cavity. Physical Review Letters, 55(22): 2409 – 2412

[5] Keller G, D'Auria V, Treps N, et al (2002) Experimental demonstration of frequency-degenerate bright EPR beams with a self-phase-locked OPO. Optics Express, 16(13): 9351 – 9356

[6] Rosenbluh M, Shelby R M (1991) Squeezed optical solitons. Physical Review Letter, 66: 153 – 156

[7] Shannon C E (1948) A mathematical theory of communication. The Bell system Tech Journal, 27: 379 – 423; 623 – 656

[8] Takesue H, Nam S W, Zhang Q, Hadfield R H, et al (2007) Quantum key distribution over a 40dB channel loss using superconducting single photon detectors. Nature Photonics, 1: 343 – 348

[9] Hertz H (1887) Ueber einen einfluss des ultravioletten Lichtes auf die electrische entladung. Annalen der Physik, 267(8): 983 – 1000

[10] Einstein A (1905) Uber einen die erzeugung und verwandlung des lichtes betreffenden heuristischen gesichtspunkt. Annalen der Physik, 322(6): 132 – 148

[11] Agrawal G P (2002) Fiber-optic communications systems, 3rd edn. Wiley, New York

[12] Braunstein S L (1990) Homodyne statistics. Physical Review A, 42: 474 – 481

[13] Ou Z Y, Kimble H J (1995) Probability distribution of photoelectric currents in photodetection processes and its connection to the measurement of a quantum state. Physical Review A, 52: 3126 – 3146

[14] Vogel W, Grabow J (1993) Statistics of difference events in homodyne detection. Physical Review A, 47: 4227 – 4235

[15] Lu Y, Zeng G H, Yi Z (2008) Quantum homodyne detection based on polarization diversity technique. Chinese Physics Letter, 25(6): 1950 – 1953

[16] Grosshans F, Grangier P (2002) Continuous variable quantum cryptography using coherent states. ArXiv, 0109084

[17] Grosshans F, Assche G V, Wenger J, et al (2007) Quantum key distribution using gaussian-modulated coherent states. Nature, 421: 238 – 241 (2003)

[18] Takuya H, Yamanaka H, Ashikaga M, et al (2003) Quantum cryptography using pulsed homodyne detection. Physical Riview A, 68: 042331

[19] Takuya H, Shimoguchia A, Shirasakia K, et al (2006) Practical implementation of continuous-variable quantum key distribution. Proceedings of SPIE, 2006: 6244

[20] Thomas S, Alton D J, Assad S M, et al (2007) Experimental demonstration of post-selection-based continuous-variable quantum key distribution in the presence of Gaussian noise. Physical Review A, 76: 030303

[21] Korolkova N, Leuchs G, Loudon R, et al (2002) Polarization squeezing and continuous-variable polarization entanglement. Physical Review A, 65: 052306

[22] Jackson J D (1999) Classical Electrodynamics, 3rd edn. Wiley, New York

[23] Jauch J M, Rohrlich F (1959) The theory of photons and electrons. Addison-Wesley, London

[24] Agarwal G S, Chaturvedi S (2003) Scheme to measure quantum Stokes parameters and their fluctuations and correlations. Journal of Modern Optics, 50: 711 – 716

[25] Lorenz t, Korolkova N, Leuchs G (2004) Continuous-variable quantum key distribution using polarization encoding and post selection. Applied physic B, 79: 273 – 277

[26] Elser D, Bartley T, Heim B, et al (2009) Feasibility of free space quantum key distribution with coherent polarization states. New Journal of Physics, 11: 045014

[27] Borelli L F M, Vidiella-Barranco A (2006) Quantum key distribution using bright polarized coherent states. International Journal of Modern Physics B, 20: 1287

[28] Assche G V, Cardinal J, Cerf N J (2004) Reconciliation of a quantum-distributed gaussian key. IEEE Transactions on Informtion Theory, 50: 394

[29] Cerf N J, Ipe A, Rottenberg X (2000) Cloning of continuous quantum variables. Physical Review Letter, 85: 1754 – 1757

[30] Cerf N J, Iblisdir S (2000) Optimal N-to-M cloning of conjugate quantum variables. Physical Review A, 62: 040301

[31] Fuchs C A, Gisin N, Griffiths R B, et al (1997) Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strateg. Physical Review A, 56: 1163

[32] Lodewyck J, Debuisschert T, Brouri R T, et al (2005) Controlling excess noise in fiber-optics continuous-variable quantum key distribution. Physical Review A, 72: 050303

[33] Lodewyck J, Bloch M, Patron R G, et al (2007) Quantum key distribution over 25 km with an all-fiber continuous-variable system. Physical Review A, 76: 042305

[34] He G, Zhu J, Zeng G H (2006) Quantum secure communication using continuous variable EPR correlations. Physical Review A, 73: 012314

[35] Schneier B (1994) Applied Cryptography: protocols, algorithms, and source code in C. Wiley, New York

[36] Barbosa G A, Corndorf E, Kumar P, et al (2003) Secure communication using mesoscopic coherent states. Physical Review Letter, 90: 227901

[37] Corndorf E, Barbosa G, Liang C, et al (2003) High-speed data encryption over 25 km of fiber by two-mode coherent-state quantum cryptography. Optics Letters, 28(21): 2040 – 2042

[38] Corndorf E, Kanter G S, Liang C, et al (2004) Data encryption over an inline-amplified 200 km long WDM line using coherent-state quantum cryptography. Proceedings of the SPIE, 5436: 12 – 20

[39] Yuen H P (2004) KCQ: A new approach to quantum cryptography I. General principles and key generation, arXiv: 0311061

[40] Nishioka T, Hasegawaa T, Ishizukaa H, et al (2005) How much security does Y-00 protocol provide us? Physics Letters A, 327(1): 28 – 32

[41] Yuen H P, Kumar P, Corndorf E, et al (2005) Comment on: "How much security does Y-00 protocol provide us?" Physics Letters A, 346: 1 – 6

[42] Nishioka T, Hasegawaa T, Ishizukaa H, et al (2005) Reply to: "Comment on: "How much security does Y-00 protocol provide us?"". Physics Letters A, 346: 7 – 16

[43] Lo H K, Ko T M (2005) Some attacks on quantum-based cryptographic protocols. Quantum Information and Computation, 5(1): 40 – 47

[44] Yuen H P, Nair R, Corndorf E, et al (2005) On the security of $\alpha\eta$: response to 'some attacks on quantum-based cryptographic protocols'. Quantum Information and Computation, 6(7): 561 – 582.

[45] Yuan Z L, Shields A J (2005) Comment on "secure communication using mesoscopic coherent states". Physical Review Letter, 94: 048901

[46] Yuen H, Corndorf E, Barbosa G, et al (2005) Reply: "Comment on "Secure Communication using Mesoscopic Coherent States"". Physical Review Letter, 94: 048902

[47] He G Q, Zeng G H (2006) A secure identification system using coherent states, Chinese Physics, 15(2): 371 – 374

9 Practical Private Communication Systems

This chapter demonstrates the quantum private communication in practical communication systems. Four situations, including the fiber-based quantum private communication, free-space quantum private communication, quantum Internet networks, and applications of the quantum private communication in mobile communications, are described. Finally, problems and challenges for the practical quantum private communication are remarked.

Chapters 1 – 3 have presented a fundamental theory for the quantum private communication, which is built using quantum information theory, quantum complexity theory, and quantum secure theory. Then, typical approaches for protecting the confidentiality and authentication of secret information and private communication using quantum techniques are described in Chapter 4 – 6. After that, physical implementation ways of the quantum private communication with single photon signals or continuous variables signals are illustrated in Chapters 7 – 8. These theories, approaches, and techniques have built an integrated architecture for the quantum private communication. Subsequently, applications of the quantum private communication in practical communication systems becomes naturally an significant issue. This chapter focuses on this topic and four situations of the quantum private communication in practical applications are described.

9.1 Introduction

Aim of the classic private communication as well as the quantum private communication is to protect the confidentiality and authentication of transmitted message in a channel as described in previous chapters. With this aim, there are currently two ways for applying the quantum private communication in practical communication systems. One is the combination of quantum key distribution (QKD) schemes and classic cryptographic algorithms which is called QKD-based cryptosystem, and another way is to employ directly a suitable quantum cryptosystem, e.g., the quantum Vernam cipher, in the practical communication system. Like that in the classic private communication, the involved cryptosystems can be employed in both the confidentiality and authentication protections.

From viewpoint of the classic private communication [**?**], cryptography is a vital part of today's computer and communication networks, protecting everything from business e-mails to bank transactions and Internet shopping. Although modern algorithms such as the Advanced Encryption Standard (AES) are very hard to break without the key, this system suffers from an obvious weakness: the key must be known to both parties. Thus the problem of confidential communication reduces to that of how to distribute these keys securely so that the encrypted message itself can then safely be sent along a public channel. A common method is to use a trusted courier to transport the key from sender to receiver. However, any distribution method that relies on humans is vulnerable to the key being revealed voluntarily or under coercion. In contrast, QKD provides an automated method for distributing secret keys with ultra-secure using standard communication fibres or air channels. Furthermore, QKD allows the key to be changed frequently, reducing the threat of key theft or "cryptanalysis", whereby an eavesdropper analyses patterns in the encrypted messages in order to deduce the secret key. These features of QKD schemes make the QKD technique become naturally substitution of classic key distribution approaches. The combination of both classic cryptosystems and QKD motivates the QKD-based cryptosystem whose mechanism has been introduced in Chapter 5. Currently, this way has become a main way for applying in the practical secure communication systems.

Except for the QKD-based cryptosystem, exploiting directly a suitable quantum cryptosystem, e.g., the quantum Vernam cipher or quantum block cipher, in the practical communication system has also become possible if only simple quantum operations are involved in such algorithms. In this scenario, messages are directly encrypted and decrypted using quantum cryptographic algorithm with classic key or quantum key. A typical example is the quantum cryptosystem which makes use of a coherent state in a wave division multiple (WDM) telecommunication fiber network, proposed by the group in Northwest University in USA. The details of this algorithm has been introduced in the Section 8.6 [**?**].

The presented private communication approach in quantum ways may be applied in many modern communication systems. On the one hand, since the quantum communication is actually a special kind of optical communications, it can be applied in all situations where a classic optical communication system is suitable. For instance, the quantum private communication may be implemented in the well-known fibre telecommunication system. In this scenario, the point-to-point communication, point-to-multipoint communication, and multipoint-to-multipoint communication have been investigated [3 – 9]. In free-space optical communication systems, i.e., the wireless optical communication systems, the quantum private communication has been applied in the satellite-based optical communication system [10 – 19]. In addition, the combination of quantum cryptographic techniques and well-known Internet network has attached much attention [20 – 23]. On the other hand, since one may generate random number string which is very close to the true

random number, techniques of the quantum private communication have also been applied in some modern communication systems such as the well-known mobile communication system [**?**]. Of course, there still exist many problems and challenges for applications of the quantum private communication in practical communication systems. These topics needs to be investigated further.

Technically, to implement the quantum private communication in a practical communication system depends on matureness of technical implementations. From the first laboratory demonstrations over 30 cm of air in 1989 [**?**] to the first practical QKD system, a practical system with primitive function for application, manufactured by id quantique company [**?**], the quantum private communication has certainly come a long way in the last two decades. Fortunately, great progresses have been made in the recently years, and commercial applications of the private communication in quantum ways has become possible. With fiber-channel the latest fibre-based system has been operated over 200 km [**?**], and a latest system with air-channel transmitting 1485 km between space and Earth has been built [**?**]. While the combination of the quantum private communications and Internet networks has become practical gradually. In addition, the technology has shrunk into compact units the size of typical network equipment and is fully automated. All these implementations indicate that the quantum cryptography has become a reality although practical quantum computers will take many years to develop [**?**]. This implicates the quantum techniques have entered the industry, which motivates the commercial development of quantum private communication systems.

The commercial potential of the quantum cryptography has attracted private investment in several start-up companies in the US and Europe. The firm id Quantique [**?**], for example, spun out from pioneering research at the University of Geneva. While in the US, commercial developments are led by MagiQ Technologies, based in New York and Massachusetts [**?**]. Recently a third start-up called SmartQuantum has been established in Brittany, France [**?**], and major corporate players such as HP, IBM, Mitsubishi, NEC, NTT, and Toshiba all have active quantum-cryptography programmes. With several quantum-cryptography products already on the market, the quantum information industry has arrived. At Toshiba, researchers have developed a "link encrypter" that can send data at 1 Gbit/s between corporate sites, combining the AES data encryption with secure key distribution using one-way QKD. Meanwhile, id Quantique announced that it will install its "Vectis" link encrypter between two centers of data-hosting company IX Europe in Zurich. In the US, MagiQ Technologies has recently developed its own encrypted link, targeted at government applications including the military, intelligence gathering, and homeland security. In China, a testbed of the quantum private communication for guaranteing security of the next generation Internet network has been building.

9.2 Transmission Loss

The transmission mechanism of quantum signals has been described in Sections 7.2 and 8.2. Due to the decoherence in the transmission channel and measurement channel, transmission losses exist inevitably. This is an important effect for the quantum private communication in practical applications. This section describes the transmission loss in practical single mode fiber and atmosphere.

9.2.1 In Single Mode Fiber

Optical fibers are widely used in the fiber-optic communication, which permits transmission over longer distances and at higher data rates than other forms of communications. The light beam is kept in the "core" of the optical fiber by total internal reflection. This causes the fiber to act as a waveguide. Fibers which support many transverse modes are called multi-mode fibers, and which can only support a single mode are called single-mode fibers. Multimode fibers are generally used for short-distance communication links and for applications where high power must be transmitted. Because the core of multimode fibers is usually 50 μm in diameter, there are many bound modes existing which leads to a non-isolated environment for transmission of qubits. Hence multimode fibers are not appropriate as quantum channels. However, a single mode fiber is well suited to carry quantum signal, since its core is so small, normally 8 μm, that only one single spatial mode is guided. Single photons can be transmitted for a very long distance in a standard optic fiber before losses dominate. Over the past years, a lot of effort has been made to reduce transmission losses. Nowadays, the attenuation is as low as 2 dB/km at 800 nm wavelength, 0.35 dB/km at 1310 nm, and 0.2 dB/km at 1550 nm. Modern telecommunication is based on wavelength around 1310 nm and around 1550 nm. Fig.9.1 shows the transmission loss versus wavelength in optical fibers.

Although a single-mode fiber with perfect cylindric symmetry could be a perfect quantum channel in an ideal world, all real fibers, however, suffer from asymmetries, the dispersion characteristics of which cause the shape of the transmitted pulse to spread as it travels along the fiber and generates an intrinsic error rate. A typical single mode optical fiber has a core diameter between 8 μm and 10 μm and a cladding diameter of 125 μm. There are a number of special types of single mode optical fiber which have been chemically or physically altered to give special properties, such as dispersion-shifted fiber and nonzero dispersion-shifted fiber. Data rates are limited by the polarization mode dispersion and chromatic dispersion.

Consider that the typical effects in the single mode fiber are the chromatic dispersion, birefringence, polarization mode dispersion, and polarization

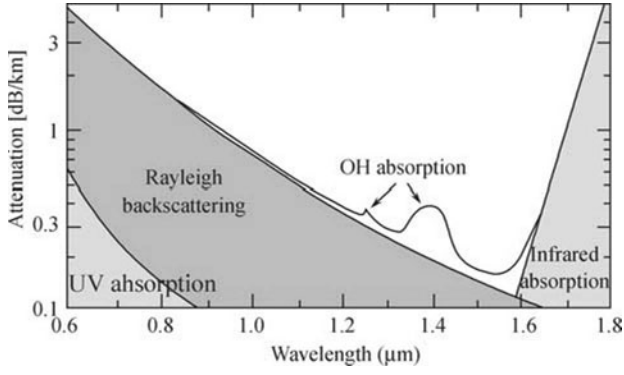

Fig. 9.1. Transmission losses versus wavelength in optical fibers

dependent loss, details regarding on these effects are described in follows.

1) Chromatic Dispersion

Generally, chromatic dispersion in a fiber is partly due to material dispersion, the dependence of the fiber core index of refraction on the wavelength, and to waveguide dispersion, the dependence of the constant propagation mode on the wavelength [**?**]. For single mode fibers that transmit qubits at 1550 nm, the amount of chromatic dispersions is given by

$$d_{\mathrm{CD}} \simeq 4 \text{ ps} \cdot (\text{nm} \cdot \text{km})^{-1}. \tag{9.2.1}$$

Assuming a laser source with a line width of 0.8 nm, the corresponding chromatic dispersion pulse delay time for a cable link of $L = 50$ km is given by

$$\tau_{\mathrm{CD}} = d_{\mathrm{CD}} \cdot L \cdot \Delta\lambda \simeq 160 \text{ ps}. \tag{9.2.2}$$

Fig.9.2 demonstrates a typical chromatic dispersion curve for a plasma activated chemical vapor deposition (PCVD) single mode fiber. In a case of an interferometry-based quantum private communication system, especially the interferometry-based QKD system which has been described in Chapters 7 and 8, one should compare the dispersion delay time with the coherence time τ_{COH} of the employed quantum signal and the reciprocal of the pulse repetition frequency $1/\tau$, associated with the data source laser. Assume that the source has a coherence time of at least 1 ns, then one gets

$$\tau_{\mathrm{CD}} < \tau_{\mathrm{COH}},$$

which means chromatic dispersion does not influence the quantum private communication. However, if

$$\tau_{\mathrm{CD}} > \tau_{\mathrm{COH}},$$

which means one uses a fast data source with a bit period shorter than 160 ps, the chromatic dispersion must be mitigated. Fortunately, in case of faint laser

pulses where the line width is typically less than 1 nm, chromatic dispersion is not a serious issue. And since the chromatic dispersion of optical fibers does not change with time, online tracking and compensation is not required. It thus turns out that qubits of phase coding in optical fiber is particularly suited to transmission over long distances.

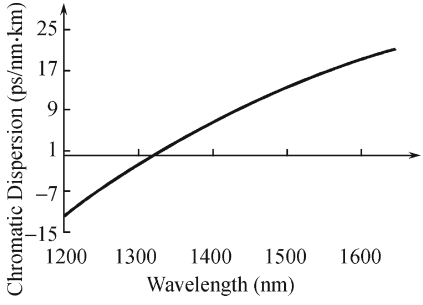

Fig. 9.2. Typical chromatic dispersion curve for a PCVD single mode fiber

2) Birefringence

The birefringence is the presence of two different phase velocities for two orthogonal polarization states. It is caused mainly by elliptical core deformation and stress anisotropy [**?**]. Nowadays, the birefringence is small enough for the telecom industry, but for quantum communication, any birefringence, even extremely small, will always remain a concern. Even in a phase-coding system, the visibility of interference depends on polarizations of two beams. When the polarized waves are employed for optical fiber transmissions, the polarization planes may suffer from rotation. Propagation constant variation due to dielectric constant perturbation $\delta\varepsilon$ is given by the following equation,

$$\delta\beta = \frac{\omega}{2} \cdot \frac{\int \delta\varepsilon \cdot \hat{E} \cdot \hat{E}^* \cdot dS}{\int \mathrm{Re}(\hat{E} \times \hat{H}) z_0 \mathrm{d}S}, \tag{9.2.3}$$

where $\hat{E}$ and $\hat{H}$ are the unperturbed electric field and its conjugate, z_0 is the unit vector in the direction of the wave propagation, and ω is optical angular frequency. The integration is over an infinite surface perpendicular to the waveguide. A circular core step-index fiber is chosen as an unperturbed waveguide. If there is elliptical core deformation, and if there is also a stress anisotropy between the principal axes of the ellipse, the perturbation $\delta\varepsilon$ is expressed as

$$\delta\varepsilon = \begin{pmatrix} \delta\varepsilon_x & 0 & 0 \\ 0 & \delta\varepsilon_y & 0 \\ 0 & 0 & 0 \end{pmatrix}. \tag{9.2.4}$$

Consider only $\delta\varepsilon_x$ for the moment since $\delta\varepsilon_y$ is calculated in the same way. The perturbation can be divided into three terms by the origin,

$$\delta\varepsilon_x = \delta\varepsilon_e + \delta\varepsilon_{1s} + \delta\varepsilon_{2s}, \tag{9.2.5}$$

where $\delta\varepsilon_e$ is the perturbation caused by elliptical core deformation, and $\delta\varepsilon_{1s}$ and $\delta\varepsilon_{2s}$ are the perturbations caused by stress in the core and cladding, respectively. Then the value $\delta\beta$ is finally simplified as

$$\delta\beta = G(v)\, nk_0\Delta^2\ell + nk_0\left(\delta\varepsilon_y - \delta\varepsilon_x\right)/(2\varepsilon), \tag{9.2.6}$$

where $G(v)$ indicates the normalized frequency dependence of the coupling efficiency caused by an elliptical core deformation, n is core refractive index, k_0 is the wavenumber in vacuum, and ℓ is the ellipticity of the core. The first term expresses the effect of elliptical core deformation and the second term expresses the photo elastic effect. If this rotation is stable, which needs slow thermal and mechanical variations, The communicators Alice and Bob can compensate for it. Another type of specially made fibers called polarization-maintaining fibers is utilized highly birefringent for transmission of two polarization eigenmodes. This type of fibers is very helpful when phase-coding systems are used. But note that only two orthogonal modes are maintained means that if the polarization of the input light is not aligned with the stress direction in the fiber, the output will vary between linear and circular polarization, and generally will be elliptically polarized. The exact polarization will then be sensitive to variations in temperature and stress in the fiber. Polarization-maintaining fibers are rarely used for the long-distance transmission, because they are expensive and have higher attenuation than single-mode fiber.

3) Polarization Mode Dispersion

Polarization mode dispersion is a form of modal dispersion where two different polarizations of light in a waveguide, which normally travel at the same speed, travel at different speeds due to random imperfections and asymmetries, causing random spreading of optical pulses. Unless it is compensated, which is difficult, this ultimately limits the rate at which data can be transmitted over a fiber. In an ideal optical fiber, the core has a perfectly circular cross-section. In this case, the fundamental mode has two orthogonal polarizations (orientations of the electric field) that travel at the same speed. The signal that is transmitted over the fiber is randomly polarized, for example a random superposition of these two polarizations, but that would not matter in an ideal fiber because the two polarizations would propagate identically. In a realistic fiber, however, there are random imperfections that break the circular symmetry, causing the two polarizations to propagate with different speeds [**?**]. The symmetry-breaking random imperfections fall into several categories. First, there is geometric asymmetry, slightly elliptical cores. Second, there are stress-induced material birefringence, in which the refractive

index itself depends on the polarization. Both of these effects can stem from either imperfections in manufacturing (which is never perfect or stress-free) or from thermal and mechanical stresses imposed on the fiber in the field, which generally could be controlled to vary over time. In this case, the two polarization components of a signal will slowly separate, causing pulses to spread and overlap. Fig.9.3 shows this problem. Because the imperfections are random, the pulse spreading effects correspond to a random walk, and thus have a mean polarization-dependent time-differential τ_{PMD} (also called the Differential Group Delay) proportional to the square root of propagation distance L,

$$\tau_{\mathrm{PMD}} = d_{\mathrm{PMD}}\sqrt{L}, \tag{9.2.7}$$

where d_{PMD} is the polarization mode dispersion parameter of the fiber, typically measured in $\mathrm{ps}\cdot\mathrm{km}^{-1/2}$. In currently available single mode fiber operating at 1550 nm, d_{PMD} is typically given by

$$d_{\mathrm{PMD}} \simeq 0.1\ \mathrm{ps}\cdot(\mathrm{km})^{-\frac{1}{2}}. \tag{9.2.8}$$

Subsequently, given a cable link of $L = 50$ km, the polarization-dependent time-differential,

$$\tau_{\mathrm{PMD}} = d_{\mathrm{PMD}}\sqrt{L} \simeq 0.7\ \mathrm{ps}. \tag{9.2.9}$$

Again assuming a laser coherence time of 1 ns, this polarization arrival time dispersion strongly satisfies the requirement

$$\tau_{\mathrm{PMD}} < \tau_{\mathrm{COH}}. \tag{9.2.10}$$

Furthermore, the requirement

$$\tau_{\mathrm{PMD}} < \tau$$

could also be satisfied easily unless the pulse repetition rate is greater than 1.43 THz. Thus polarization-mode dispersion in quantum private communication will not be a practical problem.

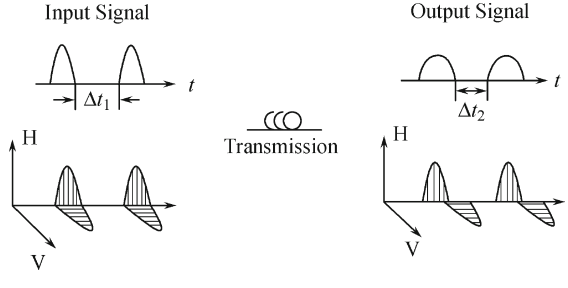

Fig. 9.3. Pulse spreading and overlapping due to polarization mode dispersion

4) Polarization Dependent Loss

Since a single-mode fiber actually supports two polarization modes, its attenuation also depends on the polarization of the propagating signal. Such an effect is called the polarization dependent loss, which is extremely negligible for standard telecom fibers. However, components like couplers, phase modulators and switches are known to be affected by polarization dependent losses. In particular, some integrated optic waveguides actually guide only one mode and thus behave almost like polarizers, e.g., $LiNbO_3$ phase modulators. When several of these elements are combined, such as in a QKD system where two $LiNbO_3$ phase modulators are used, the polarization dependent loss will affect the system performance. In this situation, the global attenuation is generally not the sum of the attenuation of the elements. Indeed, the first phase modulator will partially polarize qubits, hence the attenuation of the second phase modulator depends on the relative orientation of the two phase modulators and on the polarization rotation produced by the connecting standard fiber. This example also illustrates the fact that the relation between the polarization state and polarization dependent losses may fluctuate, producing random outcomes [**?**]. Hence, in almost all quantum private communication systems, the polarization state of qubits should be well tracked and passively compensated.

9.2.2 In Free Space

The free space optical communication is a technology that uses light signal propagating in free space to transmit information between two points. Historically, the free space optical communication was originated from several thousand years ago. The invention of laser in the 1960s, revolutionized the modern free space optical communications. Military organizations were particularly interested and boosted development in this direction. Although communication based on optical fiber is very popular today, the physical connection by the means of fiber optical cables may be impractical in some special situations, such as the communication in outer space, in water and the communication bestriding a canyon as mentioned in Chapter 1. Accordingly, investigations on the free space optical communication have been reactivated in recent years. In a manner similar to fiber optical communications, the free space optics uses laser source for transmission. However, in the free space optics, signals are collimated and transmitted through the space rather than being guided through an optical cable. These signals, operating in the Tera-Hertz portion of the spectrum, are focused on a receiving lens connected to a high sensitivity receiver.

The quantum private communication in a free space is a special case of the free-space optical communications. Recently, it has attracted much attention since it may be extended to the space optical communication which plays an

important role in military. Compare to the classic one, the quantum free space optical communication is the same except for the generations and detections of qubits. Especially, signal transmission ways are the same for both the quantum and classic free-space optical communication.

Transmission over free space has some advantages as follows. Unlike radio and microwave systems, the free space optical communication requires no spectrum licensing, and interference to and from other systems is not a concern. The point-to-point laser signal is extremely difficult to intercept, making it ideal for covert communications which called full-duplex and very secure due to the high directionality and narrowness of the beam. In addition, the free space optical communication offers data rates comparable to fiber optical communications at a fraction of the deployment cost while extremely narrow laser beam widths provide no limit to the number of free space optical links that may be installed in a given location. The atmosphere has a high transmission window at a wavelength of around 770 nm, which is perfect for single photon detection with Si avalanche photodiodes (APDs). Fig.9.4 shows the atmospheric transmission loss versus wavelength.

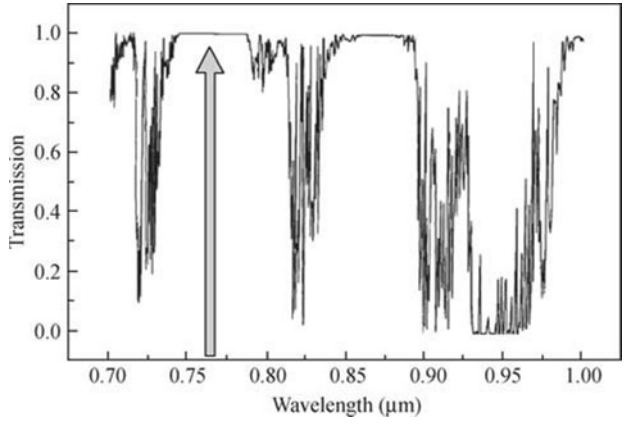

Fig. 9.4. Atmospheric transmission losses versus wavelength

Furthermore, the atmosphere is only weakly dispersive and essentially non-birefringent at these wavelengths, since air is not subject to stress. Hence, it will thus not change the polarization state of single photons. However, the fundamental limitation of free space optical communications arises from the environment through which it propagates. Free space optical communication systems can be severely affected by fog and atmospheric turbulence. The main design challenges in free space optical communications are as follows: static atmospheric losses due to atmospheric scattering and absorption, beam spreading, beam wander, and scintillation. Other disadvantages such as turbulence-induced coherence loss, pulse distortion and thermal blooming are not mentioned here as these are negligible using quantum signal, e.g.,

single photon signal, in the quantum private communication.

1) Static Atmospheric Losses

Even in the absence of any turbulence at all, the atmosphere would still induce a variety of scattering and absorptions of beam pulses, leading to a decreasing in the received signal intensity at the receiver Bob [**?**]. Rain, and even light drizzle, will severely attenuate the beam to the extent that in many cases useful signal cannot be transmitted at all. Moreover, fog is vapor composed of water droplets, which are only a few hundred microns in diameter but can modify light characteristics or completely hinder the passage of light through a combination of absorption, scattering, and reflection. This can lead to a decrease in the power density of the transmitted beam, decreasing the effective distance of a free space optical link. However, the static atmospheric attenuation effectively disappears when the two ends of the link are located at elevations of 10 km and 300 km, respectively. Hence, the free space optical communication in quantum ways is more suitable for the satellite-ground (or possibly an stratosphere platform) system demonstrated in Section 9.4.

2) Beam Spreading

The beam that transmitted from Alice to Bob becomes a spread beam due to divergence. According to standard results in a turbulence research [**?**], the mean squared value of the beam spread radius ρ_s is composed of two parts which are influenced by vacuum geometrical effect and turbulence effect individually, respectively, i.e.,

$$\left\langle \rho_s^2 \right\rangle = \rho_d^2 + \frac{4L^2}{\left(\kappa\rho_0\right)^2}\left[1 - 0.62\left(\frac{\rho_0}{D_{\mathrm{A}}}\right)^{\frac{1}{3}}\right]^{\frac{6}{5}}, \tag{9.2.11}$$

where κ is the wavenumber, L is the path length over which the signal propagate, and D_{A} is the diameter of aperture of the sender's transmitting instrument. Then the total beam spread loss is given by

$$L_{BS} = 10\log_{10}\left(\frac{D_{\mathrm{B}^2}}{4\left\langle \rho_s^2 \right\rangle}\right), \tag{9.2.12}$$

where D_{B} is the diameter of the receiver's receiving instrument. When the area of receiver's receiving instrument is less than the effective area of the fully spread beam, the expression gives a negative value. For example, using 20 cm diameter optics, the spot size after 300 km is about 1 m. This means that for the case in which a free space quantum private communication channel is utilized, such as for a QKD system between a satellite and a ground station, it is advantageous to increase the size of the receiver's receiving instrument aperture compared to the sender's.

3) Beam Wander

The beam wander arises when turbulent wind current (eddies) larger than the diameter of the transmitted optical beam. This effect causes a slow, but

significant, displacement of the transmitted beam. The beam wander may also be the result of seismic activity that causes a relative displacement between the position of the transmitting laser and the receiving photon detector. In addition, a turbulent medium could also lead to arrival-time jitter. Fortunately, the atmospheric turbulence varies around 0.1 to 0.01 s. Hence these errors can be mitigated by sending a reference pulse at a different wavelength around 50 ns before each signal pulse. Since the signal pulse experiences the same atmospheric condition right after the reference one, the signal pulse will arrive exactly with no jitter in the time-window triggered by reference pulse. And by employ fast steering mirrors that scan and reflect back the incoming tracking beam to Alice, the direction of the laser beam could also be corrected. Existing engineered devices that apply active closed-loop feedback control between Alice and Bob are available to generate in excess of 30 dB rejection of the beam wander [**?**]. Therefore, it is possible to construct a quantum private communication system in which the beam wander loss is effectively eliminated.

4) Scintillation

The scintillation is the temporal and spatial variation in light intensity caused by atmospheric turbulence. Such a turbulence is caused by wind and temperature gradients that create pockets of air with rapidly varying densities and, therefore, fast-changing indices of optical reflection. These air pockets act like lenses with time-varying properties and can lead to sharp increases in the bit-error-rates of free space optical communication systems, particularly in the presence of direct sunlight. Scintillation effects are always much more pronounced near the horizon than near the zenith. Parcels of the order of only centimeters to decimeters are believed to produce most of the scintillatory irregularities in the atmosphere. Scintillation effects are reduced by using a larger receiver aperture. This effect is known as aperture averaging.

9.3 Private Communication Over Fiber

As well-known, the fiber-based telecommunication optical communication is an important way for the modern communication. Since the quantum communication is actually a special optical communication at an extreme condition, i.e., at the condition of using very weak optical signal or even single photon signal as signal source, the fiber-based quantum private communication is naturally regarded as a main way for the quantum optical communication. As introduced in Chapters 7 and 8, the fiber-based quantum communication has been implemented experimentally with single photon signal or continuous variable signals. These techniques have paved the road for building practical fiber-based quantum private communication system.

In classic optical communication systems, there are three kinds of com-

munication ways from the viewpoint of physical transmissions. These include the point-to-point (P2P) communication, point-to-multipoint communication, and multipoint-to-multipoint communication. These communication ways may be implemented also in quantum technologies. Correspondingly, there are three kinds of fiber-based quantum private communication ways. This section introduces firstly the P2P quantum private communication system, and then discusses the passive optical network system which consists of P2P communications and point-to-multipoint communications. These technologies lead the possibility of toward global fiber communication systems.

9.3.1 Point-to-point Private Communication

Currently, the quantum private communication is implemented in practical communication systems using QKD-based classic cryptosystems or classic-key-based quantum cryptosystem to guarantee the confidentiality and authentication of transmitted messages. Especially, the QKD-based cryptosystem has been widespread applied in the experimental research and product manufacture for secure communications in quantum ways. Two steps are involved in this kind of cryptosystems. The first step generates and distributes a symmetrical key pair using QKD schemes, then a classic algorithm, such as AES or classic Vernam cipher, is employed to encrypt the message with the obtained keys. Clearly, how to generate the secret keys plays important role for the P2P quantum private communication. Thus, this subsection focuses on how to distribute secure keys using practical P2P fiber-based QKD techniques.

In principle, the so-called P2P fiber-based QKD exploits fundamentals of quantum physics to build a secure and available key generation and distribution system through a fiber communication link so that the confidentiality and authentication of private messages can be guaranteed with a suitable QKD-based cryptosystem. The employed communication link is a directly physical connection using telecommunication fibers. In such communication, the adopted quantum signal, e.g., the single photon signal, faint laser pulse signal, coherent state quantum signal, or squeeze state quantum signal, are transmitted directly from one station to another without any router connection. The main fiber-based replacement architecture is shown in stylized form in Fig.9.5. In this figure, the symbols Rx and Tx denote the transmitter and receiver, respectively. The two links represent the communication is a two-way communication. In the optical fiber communication, the link from Alice to Bob is called a downstream communication, and the vice versa is called upstream communication. Apparently, the P2P communication is a simplest way, but it is an important component in modern communications.

In the quantum communication, information should be encoded in quantum states of the involved quantum signal. Several different ways have been

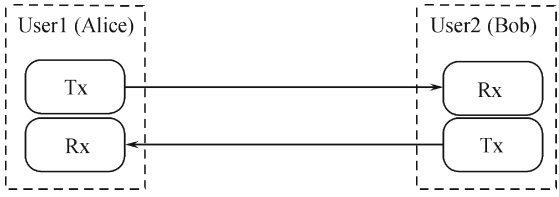

Fig. 9.5. Point-to-point architecture with transmitters (Tx) and receivers (Rx) at each point

involved which have been described in Chapters 7 and 8. The first laboratory demonstration of QKD by Bennett and Brassard in 1989 over 30 cm of air used the polarization state of photons. However, transmitting photons along an optical fibre can randomize their polarization, so a better approach pioneered by Paul Townsend, formerly of BT Labs in the UK, is to alter the phase of photons. In this method, laser pulses with quantum attributes are injected into an interferometer. By applying different voltages to a "phase modulator" in one arm of the interferometer, Alice can encode bits as a phase difference between the two emergent pulses sent to Bob. Then Bob passes the pulses through another interferometer and determines which of his two detectors, corresponding to "0" and "1", they emerge at. To make this scheme work, one must keep relative lengths of interfering paths in Alice's and Bob's interferometers stable to a few tens of nanometres. However, temperature changes of just a fraction of a degree are enough to upset this balance. An ingenious solution to this problem was introduced by the Geneva group in 1997, which led to the first QKD system suitable for use outside the laboratory. The idea is to send the laser pulses on a round trip from Bob to Alice and then back to Bob so that any changes in the relative arm lengths are canceled out. This is the so-called two-way QKD, which has been discussed in Chapter 7. At the Toshiba lab in Cambridge, the researchers have developed an alternative compensation technique that allows pulses to be sent just one way, by sending an unmodulated reference pulse along with each signal pulse. These reference pulses are used as a feedback signal to a device that physically stretches the fibre in one of the two arms of the interferometer to compensate for any temperature-induced changes. In trials with the network operator Verizon, the one-way QKD system was continuously operated for over a month without requiring any manual adjustment. The principles have been presented in Chapters 7 and 8.

To reach the level of practical application, two ingredients, i.e., the secure key rate and transmission distance, are very important. Currently, many investigations regarding on the fiber-based QKD have focused on extending the achievable transmission distance on P2P links and improving the secure key rate in such links.

In practical applications, the secure key rate that can be achieved decreases with the length of the optical link due to the scattering of pho-

tons from the fibre, the influence of noise and the channel lossy. For these reasons, the best performance is usually achieved using photons with a wavelength of 1550 nm, at which standard optical fibre is most transparent. Even so, when the fibres get so long that the signal rate becomes comparable to the rate of false counts in the receiver's detectors, sending a secure key is no longer possible. For example, when the transmission distance has reached beyond 100 km using faint laser pulse as quantum signals, the key bit rate is only several bits per second. This is clearly no meaningfulness for the practical P2P quantum private communication. However, typical secure key rates for complete QKD systems for a 20 km fibre link are in the range of from 10 to 50 kbit/s or at the level of 1 Mbit using faint laser pulse or coherence state laser pulse as quantum signal, respectively. Although these may seem low compared with the rate data are transferred in optical communications (typically from 1 to 40 Gbit/s), it is enough for up to 200 AES encryption keys (each of which comprises 256 bits) to be sent per second. Actually, it is sufficient for most cryptographic applications. Of course, to use practically the one-time pad one needs a higher level of the key-bit rate.

Regarding on the transmission distance, a P2P quantum private communication system which uses the differential phase shift (DPS) QKD techniques is here demonstrated. Fig.9.6 shows the configuration of the DPS-QKD system [**?**]. A continuous wave output from a 1557.40 nm wavelength laser is transformed into a 10 GHz clock pulse train by an InGaAsP electro-absorption modulator. The pulses are generated with a full width at half

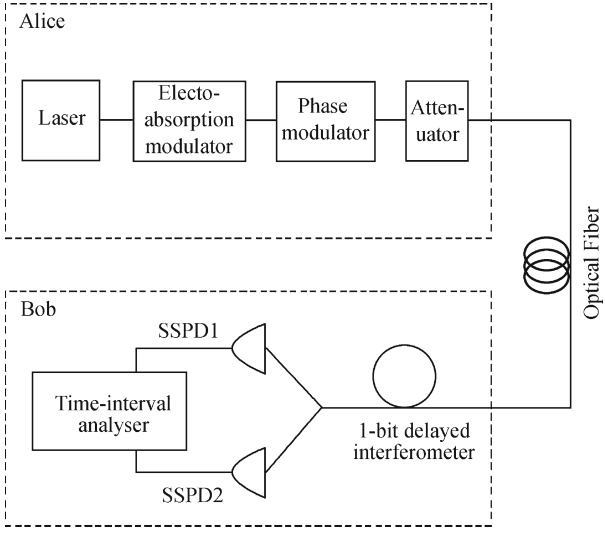

Fig. 9.6. Experimental set-up for P2P QKD with 10 GHz clock

maximum (FWHM) of 15 ps. The phase of each pulse was modulated by a phase modulator driven by a 10 GHz pseudorandom bit pattern from a

high-speed pulse pattern generator. The average photon number per pulse was adjusted to 0.2 by an optical attenuator. The quantum channel was a dispersion-shifted fibre or a single attenuator. Bob was equipped with a 1-bit delayed interferometer fabricated using planar lightwave circuit technology. The excess loss of the interferometer was 2.5 dB. Each output port of the interferometer was connected to superconducting single photon detectors (SSPD). The photon detection time instances and which-detector informations were recorded using a time-interval analyser in the experiment. This system used the DPS-QKD protocol and implemented with a 10 GHz clock frequency and SSPD based on NbN nanowires. The SSPD offers a very low dark count rate (a few Hz) and small timing jitter (60 ps, FWHM). The keys generated in this experiment are secure against both general collective attacks on individual photons and a specific collective attack on multiphotons, known as a sequential unambiguous state discrimination (USD) attack. The employment of SSPD allows to achieve a 12.1 bit/s secure key rate over 200 km of fibre. At 105 km, the secure key rate is 17 kbit/s. The maximum channel loss for the secure key generation is 42.1 dB, which almost doubled the maximum secure key distribution distance of previous terrestrial QKD experiments over optical fibre. One should note that the channel loss does not include the loss of the planar-lightwave-circuit interferometer. Fig.9.7 demonstrates the secure key rate as a function of fibre length.

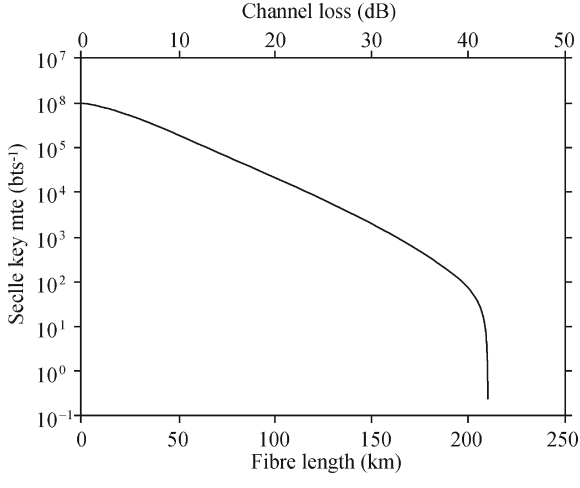

Fig. 9.7. Secure key rate as a function of fibre length with 0.2 dB/km loss and channel loss

The basic principle of the P2P fiber quantum private communication has been discussed in above. This kind of communication system can be applied in two practical scenarios. One is the direct communication between two parties, i.e., the direct communication through a link. The other is applied as

a basic component of a communication network where many such links are adopted. Since the transmission distance for the P2P fiber quantum private communication has reached 200 km in currently experimental techniques and the available length has reached at least 100 km, the P2P quantum private communication techniques make the application in metropolitan-area-sized networks become possible. Clearly, the P2P quantum private communications are important in practices not only for the P2P communication itself but also for constructing fiber optical network which will be discussed in the later.

In the above, the P2P quantum private communication with the QKD-based cryptosystem over fiber has been addressed. Investigation demonstrates that the P2P quantum private communication with the classic-key-based quantum cryptosystem has also become possible. In this case, a classic key or a seed key with linear feedback shift-register (LFSR) is employed directly for a quantum symmetrical key algorithm, and there are no limitations on the secure key rate for key generation since the key are generated using classic ways. Subsequently, such kind of P2P quantum private communications may be implemented in a long distance, e.g., 100 km or even longer, with high transmission rate, e.g., 650 Mbit/s [**?**]. Of course, such kind of systems can not reach the so-called unconditional security but a quasisecure which relies on some physical parameters. By controlling these parameters communicators may choose the demanded security level in practical application. The principles of this system have been presented in Chapter 8.

9.3.2 Private Communication Network

The above has introduced the P2P quantum private communication exemplified with the P2P fiber QKD system and the classic-key-based quantum cryptosystem system. Since most popular communications are implemented in networks, natural extension is to develop the quantum private communication from simple point-to-point links to "quantum private network" or called "quantum secure network". It is stressed that the quantum network mentioned here only means the fiber-based telecommunication optical communication network. This is different from the so-called quantum network which is actually a graphic state [**?**]. With constructed quantum secure networks, multiple nodes in the networks may be connected securely each other. Moreover, they allow the range of QKD to be increased from the length of a single fibre link to any distance covered by the network, and safeguard against outages of individual links by automatically routing traffic around them. Surely, the quantum repeater is necessary for distant transmissions.

There are three kinds of communication modes, i.e., the P2P communication, point-to-multipoint communication, and multipoint-to-multipoint communication. All these modes or their admixtures may be employed to build a quantum network. The architectures for these communication networks are

shown in stylized form in Fig.9.8. For simplicity, only the downstream part

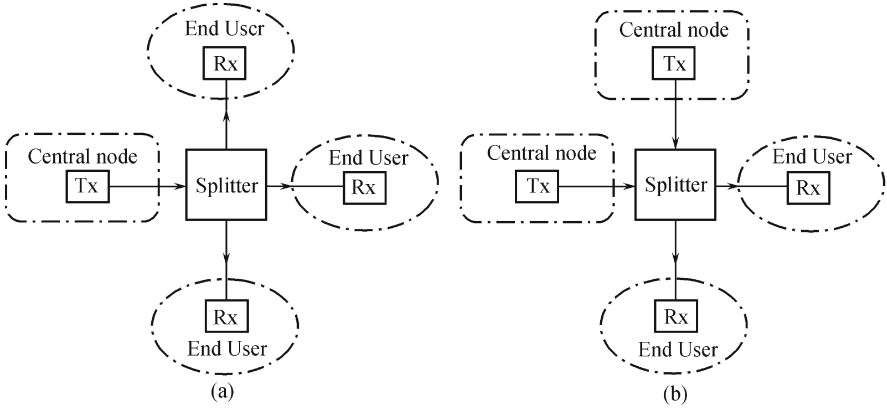

Fig. 9.8. Network architecture with transmitters (Tx) and receivers (Rx) at each point

(a) Point-to-multipoint network architecture (b) multipoint-to-multipoint network architecture.

of the network is shown with the transmitter (Tx) at the central node and the receivers (Rx) at the end-user locations. However, in practice each end-user would also contain a transmitter to enable upstream communication to a receiver in the central node. The WDM is usually employed to allow the two channels to share the same fiber without interference, with the upstream channel typically operating in the wavelength band around 1300 nm and the downstream channel (or channels) operating in the wavelength band around 1500 nm. In Fig.9.8, only the single "star" type network topologies have been drawn, but other architectures with, for example, distributed splitters in "tree-" or "bus-" type configurations are also possible.

Making use of three communication modes mentioned in the above, one may construct various practical fiber-based quantum private communication networks. Generally, four typical network topologies illustrated in Fig.9.9 have been involved, and their performances are compared in the Ref.[**?**]. They may be employed dependently in practices or as basic components for constructing a larger communication network.

The topology of the passive-star QKD network is shown in Fig.9.9(a). Such network was first demonstrated by Townsend and coworkers to connect four users over 5.4 km of optical fiber using faint laser pulses as the quantum signal [**?**]. Essentially, this topology is an extension of the two-user system, with Alice linked to multi-receivers through a $1 \times N$ splitter. Alice is equipped with a pulsed laser source (PLS). The emitted laser pulses are reduced by a tunable attenuator (TA) to generate faint laser pulses which is transmitted into a $1 \times N$ splitter, and the received faint laser pulses are detected finally

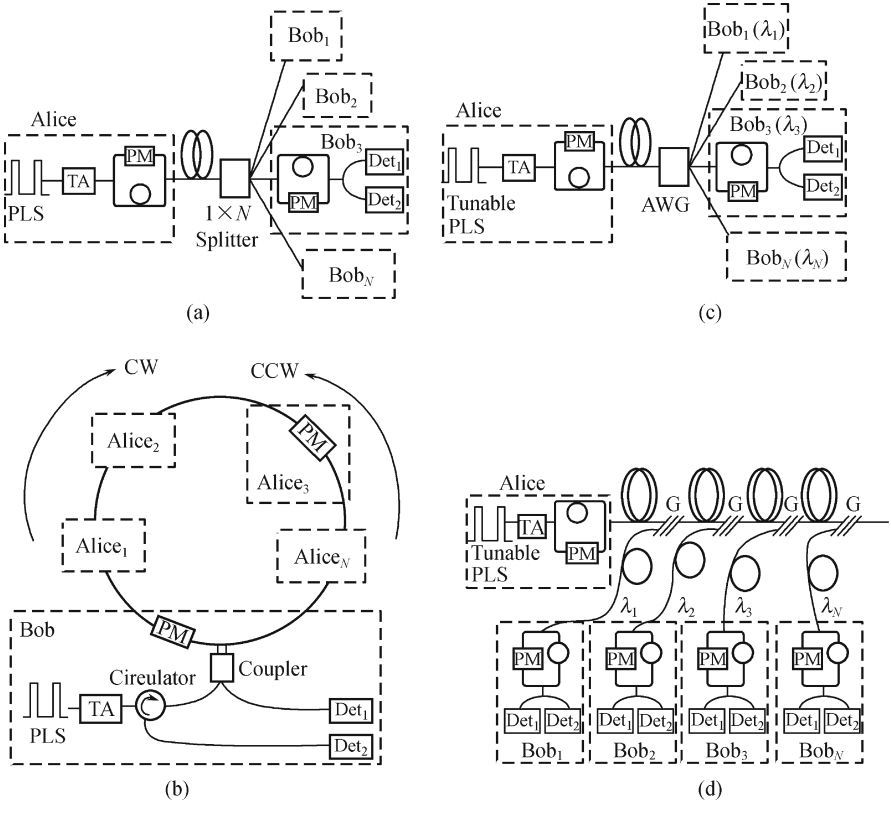

Fig. 9.9. Four typical topologies for quantum private network

by the detectors. The splitter may be substituted using WDM or arrayed waveguide grating (AWG). Due to the indivisible nature of the photon, each photon is randomly routed to a single user by the $1 \times N$ splitter. This topology can be easily implemented but suffers from the effective loss induced by the $1 \times N$ splitter, which reduces the probability of photons reaching the detectors of any particular user. This reduction scales inversely as the number of users on the network. Although this drawback can be partially mitigated by higher initial qubit rates, the routing of photons to each user is inherently nondeterministic. This nondeterministic detection rate will constrain the design of secure quantum networks by limiting the amount of information that can be securely encrypted. Of course, one may use continuous variable signals such as the coherent state signal to solve this problem, however, the involved local oscillator signal in such scenario results in a more complicated topology.

An optical-ring network topology is plotted in Fig.9.9(b). This topology uses the Sagnac interferometer to substitute the unbalanced Mach-Zehnder Interferometer (MZI). The Sagnac interferometer has the advantage of

being free from thermal fluctuations since the counterpropagating pulses pass through the exact same fiber paths inside the loop. A two-user QKD system based on the optical fiber Sagnac interferometer has been demonstrated by Nishioka and coworkers [**?**]. In this topology, the single photon pulse enters the Sagnac interferometer through an optical circulator. This pulse splits into two in the 50/50 coupler, and each travels around the Sagnac loop in clockwise (CW) and counterclockwise (CCW) directions, respectively. Any user on the loop that is communicating with Bob modulates the pulse traveling in the CW direction. While Bob modulates the pulse traveling in the CCW direction. The position of Bob's PM is important since the pulse that it modulates must be returning from its round trip in the loop in order to prevent any information about Bob's modulation choice from traveling through the loop. A timing and control mechanism must also be established so that only one Alice can modulate the photon at a time. Upon traveling around the loop, the pulses interfere in the coupler and enter one of two photon detectors. Photons enter Detector 1 when they experience a phase shift between the CW and CCW pulses inside the Sagnac interferometer. On the other hand, they enter Detector 2 when they experience a phase shift between the CW and CCW pulses inside the Sagnac interferometer. In such topology, each user on the network, except Bob, contains only a single-PM and no photon detectors. This can simplify any deployment of a secure ring network using the Sagnac because Bob is the only user that requires the single photon detectors. This topology can also be used to distribute key between arbitrary two users in the ring, e.g., A_l and A_m ($l, m = 1, 2, \ldots, N$ and $l \neq m$) with Bob's assistant. However, this topology is fragile for resisting the attack of any dishonest user in the optical-ring since the dishonest user can easily operate the quantum signal.

The schematic diagram of the wavelength-routed network topology is shown in Fig.9.9(c). This topology is implemented with unbalanced MZIs and is very similar in layout to the star network presented in Fig.9.9(a). The major difference is that Alice has the ability to control which user receives the photons by employing a wavelength-routing scheme. Alice is equipped with a wavelength tunable PLS and the receivers are assigned their own wavelength channel. Alice transmits to a particular user by tuning her source to that user's wavelength and the photons are routed via an AWG. The advantage of this topology is that the insertion loss of the AWG is approximately uniform regardless of the number of channels. Theoretically, the number of users that this type of network will support is limited only by the channel spacing of the AWG and the bandwidth of the fiber. In addition, single photon detectors must be sensitive for the entire range of frequencies used in the network. This is not a concern as avalanche-photodiode (APD)-based single photon detectors respond to a much broader spectrum than the band of wavelengths used in multiwavelength networks.

The wavelength-addressed bus network is also based on the unbalanced MZI setup and is shown in Fig.9.9(d). Like the wavelength-routed network,

this network also allows Alice to route her photons to a desired user by tuning the photons to be desired wavelength. In such a system, Alice is equipped with a tunable PLS, and each receiver is assigned their own wavelength channel. Alice selects an intended receiver by tuning her source to that user's wavelength and transmits the encoded photons along the bus. The receivers are connected to the bus line through a fiber Bragg grating (G), which allows them to retrieve only the photons intended for them. These gratings are designed to reflect photons of a specific wavelength to a given user and transmit all others. The network accommodates multiple users by placing several fiber Bragg gratings in series along the bus. One of the merits of this topology is that it can be easily expanded to accommodate more users by simply tapping the bus and inserting a suitable grating.

In the fiber telecommunication system, the so-called passive optical network (PON) is an important access network. Generally, a PON network consists of one optical line terminal (OLT) and N optical network units (ONUs). Between the OLT and ONUs there is a $1 \times N$ splitter or router. Thus, these configurations in Fig.9.9(a, c, d) are all PONs. Commonly, the OLT can send an optical signal to ith ONU which calls downstream, and the ith ONU can also send an optical signal with different wavelength to the OLT, which is called upstream. However, any two ONUs cannot directly communicate each other without the help of the OLT. Of course, with optical virtual private network (VPN) techniques this problem can be circumvented. Since the transmission distances in a PON range from several kilometers to dozens of kilometers, the quantum private communication can be apparently employed in a practical PON system. Thus, if based on current network topologies and technologies then these access links are likely to have a span of up to around 10 km and to be based on either multiple P2P links or point-to-multipoint PONs. Optical access solutions of these types are currently in deployment in a number of regions of the world, where network operators are upgrading preexisting copper-based access networks with optical fiber in order to supply new, high bandwidth services to customers.

A point-to-multipoint PON uses an 1×32 standard telecommunication optical splitter (fabricated using ion-exchange technology and single-mode at a wavelength of 1550 nm) within the insecure transmission channel has been investigated [**?**]. The schematic diagram is shown in Fig.9.10. In this figure, Alice plays the role of OLT as a central node and 32 Bobs serve as different ONUs. This application is based on an 850 nm wavelength gigahertz clock-rate single-receiver system. The input and output ports of the optical splitter were fusion spliced to the single-mode at 850 nm optical fiber from Alice and Bob, respectively, to suppress the propagation of the LP11 mode within the splitter. The employed quantum channel is constructed from a single-mode fiber at a wavelength band of 1550 nm which is not currently utilized in access networks, so that it is compatible with existing telecommunications fiber. The developed quantum key distribution networks are capable of transmitting over distances consistent with the span of access links for metropoli-

tan networks (10 km), at clock frequencies ranging up to 3 GHz.

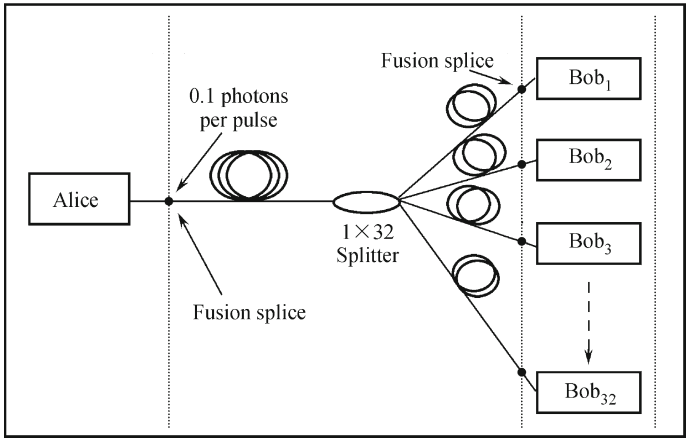

Fig. 9.10. Quantum key distribution in point-to-multipoint PON

To implement the fiber-based private communication network in quantum ways, routers for quantum signals from one sender to an arbitrated receiver in the network are necessary. Since the quantum private communication is a special optical communication at the extreme condition, i.e., the weak laser pulse or even single photon, routers for classic optical fiber communication systems may be applied also for the quantum private communication. Accordingly, the router for quantum private communication can be achieved using WDM in a network architecture where photons at a given wavelength are routed to a particular user. This architecture also allows the use of optical entanglement. This helps in reducing security constraints. Actually, many devices which are employed for the classic optical fiber communication may be employed for the quantum private communication. However, the amplifier cannot be used for the quantum private communication because it will influence the security of the quantum communication system.

9.4 Private Communication Over Free-Space

Except for the fiber-based quantum private communication, several important experiments have demonstrated possibilities of practical quantum private communications in free-space [**?**, **?**, **?**]. This section describes the basic principle and presents several typical free-space private communication systems in quantum ways, including the point-to-point private communication in an atmosphere channel close to the earth surface, stratospheric-platform-based private communication, and satellite-based private communication. Since the free-space private communication is implemented using optical sig-

nal with quantum constraints, i.e., using faint laser pulses, single photon signals, or coherent state signals, this scenario may be viewed as a special kind of wireless optical communication which has been investigated in the classic optical communication. Accordingly, this kind private communication may be called the wireless quantum private communication.

9.4.1 Transmitter, Receiver, and Relay

To set up a practical free-space quantum private communication system, three core components should be considered: the transmitter, relay, and receiver. They are similar to those components used in the wireless optical communication systems.

Generally, a transmitter module comprises a quantum signal source which emits quantum signal suiting for transmission in a free-space channel, a module for timing synchronization with the receiver station and channel for classical communication, and an optical antenna module for transmitting quantum signal to the free-space channel. Obviously, the transmitter module for the free-space quantum private communication is more complex than that in the fiber-based system. The quantum signal source is employed to emit the needed quantum signal. Both single photon signals and continuous variables signals are all appropriate for the free-space quantum private communication. Thus, the addressed quantum signal sources include photon source for application separately or for generating entangled photon pairs (including passive or active manipulation of single qubit-states) and continuous variable quantum signal source for generating coherence state signal, squeezed state signal or continuous variable entanglement state signal. Mechanisms for generating these quantum signals have been described in Chapters 7 and 8. The timing synchronization module is the same as that in the wireless optical communication systems. Of course, quantum timing synchronization [**?**] has become possible which is more accurate than the classic timing synchronization. The optical antenna module consists of telescopes which play the role as antenna in wireless radio communication systems.

A receiver module comprises one or more optical input channels, each of which allows independent manipulation of quantum signals such as the rotation of photon polarization or the modulation of an interferometric phase. Additionally, it has to be equipped with quantum signal detectors at each input port, a receiver module for timing-synchronization, a classical channel for communication with the transmitter, and optical antenna module for receiving the quantum signal and classic optical signal. As described in previous, three kinds of quantum signal detectors, i.e., the single photon detector, homodyne detector, and direct intensity measurement, are always employed in quantum private communication systems. In practices, which kinds of quantum signal detectors are deployed depending on the employed

quantum signal source and adopted cryptosystem. For example, in QKD schemes, if the single photon signal source is exploited in the transmitter module, single photon detectors should be deployed in the receiver module; while homodyne detectors should be deployed when continuous variable quantum signal sources are employed in the transmitter module. Compare to the classic wireless optical communication system, the receiver module is more complex since the qubit may be remotely controlled when entanglement states are exploited. Subsequently, there are two kinds of receiver modules depending on whether active (remote) control of optical elements for qubit manipulation is possible or not (via, e.g., a polarizer or a retarder). Passive manipulation only requires a static setup of linear optic components. Typically, beam splitters in the input ports would randomly distribute incoming photons to differently oriented retarders, polarizers, or beam splitters, where a manipulation and successive detection of single photons takes place. For active control of single qubit manipulation, an additional information concerning the arrival time (i.e., a timing synchronization) is required.

The free-space optical communications are associated with the optical signal transmission in atmosphere and space. This is the same for the wireless quantum private communication system. Currently, the transmission in space is more popular since the importance of the application of satellite communications. This involves the transmitter and receiver which may be combined to call transceiver. Optical transceivers for space-to-ground links or inter-satellite links are almost state of the art. The major design parameters for the transmission subsystem are laser wavelength, modulation format and data rate, and reception technique. Of equal importance is the subsystem required for link acquisition, beam pointing, and automatic mutual terminal tracking which is always called APT. Because of the very narrow widths of the communication beams involved, APT asks for highly sophisticated concepts and for electro-mechanic and electro-optic hardware meeting exceptional technological standards. Major parameters entering the link capacity are telescope size, optical transmit power, link distance, and receiver sensitivity. Other aspects are mass, volume, and power consumption of the terminal. Examples for existing space laser communication links include ESA's inter-satellite link SILEX (semiconductor Laser Inter-satellite link experiment) and a satellite ground link, which was only recently realized between ARTEMIS and ESA's optical ground station OGS at Tenerife.

In transmission for optical signal as well as quantum signal, relay modules are necessary in some cases for redirecting and/or manipulating quantum signal without actually detecting them. Possibilities for its implementation range from a simple retroreflector to a more sophisticated relay-satellite (e.g., for deep-space communications). A new technique called quantum swapping has, in principle, become possible to play the role as a traditional relay. This leads the well-known quantum repeater which is a hot research topic in the quantum communication. Although theoretical models and some physical experiments have been presented, it is still not available in practices. It

is worth emphasizing that a relay cannot serve as an amplifier since the amplifying operation will destroy the transmitted qubits. This is a consequence of the quantum no-cloning theorem.

As demonstrated in above, photon sources and detectors presently implemented in classical space laser communication systems can, in general, not be directly employed in quantum communication systems. However, most modules in the classical space laser communication systems are suitable for the quantum private communication. In addition, the experience available may serve as a starting point for the development of space qualified components needed for quantum space experiments. The available optical communication technology could, of course, be applied to provide the classical channel that is always necessary in parallel to the quantum channel. One would also make synergistic use of some of the optics employed for APT and employ one and the same telescope as antenna for both the classical and the quantum channel, which is a novel way of quantum-classical-multiplexing.

9.4.2 Link Attenuations

Quantum signal would be attenuated in the transmission due to the noisy and lossy channel, which has been described in Section 9.2. These effects result in the link attenuation for the employed quantum signal. Physically, the link attenuation implies power attenuation of the transmitting quantum signal in a channel. It is always described using a link attenuation factor A, which is defined as the ratio of the mean transmit and receive power, P_t and P_r, measured at the entrance and the exit of the transmit and the receive telescope, respectively. Clearly, losses due to quantum signal detection efficiency and optical elements are not included in this value. Generally, the logarithmic representation is adopted since the dB is always employed as a unit for the power attenuation in the communication. Thus, the link attenuation factor A is defined mathematically as

$$A = 10 \lg \left(\frac{P_t}{P_r} \right) \quad \text{(dB)}. \tag{9.4.1}$$

In the vacuum, the parameters P_t and P_r have the following relationships when $0 \leq l < D_T^2/\lambda$,

$$P_r = \begin{cases} P_t T_t T_r L_p \dfrac{D_r^2}{D_t^2}, & D_r \leq D_t \\ P_t T_t T_r L_p, & D_r > D_t \end{cases} \tag{9.4.2}$$

and when $l \geq D_t^2/\lambda$,

$$P_r = \begin{cases} \dfrac{P_t T_t T_r L_p D_r^2}{2l \tan\left(\dfrac{\lambda}{2D_t}\right) + D_t^2}, & D_r \leq 2l \tan\left(\dfrac{\lambda}{2D_t}\right) + D_t^2 \\ P_t T_t T_r L_p, & D_r > 2l \tan\left(\dfrac{\lambda}{2D_t}\right) + D_t^2 \end{cases} \tag{9.4.3}$$

where the subscripts t and r denote the transmitter and receiver, respectively, l is the path length, λ is the wavelength, D_t and D_r are the apertures of the transmit and receive telescopes, respectively, T_t and T_t are the transmission factors of the telescopes, respectively, and L_p is the pointing factor.

Atmospheric effects on propagation at optical beams can be divided into three categories: absorption, scattering, and turbulence. The effects have been described in Section 9.2. Since the absorption and scattering mainly depend on wavelength and visibility conditions, the net impact of atmospheric turbulence additionally depends on the elevation angle and direction of transmission. The main effect of atmospheric turbulence is an enlarged beam divergence, resulting in a reduced amount of signal power collected by the receive telescope. Further turbulence-induced effects are beam-wander, loss of coherence, scintillation, pulse distortion, and broadening as described in Section 9.2. The effect of turbulence in atmosphere is in general quite different for a space-to-ground link and a ground-to-space link. In a space-to-ground link the light propagates through vacuum for the most of distances first before being disturbed by the atmosphere, whereas for a ground-to-space link the beam spreading effects of turbulence take place at the beginning of the propagation, causing a strongly enhanced divergence.

Assume that the divergence due to turbulence adds quadratically to the divergence of the telescope. Then the influence of the atmosphere can be taken into account by the so-called Fried parameter, r_0, which can be interpreted as an "effective aperture". Thus, the effects of turbulent medium in atmosphere cause an additional diffraction angle $\theta_{\mathrm{a}} = \lambda/(2r_0)$. Consider the quantum signal has the similar transmission properties as the classic optical signal except for the allowable condition, according to the model presented in [**?**] which is widely used, link attenuation can be calculated as follows. When $0 \leq l < {D_t}^2/\lambda$, the link attenuation is calculated by

$$A\ (\mathrm{dB}) = \begin{cases} 10 \lg\left(\dfrac{d_0^2}{T_t L_p T_r D_r^2}\right) + A_{\mathrm{atm}}, & D_r \leq d_0 \\ 10 \lg\left(\dfrac{1}{T_t L_p T_r}\right) + A_{\mathrm{atm}}, & D_r > d_0 \end{cases} \tag{9.4.4}$$

where $d_0 = 2l \tan\left(\dfrac{\lambda}{2r_0}\right) + D_t$ and A_{atm} denotes the absorption and scattering of atmosphere. The parameter A_{atm} should be calculated using

$$A_{\mathrm{atm}} = A_{\mathrm{a}} \times 10 \lg \mathrm{e} \tag{9.4.5}$$

with A_{a} being the attenuation coefficient of aerosols. It is noted here that the relationship $A' = A \cdot 10 \lg \mathrm{e}$ between two parameters, i.e., the attenuation coefficient $A(\mathrm{km}^{-1})$ and attenuation $A'(\mathrm{dB} \cdot \mathrm{km}^{-1})$ are exploited, which is frequently exploited in engineering calculation. When $l \geq {D_t}^2/\lambda$, the diffraction effect of transmit telescope should be taken into account, which can be measured through diffraction angle $\theta_{D_t} = \lambda/2D_t$. Thus the link attenuation is

$$A\ (\mathrm{dB}) = \begin{cases} 10 \lg \left(\dfrac{d_1^2}{T_t L_p T_r D_r^2} \right) + A_{\mathrm{atm}}, & D_r \leq d_1 \\ 10 \lg \left(\dfrac{1}{T_t L_p T_r} \right) + A_{\mathrm{atm}}, & D_r > d_1 \end{cases} \tag{9.4.6}$$

where $d_1 = 2l \tan \left(\dfrac{\lambda}{2r_0} + \dfrac{\lambda}{2D_t} \right) + D_t$.

Above equations demonstrate that the link attenuation factor A strongly depends on the atmosphere loss A_{a}, which is influenced by both the absorption and scattering of atmosphere molecules and aerosols. The parameter A_{a} can be calculated using Eq.(9.4.5) and the parameter

$$A_{\mathrm{a}} = \kappa + \sigma, \tag{9.4.7}$$

where κ and σ are absorption and scattering coefficient, respectively. Separating the effects of molecules and aerosol, the factor A_{a} is rewritten as

$$A_{\mathrm{a}} = \kappa_m + \kappa_a + \sigma_m + \sigma_a, \tag{9.4.8}$$

where the subscripts m and a refer to the atmosphere molecules and aerosol, respectively. Since σ_m is about 10^{-2} of σ_a, when the dimensions of atmosphere molecules are smaller than the wavelength of optical signal, and κ_m is in the range of from 10^{-3} to 10^{-5} of σ_m at the laser wavelength of $\lambda = 860$ nm, the effect of atmosphere molecules can be neglected. Therefore, the factor A_a is mainly caused by aerosols in the atmosphere.

The above has investigated the propagation properties in atmosphere of the quantum signals which is actually a special kind of optical signals at an extreme condition. These propagation properties do not involve the quantum characteristics which are appeared in the quantum measurement, i.e., quantum signal detections. Actually, quantum measurements lead the allowable conditions for the quantum signal transmission in free-space to be more strict.

As an example, consider the transmission of two-photon entanglement pair in atmosphere. In this scenario, the accidental coincidence rate is given by $C_{acc} = S_1 S_2 \Delta\tau$, where S_1, S_2 are dark count rates of two detectors and $\Delta\tau$ is the timing resolution for the electronic registration of a two-fold coincidence event. Making use of the minimum signal-to-noise ratio (SNR) that required for violating the Bell-inequality, since this guarantees at the same time the security of certain quantum cryptography schemes. For the

case of polarization-entangled photons this necessitates a two-fold coincidence visibility of at least 71%, corresponding to a SNR of 6 : 1. Below that ratio a local realistic modeling of the observed correlations is possible thus allowing unobserved eavesdropping. Therefore, in order to discriminate the signal from background coincidences, the minimal observed coincidence rate C_{min} must be at least 6 times larger than C_{acc}.

The coincidence detection rate is determined by the total coincidence efficiency link, which is the product of the individual efficiencies for the two qubit links, $\eta_{link} = \eta_{Link1}\eta_{Link2}$. The detected signal coincidences C are given by the product $C = P\eta_{link}\eta_{det1}\eta_{det2}$, where P is the pair production rate of the source and η_{det1}, η_{det2} are the detection probabilities. In order to achieve a violation of Bell's inequality, the signal coincidences must exceed the limit $C_{min} = SNR \cdot C_{acc}$, which leads to the following limit for the total link efficiency,

$$\eta_{link} \geq SNR\frac{C_{acc}}{P\eta_{det1}\eta_{det2}} = SNR\frac{S_1 S_2 \Delta\tau}{P\eta_{det1}\eta_{det2}}. \tag{9.4.9}$$

9.4.3 Atmosphere-based Private Communication

The quantum private communication implemented in atmosphere has become possible. Especially, QKD in atmosphere has entered the practical application stage. In the case of transmission through free space, the polarization states of photons have been used to conveniently encode information, since they do not change significantly in transit. Of course, it sounds difficult to detect single photons against background light, but the first experiment has demonstrated the possibility of the free space QKD. The systems developed for free space applications are actually very similar to the one for optical fibers. The main difference is that the emitter and receiver are connected to telescopes pointing at each other, instead of an optical fiber. The contribution of background light to errors can be maintained at a reasonable level by using a combination of the timing discrimination, spectral filtering, and spatial filtering.

To demonstrate the quantum private communication implemented in atmosphere, two typical QKD schemes experimentally implemented in atmosphere are exemplified. The first is the experimental implementation between two mountains with a distance 23.4 km in Germany. The second, which uses decoy state to prevent the photon-number splitting (PNS) attack strategies, has been experimentally implemented in Spain with a distance 144 km. These implementations have motivated the investigation on links from ground to low-orbit communication satellites.

1) Experiment in Germany

A semi-portable free-space quantum cryptography system has been tested and worked for key exchanging between two mountain tops, Karwendelspitze

(2244 m) and Zugspitze (2960 m), in Southern Germany [**?**]. Compared to the original experiment using polarization rotations performed by high-voltage piezoelectric ceramic transformer (PZT), it is by far advantageous to use separate laser diodes for every polarization at the transmitter. An additional simplification of the equipment can be achieved by randomly splitting the light in the receiver between the analyzers for two bases by a nonpolarizing beamsplitter. This allowed one to design a long-range free space key exchange apparatus capable of exchanging keys over free space ranges greater than 20 km where diffraction/turbulence and absorption losses reach up to 20 dB.

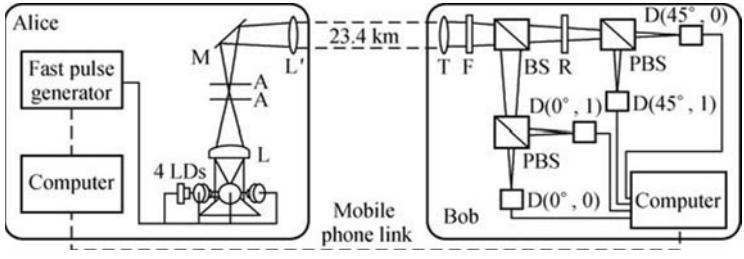

Fig. 9.11. Overview of experiment configuration for QKD in atmosphere

The transmitter in Fig.9.11 is designed round a 80 mm diameter transmit telescope. A novel miniature source of polarization coded faint pulses approximating single photons is used. This consists of four laser diodes (850 nm wavelength) arranged on a ring around a conical mirror. Each laser is rotated to produce one of the four polarizations: 0, $\pi/4$, $\pi/2$, $3\pi/4$ and illuminates a spatial filter consisting of two pinholes with a diameter of 100 μm spaced at a distance of 9 mm. Since the overlap of emission modes of the four laser diodes with the filter mode is rather poor, the initially very bright laser pulses are attenuated to the required single photon level. Lasers are randomly driven from a computer via a digital output card at 10 MHz repetition rate using sub-nanosecond duration pulses. This creates about 500 ps duration optical pulses randomly polarized in 0, $\pi/4$, $\pi/2$ or $3\pi/4$ directions. The computer uses a pre-stored random number to choose the polarization for the present set of experiments. The receiver consists of a 25 cm diameter commercial telescope with computer controlled pointing capability. Unfortunately, the resolution of mechanics of this system was the limiting factor for the alignment of the receiver, and was also difficult to handle at the harsh outdoor condition. Yet, the stability of the system was very convincing. A compact four-detector photon counting module was coupled to the back of the telescope after a long pass filter to block out short wavelength background. The module consists of a polarization-insensitive beamsplitter passing two beams to polarizing beamsplitters that are followed by four photon counting avalanche diodes. One polarizing beamsplitter is preceded by a 45° polarization rotator. Photons detected in this channel are thus measured

in the $\pi/4$ basis, while the other polarizer allows measurement in the $0-\pi/2$ basis. Since the splitting of incoming photons to the two analyzers by the beamsplitter is truly random, no other random number sequence for basis choosing is required on the receiver side, although it suffers the expense of more detectors.

The distance between the two locations is 23.4 km. At this distance, the transmitted beam was 1-2 m in diameter and was only weakly broadened by air-turbulence effects at this altitude. Lumped optical losses of about 18 – 20 dB were measured and, using faint pulses containing 0.1 photons per bit, the detected bit rate at Bob was 1.5-2 kb/s with the receiver efficiency of 15%. Operating at night with filters of the 10 nm bandwidth reduced the background counts, and errors appeared in less than 5%. After sifting and error correction, net key exchange rates were hundreds of bits per second. In a series of experiments, several hundreds of kilobits of identical key string were generated at Alice and Bob. By improve the receiver efficiency and background counts, key exchange could still be carried out when the transmission loss is beyond 33 decibels. This marks a step towards accomplishing key exchange with a near-Earth orbiting satellite and hence a global key-distribution system.

2) Experiment in Spain

More recently, an experiment by transmitting quantum signals over a distance of 144 km between the Canary Islands of La Palma and Tenerife in Spain via an optical free-space link has been implemented. These experiments are performed by a united research group in European. Two kinds of quantum signals including the weak coherent laser pulse and entangled photon are employed in two different experiments. The experiment using weak coherent laser pulses was implemented in 2007. In this experiment the optics of the QKD transmitter (Alice) consist of four laser diodes, whose orientation was rotated by 45° relative to neighboring ones. At a clock rate of $R_0 = 10$ MHz one of them emitted a 2 ns optical pulse centered at 850 nm with a full width at half maximum (FWHM) of 1.5 nm, according to random bit values, that were generated beforehand by a physical random number generator and stored on Alice's hard disk. Output beams of all diodes were overlapped by a concaveconvex pair of conical mirrors and coupled into a single mode optical fiber running to the transmitter telescope. Decoy pulses, which are additional quantum states for eavesdropping detection in the transmitted qubit sequence, at higher mean photon number μ_d were randomly interspersed in the signal sequence by firing two randomly chosen diodes simultaneously. For the empty decoy pulses, the electrical pulse driving the laser diode was suppressed. The mean photon number for all decoy states was monitored with a calibrated single photon detector at one of the output ports of a 50:50 fiber beam splitter before coupling to the telescope. The single photon polarization analysis was performed inside the transmitter telescope to correct changes along the fiber.

The experiment using entangled photon was implemented by the same group in 2007. The transmitted photon was received in the Optical Ground Station of the European Space Agency, and the entangled partner photon was detected locally at the transmitter. In this experiment, quantum correlations of the transmitted photons with its partner are sufficiently high to violate Bell's inequality and are also used to generate a quantum cryptographic key. The experiment fully exploits the distance limits for ground-based free-space communication, significantly longer distances can only be reached using air- or space-based platforms. The range achieved thereby demonstrates the feasibility of quantum communication in space, involving satellites or the International Space Station (ISS).

9.4.4 Stratosphere-based Private Communication

Above experiments indicate possibilities for free-space quantum private communication based on stratospheric platforms, which have been employed in the radio wireless communication system. In the classic stratospheric communication, stratospheric platforms are usually suspended at the height of about 20 km above ground surface since the atmosphere condition of the stratosphere is quite stable. Employing the physical architecture of the classic stratospheric communication network and the experimental results of quantum signal in atmosphere, a practical quantum communication model called as quantum stratospheric communication (QSC) become possible.

Analogy to the configuration of the classic stratospheric communication which has been used for the free space optical communication and wireless communication, QSC model also consists of stratospheric platforms and ground stations. A stratospheric platform or a ground station may be called as a network node. All nodes may construct various architectures in practical network. To warrant the quantum private communication, optical equipments for quantum signals are embarked on stratospheric platforms and ground stations. The stratospheric platform may be regarded as a transmitter, a receiver or a relay station. Communicators may exchange information via a quantum channel or a hybrid channel which combines a quantum channel and some classical channels.

In the stratosphere-based private communication, one of key problems is the link attenuation. Consider a faint laser beam with average photon number of 0.1 in each laser-pulse as employed in many experimental systems. This kind of quantum signals is regarded approximately usually as the single photon signal. Suppose that the quantum state carried by the quantum signal holds a polarized entangled state, which can be expressed as

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle_a|\downarrow\rangle_b - |\downarrow\rangle_a|\uparrow\rangle_b\right),$$

where subscripts a and b denote two photons of each entangled pair, respec-

tively, $|\uparrow\rangle$ and $|\downarrow\rangle$ are possible states they maybe, respectively. From Section 9.4.2, the minimum SNR required for violating the Bell-inequality is 5.89 and the corresponding maximal link attenuation is 60 dB for the polarized entangled photons. According to this requirement, the allowable condition for the quantum signal transmission with the entanglement state is that the link attenuation should be under 60 dB.

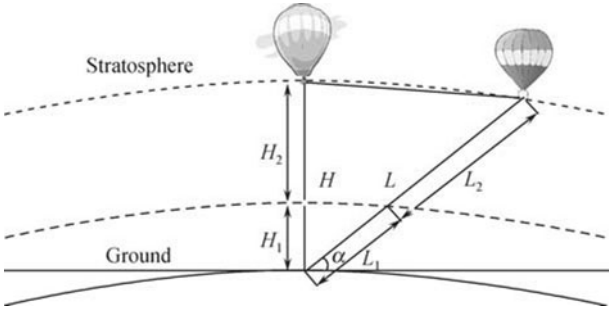

Fig. 9.12. Model of quantum stratospheric communication

Generally, the thickness of aerosols decreases exponentially as the altitude increases, but the thickness above the height of 5 km is almost a constant which is independent of the ground visibility [**?**]. This feature indicates that the atmosphere between the ground surface and stratosphere platform can be divided into two layers, i.e., the lower layer and upper layer. In Fig.9.12, H_1 is the altitude from ground surface to 5 km high and H_2 is the altitude from 5 km to the stratosphere platform, α is the elevation angle. Then, the atmospheric attenuation of link L is given by

$$A_{\mathrm{a}}^{L} = A_{\mathrm{a}}^{L_1} + A_{\mathrm{a}}^{L_2}, \tag{9.4.10}$$

where $A_{\mathrm{a}}^{L_1}$ and $A_{\mathrm{a}}^{L_2}$ are atmospheric attenuations of links L_1 and L_2, respectively.

According to characteristics of the aerosol distribution in atmosphere, the atmospheric attenuation coefficient at each altitude can be calculated by

$$A_{\mathrm{a}}(h) = \begin{cases} \dfrac{3.91}{V}\left(\dfrac{\lambda}{0.55}\right)^{-\mathrm{q}} \exp\left(-\dfrac{h}{H_s}\right), & 0 \le h \le H_1 \\ \gamma, & H_1 \le h \le H \end{cases} \tag{9.4.11}$$

where V is the ground visibility, q is a constant depending on V, H_s is the scale height, γ is the attenuation coefficient of the upper layer. The aerosols attenuation coefficient is assumed to be a constant in any case since the density of aerosols is extremely low in the upper layer.

The stratospheric platform is assumed to be suspended at the height of 20 km as in the classic stratospheric communication, i.e., $H = 20$ km.

According to the experimental implementations and the stratospheric properties, following parameters are adopted. The telescope transmission factor is 0.8, diameters of transmit telescope and receive telescope are 5 cm and 25 cm, respectively, $\lambda = 860$ nm, $\gamma = 0.0025$ and the earth radius R = 6378 km which gives rise to the Earth's curvature. Let the average impact of turbulence on the whole link be $r_0 = 6$ cm. The impact of turbulence on different parts of the link is random, however, the involved model is suitable to calculate bounds of the link attenuations in the QSC.

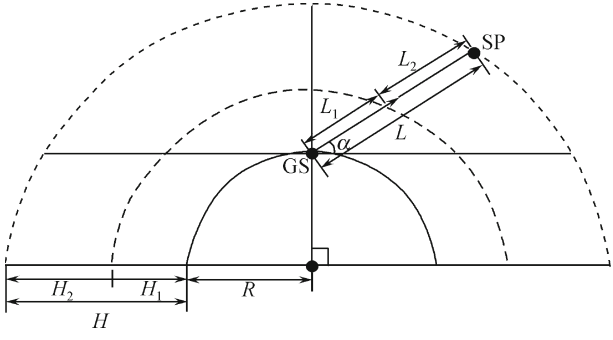

Fig. 9.13. Diagram of link between ground station and arbitrary stratospheric platform

For the link between the ground station and stratospheric platform (GS-SP), which has been shown in Fig.9.13, the path length can be calculated by

$$L^{gs} = \sqrt{R^2 \sin^2 \alpha + H^2 + 2RH} - R \sin \alpha. \tag{9.4.12}$$

Then, the atmospheric attenuation of GS-SP link is

$$A_{\mathrm{a}}^{\mathrm{gs}} = \int_0^{L_1} \frac{3.91}{V} \left(\frac{\lambda}{0.55} \right)^{-\mathrm{q}} \mathrm{e}^{-\xi_0} \, \mathrm{d}l + \gamma L_2, \tag{9.4.13}$$

where $\xi_0 = (\sqrt{R^2 + 2Rl \sin \alpha + l^2} - R)/H_s$.

The GS − SP link attenuation A^{gs} as a function of the elevation angle is shown in Fig.9.14. Consider two typical weather conditions, i.e. clear and light haze, and corresponding ground visibilities are $V = 23$ km and $V = 15$ km, respectively. As a comparison, the link attenuation in vacuum is also plotted.

Since the allowable attenuation is up to 60 dB for the polarized entanglement state, Fig.9.14 shows that the elevation angle α should be in the range of $5^\circ \leq \alpha \leq 90^\circ$. Accordingly, for any $\alpha \in [5^\circ, 90^\circ]$, the quantum private communication is possible since the link attenuation is under 60dB at this case. The transmitted length L can be calculated by employing Eq.(9.4.11). As an example, one can obtain easily the maximal link length which may reach at least 180 km in two weather conditions, i.e. clear and light haze.

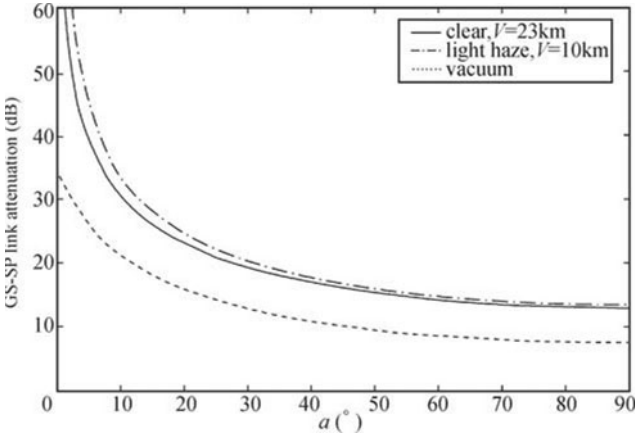

Fig. 9.14. Dependence of the GS-SP link attenuation on elevation angle α with $L_{\mathrm{p}} = 0.7$

The QSC may encounter some difficulties in the situation of $\alpha < 5°$ unless transmit telescope and receive telescope with larger apertures are used. When $\alpha = 90°$, the link attenuation reaches the minimum which is about 14 dB. This value is about 7 dB higher than one in the vacuum scenario. In addition, the dependence of the link attenuation on the visibility has been considered. Fig.9.14 shows that higher visibility gives rise to a lower link attenuation. For example, in quite clear weather or at high altitudes, the influence of atmosphere is much smaller and the performance of QSC is much better. However, fog weather and clouded skies will make the link impossible as the atmospheric attenuation increases dramatically in these scenarios.

The link between two stratospheric platforms, i.e., the SP-SP link, is more complex since the platforms are not always at the same altitude due to the influence of the Earth's curvature. To calculate the link attenuation between two platforms, the model plotted in Fig.9.15 is employed.

The link between $\mathrm{SP_A}$ and $\mathrm{SP_B}$ can be divided into three parts, i.e.,

$$L^{SS} = L_1 + L_{21} + L_{22}, \tag{9.4.14}$$

where L_1 is in the lower layer, L_{21} and L_{22} are in the upper layer. Let β denote the zenith angle. Obviously, the zenith angle is in the range of $\beta_{min} \leq \beta \leq 90°$, where the minimum zenith angle is given by $\beta_{\min} = \arcsin[R/(R+H)]$. The bound of the link length is $L_{min}^{SS} = 2(R+H)\cos\beta$. Thus the atmospheric attenuation of the SP − SP link is calculated by

$$A_{\mathrm{a}}^{\mathrm{ss}} = \begin{cases} 2\displaystyle\int_{L_{21}}^{L_{21}+\frac{L_1}{2}} \frac{3.91}{V}\left(\frac{\lambda}{0.55}\right)^{-\mathrm{q}} e^{-\xi_1}\,\mathrm{d}l + \gamma L_2, & \beta < \beta_1 \\ 2\gamma(R+H)\cos\beta, & \beta > \beta_1 \end{cases} \tag{9.4.15}$$

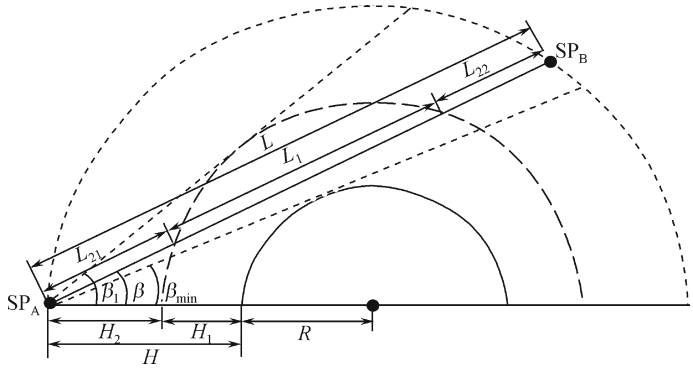

Fig. 9.15. Diagram of link between two arbitrary stratospheric platforms

where

$$\xi_1 = (\sqrt{l^2 + (R+H)^2 - 2l(R+H)\cos\beta} - R)/H_s,$$

and

$$\beta_1 = \arcsin[(R+H_1)/(R+H)].$$

The SP − SP link attenuation A^{ss} is shown in Fig.9.16. When the zenith angle $\beta < \beta_1$, the link attenuation is related to ground visibility since the SP − SP link travels through the lower layer. However the link attenuation is independent on the ground visibility when $\beta_1 \leq \beta \leq 90°$. Thus the curves of link attenuations for different ground visibilities intersect at $\beta = \beta_1$. In Fig.9.16, two curves with $V = 23$ km and $V = 10$ km are plotted respectively. One can see clearly the intersection of the two curves. From Fig.9.16 one finds that the range of the zenith angle for the SP − SP link is $86° \leq \beta \leq 90°$. Within this range, the largest distance between two stratospheric platforms can reach 890 km. When the zenith angle β approaches 90°, SP_A and SP_B should be very close. In this situation the quantum signal can always be received since the diameter of the receive telescope is larger than the broadened beam, so that the link attenuation is a constant, which is plotted in the window in Fig.9.16.

According to results of the quantum signal transmission displayed in Figs.9.14 and 9.16, a worldwide QSC network is possible in principle. In addition, such a stratospheric platform in the QSC network can serve as a relay station for connecting a ground station and satellite station. The above attenuation analysis reveals that in the weather conditions with ground visibility lager than 10 km, the maximum of the link length between ground station and stratospheric platform can reach 180 km. A stratospheric platform can cover the area at least 104 km^2. For the SP − SP link, the maximal distance between two stratospheric platforms is 890 km. Therefore, the involved QSC model is a good alternative to build up a worldwide quantum communication network. If one combines a QSC network with a fiber-based quantum communication network, a global quantum communication network can be realized. Of course, from the viewpoint of practical applications, it is not a practical way for that many stratospheric platforms are suspended in

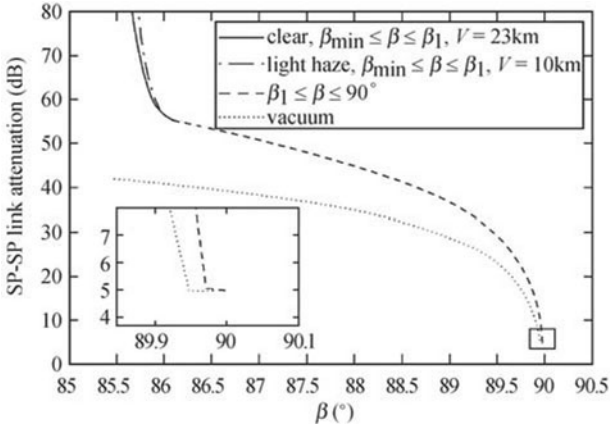

Fig. 9.16. Dependence of SP-SP link attenuation on zenith angle β with $L_p = 0.5$

the atmosphere since many satellites have been lunched. However, stratospheric platforms acting as relay stations or forming a local area network might be possible in practical applications.

9.4.5 Satellite-based Private Communication

The optical free-space link could provide a unique solution to the globe quantum private communication since they allow in principle for larger propagation distances of photons due to the low absorption of the atmosphere in certain wavelength ranges. Also, the almost non-birefringent character of the atmosphere guarantees the preservation of the polarization entanglement to a high degree. Free-space optical links have been studied and successfully implemented already for several years for their application in quantum cryptography based on faint classical laser pulses. A next crucial step is the distribution of quantum signals via such free space links. The above section has studied the quantum private communication based on stratospheric-platform. In this section, we move on to the satellite-based quantum private communication.

Broadly speaking, the satellite quantum private communication is a kind of quantum private communications which uses satellites as the terminals of transmitters and/or receivers. It may be modeled using Fig.9.17 which summarizes the scenarios considered based on satellites in geostationary orbit (GEO) and in the low earth orbit (LEO). Such satellites may serve as a platform for transmitters or receivers. This model does not envision the use of passive relays, e.g., retro-reflectors or mirrors, because of the high link loss they would introduce and because of the difficulty to implement a point-ahead angle. This model has been employed in Ref.[**?**]. In this model, five links are associated with the satellite quantum private communication system. The links 1 and 2 are associated with ground stations, and they may be called LEO-based link and GEO-based link, respectively. The links $3-5$ occur

between GEO and LEO satellites, where links 3 and 4 are LEO-to-LEO link and GEO-to-GEO link, respectively, while the link 5 is a LEO-to-GEO link. For these links, they are associated with different channel properties and attenuation. There are no attenuations in links 3∼5 since they are in vacuum. For the links 1 and 2, their attenuations can be described using the similar way as presented in previous subsection. For example, when the entangled photon-pair signal is employed, the link attenuation is the same as the calculations in Section 9.4.4.

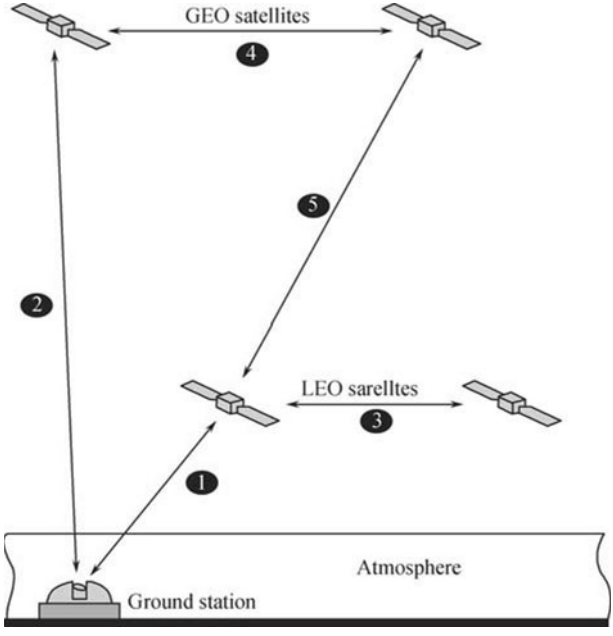

Fig. 9.17. Satellite quantum private communication model

An experiment at the conditions for the implementation of the single photon exchange between a low earth orbit geodetic satellite, called satellite Ajisai, and an Earth-based station was reported in 2008 [**?**]. This experiment mimics a single photon source on a satellite, exploiting the telescope at the Matera Laser Ranging Observatory of the Italian Space Agency to detect the transmitted photons. Weak laser pulses, emitted by the ground-based station, are directed toward a satellite equipped with cube-corner retroreflectors. These reflect a small portion of the pulse, with an average of less than one photon per pulse directed to the receiver, as required for the faint-pulse quantum communication. The returns from satellite are detected. The transmission distance has reached 1485 km which is just the perigee height of the low earth orbit geodetic satellite. Of course, the influences of the atmosphere should be considered in this case except for a very clear atmosphere.

9.5 Private Communication over IP Networks

From the viewpoint of network, modern communication systems are toward to run over the Internet protocol (IP), e.g., the IPv4 or the more recently IPv6. The security of the modern networks generally relies on one of two basic cryptographic techniques to ensure the confidentiality and authentication/integrity of traffic carried across the network: symmetric (secret) key and asymmetric (public) key. Indeed today's best systems generally employ both, using public key systems for authentication and establishment of secret session keys, and then protecting all or part of a traffic flow with these session keys. Certain other systems transport secret keys out of channel, e.g. via courier, as in classical cryptography.

As described in previous, fundamental aspects of quantum physics now suggest a third paradigm for the key distribution, i.e., the quantum key distribution. Theoretical and experimental researches have confirmed the utility of this paradigm. For example, the point-to-point quantum private communication in telecom fiber or atmosphere has entered the practical application. In modern communication, however, security of the end-to-end communication is more important than the P2P communication. Since the current end-to-end communication network, i.e., the well-known Internet network over IP protocol suites, consists of the optical fiber network and wireless communication, where the quantum private communication has become possible in these networks. This gives rise to the issue of how to implement the quantum private communication over IP networks, which is usually regarded as quantum Internet network. This section addresses this issue.

9.5.1 IPsec Extensions With QKD Protocols

The IPsec, short for Internet protocol security, is an architectural framework for secure communications within IP suite. To employ the quantum private communication system to the IP network, one has to syncretize the quantum private communication scheme into the architectural framework of the IPsec.

For clearly, the IPsec protocol suite is introduced firstly. The IPsec framework is defined by a standards-track document within the Internet engineering task force (IETF), namely request for comments (RFC) 2401, a security architecture for IP. The IPsec is a suite of protocols for securing IP communications by authenticating and/or encrypting each IP packet in a data stream. It also includes protocols for the cryptographic key establishment. In short, the IPsec opens standard that provides data confidentiality, data integrity, and data authentication between participating peers. Some important components are the authentication header (AH), encapsulating security payload (ESP), internet key exchange (IKE), and Internet security association and key management protocol (ISAKMP)/Oakley.

One of its components, the IKE protocol, permits two endpoints to agree first on which cryptographic protocols and algorithms they wish to employ for a given security association, and second on keys they use to encrypt and/or authenticate subsequent message traffic within that security association. IKE

is defined by its own standard track document within the "IETF, RFC 2409, the Internet Key Exchange". Although IKE is a relatively complicated protocol, its basic concepts are straightforward. Fig.9.18 depicts the most important elements involved in an ongoing relationship between two IKE peers. In this figure, SPD, SAD, and SA represent security policy database, security association database, and security association, respectively, and the filter is referred to the IP packets filter. This illustration is intended to be high-level and schematic rather than a detailed depiction of an actual software architecture.

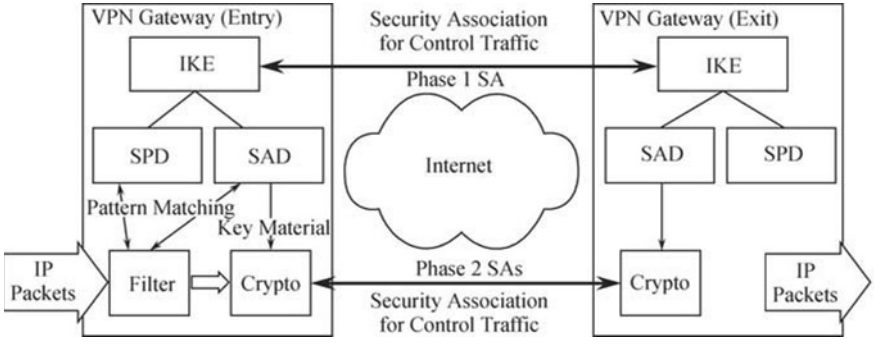

Fig. 9.18. Simplified schematic of IKE/IPsec architecture

In the IKE protocol, every security association has a maximum lifetime which governs how long the key material for that association can be used. This lifetime can be expressed either in time (seconds) or in data encrypted (kilobytes) and is configured via the security policy database (SPD) entry for a given security association. Every time of the lifetime expires, a new security association must be negotiated and it will bring with it fresh key material. This is sometimes termed "key rollover," because it replaces an older key by a newer one while still protecting the same underlying traffic flow. The key size needed for an encryption or a hash algorithm depends on the specific algorithm being employed. Some algorithms always use the same key size. For others, which can accept a range of key sizes, SPD must list the actual key size that should be employed for a given security association (SA).

Usually, the conventional IKE is implemented using public key cryptosystems, however they are associated with intractable problems. While the QKD protocol may generate a key with unconditional security. This motivates the substitution of the conventional IKE using the QKD protocol, which leads extensions of the IPsec.

The IPsec protocols operate at the network layer, i.e., layer 3 of the OSI model which consists of 7 layers including the application layer, presentation layer, session layer, transport layer, network layer, data link layer, and physical layer. As described in Chapter 4, a QKD scheme may be divided generally into 6 components: quantum signal transmission, eavesdropping detection, obtaining raw key, reconciliation, privacy amplification, and authentication. All these components are associated with at least a determined QKD protocol. Consequently, the QKD system may be also regarded as a suite of

protocols. For example, the quantum signal transmission is associated with a QKD scheme, e.g., the BB84 protocol, B92 protocol, or EPR protocol, while the channel authentication is involved in the eavesdropping detection process, and so on. In addition, there are some optical process control (OPC) subsystems in the implementation. According to the OSI model, the quantum signal transmission and OPC correspond to the physical layer and data link layer, respectively. While the remainders may be emerged into the IPsec protocols suite. According to the above description, a schematic demonstration described relationships between the IPsec and the QKD system has been built in Fig.9.19.

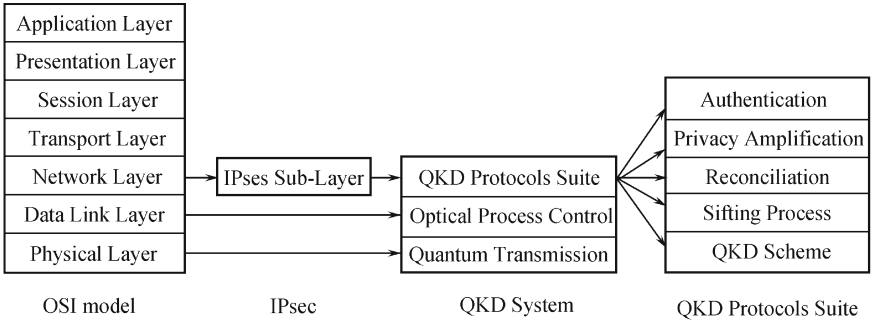

Fig. 9.19. Relationships among OSI model, IPsec and QKD system

The IPsec supports two encryption modes: transport and tunnel. The transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. The more secure tunnel mode encrypts both the header and the payload. On the receiving side, an IPSec-compliant device decrypts each packet. Usually, the transport mode provides a secure connection between two endpoints as it encapsulates IP's payload, while the tunnel mode encapsulates the entire IP packet to provide a virtual "secure hop" between two gateways. The latter is used to form a traditional virtual private network (VPN), where the tunnel generally creates a secure tunnel across an untrusted Internet. Clearly, the QKD scheme can be employed in the IPsec. Even one may substitute the classic cryptosystem using quantum cryptosystem when the later becomes mature.

Other Internet security protocols in widespread use, such as the secure socket layer (SSL) protocol, transport layer security (TLS) protocol, and secure shell (SSH) Protocol, operate from the transport layer up (OSI layers 4 – 7). This makes IPsec more flexible, as it can be used for protecting layer 4 protocols, including both transmission control protocol (TCP) and user datagram protocol (UDP), the most commonly used transport layer protocols. IPsec has an advantage over SSL and other methods that operate at higher layers: an application doesn't need to be designed to use IPsec, whereas the ability to use SSL or another higher-layer protocol must be incorporated into the design of an application. The IPsec uses IKE to handle negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPsec. The

IPsec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host. Combining the quantum cryptographic techniques and the IPsec suite protocols a more secure IP network may be built. Next, an example of combining the conventional VPN with the QKD schemes is demonstrated over the IP network.

9.5.2 Quantum Virtual Private Network

The conventional VPN for cryptographic aims use both the public-key and symmetric cryptography to achieve the confidentiality and authentication/integrity. Public-key mechanisms support key exchange or agreement, and authenticate the endpoints. Symmetric mechanisms (e.g., 3DES, SHA1) provide traffic confidentiality and integrity. Thus VPN systems can provide confidentiality and authentication/integrity without trusting the public network interconnecting VPN sites.

To implement VPN using quantum techniques, one may have at least two approaches. The first approach which has been adopted by the research group supported by the DAPPA project is as follows [**?**]. The existing VPN key agreement primitives may be augmented or completely replaced by keys provided by quantum cryptography, while the remainder of the VPN construct is left unchanged. This has been shown in Fig.9.20. In this way, the built QKD-secured network is fully compatible with conventional Internet hosts, routers, firewalls, and so forth. Of course, one may use the second approach. As that in the first approach, the key exchange protocols, cryptographic algorithm, and authentication algorithm are all is associated with the quantum techniques. These have been introduced in Chapters 4 – 6. Thus, the built quantum IP network may be employed in a high efficiency. In addition, the security and efficiency are obviously improved.

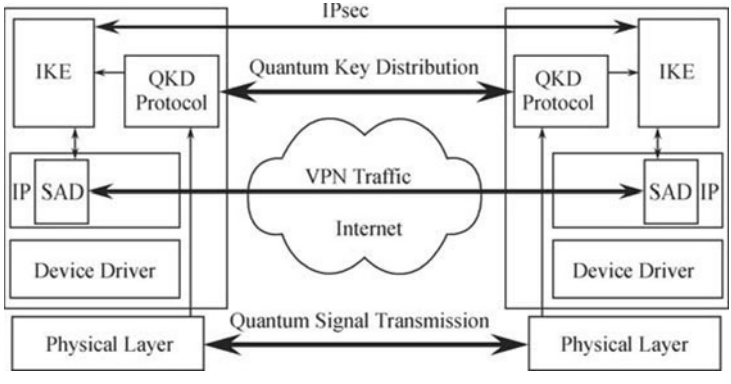

Fig. 9.20. Architecture for VPN based on quantum cryptography

9.6 Applications in Mobile Communication

Mobile communication networks require a high level of security. To fulfill these requirements end-to-end, mobile network vendors implement state-of-the-art security technologies from mobile phone trough radio links, core networks, and back-office systems. Some well-known companies, e.g., Siemens communication's mobile networks division, have recently reviewed the applicability of quantum cryptography for securing its networks and solutions. Especially, the application of QKD techniques in the mobile communication networks has attracted attention of the European telecommunication standard institute (ETSI). This section analyzes some possible applications of the quantum private communication in mobile communication networks.

1) Random Number Generation for Algorithmic Cryptography

Random numbers play important role in modern communication, especially in the secure communication system. Subsequently, the random number generation (RNG) has become an important issue in the private communication. For example, the key management system depends on the random generation. Currently, random numbers are generated using computers and other electron devices, however, these generations are often overlooked. Being deterministic, computers and other electron devices are not capable of producing truly random numbers. Accordingly, a physical source of randomness is necessary.

Quantum physics being intrinsically random, it is natural to exploit a quantum process for such a source. Quantum RNG have the advantage over conventional randomness sources of being invulnerable to environmental perturbations and of allowing live status verification. Based on quantum laws, a practical random generator, called Quantis, has been invented in id Quantique Company, and it has become commercial availability. The Quantis is a physical random number generator exploiting an elementary quantum optics process. Photons are sent one by one onto a semi-transparent mirror and detected. Exclusive events (reflection-transmission) are associated to "0" and "1" bit values. The operation of Quantis is continuously monitored to ensure immediate detection of a failure and disabling of the random bit stream.

The algorithmic cryptography and quantum cryptography are often perceived as alternatives, there are also synergies. A good example is the usage of quantum physical random generators in combination with cryptographic algorithms. In contrast to algorithms, such quantum physical random generators provide a perfect solution for generating random numbers required for the generation of cryptographic keys. Due to the commercial availability of such products, that technology is ready to use. This paves a road for application of the quantum random generation on the secure mobile communication system. For example, random number generation is often exploited in the wireless public key infrastructure (WPKI) for generating a random string.

2) Wired Equivalency Privacy with QKD

Wireless security is becoming increasingly important as wireless applications and systems are widely adopted. Wireless local area networks (WLAN) are based on the IEEE 802.11 standard. A series of standards under the

IEEE 802.11 have been used in our daily life, such as the IEEE 802.11a, IEEE 802.11b, and IEEE 802.11g. A number of impressive attacks are possible and have been heavily publicized, especially in the the IEEE 802.11b area. Wired Equivalency Privacy (WEP) is part of IEEE 802.11b. Since the leak of this protocol, WEP is completely broken and offers very little real security. QKD shows a great future in wireless security. An example of QKD for Wi-Fi networks security has been presented in Ref.[**?**]. Fig.9.21(a) shows the pairwise key hierarchy containing keys related to the encryption of unicast traffic. At the top level there is the master key titled pairwise master key (PMK) that is used to derive the other keys. The pairwise transient key (PTK) is created between the access point and the mobile terminal during the 4-way handshake. The PTK is split into three final temporal keys, namely key confirmation key (KCK), key encryption key (KEK), and temporal key (TK). Fig.9.21(b) is the framework of QKD technology works with Wi-Fi. The hierarchy is split into two parts and the right part works under the B92 protocol. The KCK is generated from the PMK to serve the mutual authentication of the supplicant and the authenticator and protect the B92 protocol from the Main-in-the-middle attack as described in Ref.[**?**]. Once the mutual authentication finished, the supplicant and authenticator start the B92 protocol for the establishment of the quantum PTK. The quantum PTK is splits into the KEK and TK. In this hierarchy QKD is used to establish the PMK, therefore all KEK, KCK, and TK are established using the involved QKD scheme.

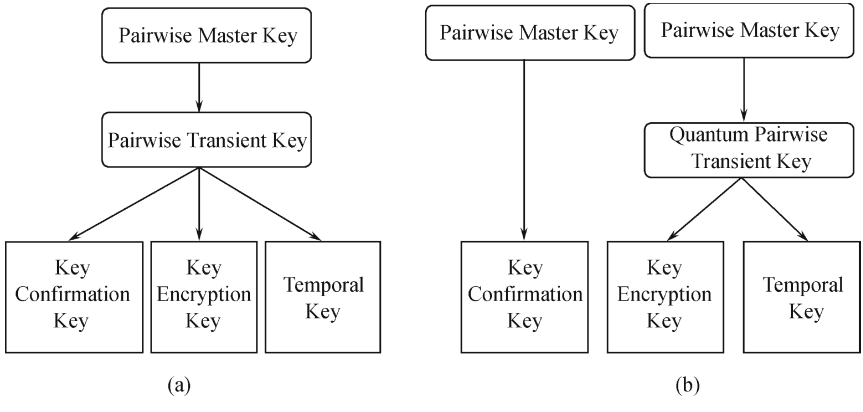

Fig. 9.21. Hierarchy of QKD in Wi-Fi Networks

(a) Pairwise key hierarchy; (b) Quantum handshake framework for B92 protocol with Wi-Fi

3) QKD-enhanced VPNs

As addressed in Section 9.5.2, QKD-enhanced VPNs over IP network has been implemented by researchers in BBN, Harvard university and Boston university. Mobile communication network is also associated with the VPN in many systems. Accordingly, one may foresee a broad range of application scenarios in mobile networks, where network security will benefit from

quantum security technologies, mainly as a replacement for dedicated connections by VPNs enhanced by QKD. Of course, in mobile networks, the adoption of such innovations will depend on the security requirements, cost considerations for technologies with comparable performance, and maturity of quantum computing.

Within the core of mobile networks, there are several systems included such as the large data base system with large amounts of subscriber data, e.g., the 2G home location register (HLR) or the home subscriber service (HSS) of 3GPP. The availability of HSS is critical for the operation of mobile networks. Mirroring of HSS data is one option to improve its availability. A classical HLR consists of 2 clusters, each holding about 50% of subscriber records, with typically 60 GB of data per HLR. Such a "mated pair" is located in geographically different locations, e.g., within a metropolitan area. The mated pairs have to be synchronized for any changes. Technically, synchronization should be performed in a duration, e.g., every 15 minutes. Security requirements regarding confidentiality and integrity are high in this scenario. To reach these aims keys with high security should be exploited. Obviously, it provides a changes for employing QKD in this scenario for interconnecting subscriber data bases. Especially, for inter-urban distances the data rates fit well with the QKD performance already available, therefore, the commercial feasibility depends mainly on the security requirements and cost/performance ratio in comparison to classical VPN solutions. Of course, improvements for inter-urban distances regarding QKD data rates may be necessary, depending on the security requirements and the resulting frequency of key exchange. For example, if the AES is employed the current key rate of QKD is available, while if the one-time pad is used the key rate of the current QKD system should be improved further.

Another application scenario for QKD-enhanced VPNs is the transport of accounting and charging information from a national mobile communication network to its back-office billing systems. Both the subscriber and the network operator require correct, timely processing of these data, so the security, e.g., integrity, proof-of-origin, etc., of charging data is critical. One method for the transport of charging tickets relies on FTP push or pull, with typical data sets comprising around 100 kbit/s. FTP pull is required with a frequency from once per day/week up to once per 10 minutes. Today, cost/performance ratio of QKD and the distances between national nodes of the mobile network still limit the commercial feasibility. As soon as distances of some hundred kilometers are supported, this becomes a potential application scenario for QKD.

Quite often, the partners communicating with their mobile phones are customers in different mobile networks. So there are interconnections necessary between these networks. Typical data here include data rates per individual connection of between 30 and 180 kbit/s, depending on the type of content (voice/data) partly with strict real-time requirements. Per million subscribers some 10.000 inter-network connections have to be supported. Given the global/nation-wide distances between single networks, the amount of connections which require separate, individual protection, and the realtime requirements for voice, this application scenario poses some extra requirements for QKD.

9.7 Limitations on Availabilities

Previous sections have introduced three typical network architectures for the quantum private communication, i.e., fiber-based, space-based, and IP networks. These architectures can be employed independently in practices or as basic elements for constructing larger communication network. When they are employed as basic elements a globe quantum private communication network becomes possible in principle.

Currently, some practical quantum private communication network systems have being presented. In October 2003, BBN Technologies set up a primitive but pioneering QKD network in Cambridge, Massachusetts, linking their site with Harvard University and Boston University. The firm showed that it was possible to direct the stream of single photons between different receiving units using an optical switch, and it also introduced the idea of "key relay" along a chain of trusted nodes. Here, each pair of adjacent nodes in the chain stores its own local key. A global key may then be sent from one end of the chain to the other, over any distance, by using the local keys and a one-time pad to encrypt each hop. A more sophisticated system is currently under development by the European SECOQC consortium, a collaboration of academic and industrial QKD researchers, classical cryptographers and telecoms engineers. It is developing the protocols required for routing, storage and management of keys within a meshed network that could in principle be very large. A trial implementation of the quantum network is executing that will allow any two users at several sites across Vienna to establish a shared key.

Of course, to go forward from current demonstrations of the two-users quantum private communication system to a globe network architecture, some important issues need to be addressed. They are actually the problems or challenges in the current availabilities of quantum private communication systems. Its current constraints, both regarding technological aspects, e.g., distance and data rate, and the rather high cost of its first commercial products, limit still its practical applicability.

9.7.1 Limitations on Communication Systems

Currently, availabilities of the quantum private communication still suffer from some limitations on communication technologies in quantum scenarios. These are associated with the quantum signal source, transmission distance, key rate of QKD, devices employments, drawbacks on the networks and quantum computing techniques, etc. The following demonstrates these limitations using a QKD system.

One of the main goals of the ongoing scientific work of QKD is to increase the distance and rates of single links, especially in the fiber-based scenario. In space-based quantum private communication system a very long distance of 1485 km has been implemented. However, although the 200 km QKD experiment in fiber provides a possibility for implementing the quantum private communication in metropolitan area network (MAN), but single links

in fiber for backbone transmissions which may be several hundred kilometers or even thousand kilometers keep a challenge. With the help of amplifiers, the distance of classical communication can be increased by restoring the amplitude of signals. Contrarily, quantum signals are not able to be amplified due to the fundamental reasons that ensure security. Nevertheless another method is in principle possible to increase the transmission distances: quantum repeater on the basis of entanglement swapping.

For example, if a station A would again like to communicate with a station B, but the distance would be slightly too long for a single link, it is possible to distribute two entangled pairs ($|\psi\rangle_{a_1b_1}$ and $|\psi\rangle_{a_2b_2}$) to them. The photon a_1 from the first pair would be received at the station A and the photon b_2 from the second pair at the station B. Both remaining pair photons (b_1 and a_2) would need to be saved in quantum memories in a repeater station C in between. If both pairs would be distributed independently, then a joint measurement of b_1 and a_2 could give an outcome that is needed that the measurement of a_1 at the station A and b_2 at the station B is formed to a common key without loosing security since b_1 and a_2 have formed an resulted entangled state $|\psi\rangle_{a_2b_1}$ after b_2 and a_1 are jointly operated at the station C. In this way, it is possible to have more than one repeater in between A and B. The basic principle of the quantum repeater has been described in Section 7.2.2.

Using of many quantum repeaters may construct naturally a quantum network. Like in classical communications where single link between stations is mostly not the most economic way of connecting also in quantum networks there are a lot of possibilities. One possibility is that the existing fiber infrastructure can be used to define a network called quantum-classic multiplexing (QCM) network. Due to different topologies in existing mesh- and ring-structures one must construct very universal QCM architectures. Because this needed infrastructure is maybe not available in the physical stations of fiber networks anyhow, it is maybe preferable to build up a QCM network starting from scratch. Then also considerations of efficiency of links and different QKD systems can be included. However, in such QCM network all nodes must be trusted when it is used for the aim of QKD, because these keys should be stored typically in embedded electronics. This main disadvantage can be explained that if a sender A and a receiver B would be connected via a network to each other, then a key is exchanged between the QCM network and sender A and also another one between the QCM network and receiver B. The network has both keys and so the full information of the secrets between A and B. Thus, the network needs to be trusted. Certainly, this way is inconvenient in practices. With quantum repeaters a real quantum network may be defined. In contrast to the QCM network all of nodes in a quantum network don't need to be trusted, because there is no quantum information transferred into classical bits. However, a long-life-quantum memory is necessary in this case. Recent developments such as a semiconductor device for generating entangled photon pairs and the teleportation of quantum states between photons and atoms bring the quantum repeater closer to becoming a reality. However, it is still far away from the practical application.

Another problem is the high efficiency detection of quantum signals such as single photons or coherent state laser pulse at a typical communication

wavelength of 1310 nm or 1550 nm. The maximal distance of any QKD system (even with perfect sources) is approximately given, when the incoming photons are roughly in the order of the noise of the detector due to dark counts and after-pulsing effects. The number of incoming photons is limited by the loss of the transmission system and the production rate of the source. Unfortunately the latter value cannot longer be increased, because the used detectors are needed to be gated with a maximal rate of $4-10$ MHz when single photon signal has been income. This problem can be solved currently in two ways. One is using new technology such as the superconducting single photon detector which has been described in Chapter 7. Another way is using the wavelength conversion approach. This is a research focus in quantum communication. The single photon is converted from 1310 nm or 1550 nm to a wave-length that is possible to detect by some avalanche photo diodes in the visible or near infrared. These devices have a very high detection efficiency of $> 65\%$ (instead of $> 10\%$ for 1550 nm) and also don't need to be gated. There low back ground is very preferable for long-distance demonstrations. Even in that first demonstration a secure key rate of 20 kHz over a distance of 50 km was presented. Another advantage is the possibility of the transfer to a wavelength that could be used for Ion-traps to act as a quantum memory and to store a single photon. This is a pre-requisite for future quantum repeaters. However, both approaches are yet not available in practice.

Most of the actual propositions for provably secure pairwise QKD over optical fibre (both with and without entanglement) require stable fibre interferometers. Stability can be achieved either with active compensation, a cumbersome task, or with passive compensation, as in the plug & play scheme. However, this is done at the expense of reducing the security level in a way which remains debated. For a network to be scalable, passively stabilized interferometers that do not threaten the security are required. These interferometers need much improvement in thermal and mechanical stability before they can be deployed in networks.

The problem of the key rate in the QKD scheme has been described in previous. Although it is possible to combine the QKD and most of classic cryptographic algorithms such as AES, the current key rate of the QKD procedure is not suitable for the one-time pad. While the later is just the initial motivation of investigating the QKD.

9.7.2 Limitations on Security

Of the cryptographic algorithms in practical use today, most rely on the fact, that it is computationally hard to find the secret key; such algorithms are rated as the computational security. But during its evolution cryptography has often found weak spots in cryptographic algorithms or their implementations. Unconditionally secure cryptographic algorithms, which have been proven secure independent of the computing power of an adversary, are an alternative to fulfill very high security requirements.

Assuming that the understanding on quantum physics is correct, and assuming perfect implementation, then QKD has been proven to be unconditionally secure. But QKD alone does not provide a secure communica-

tion system in the practical private communication. As described before, two more requirements have to be fulfilled to enable secure communications are authentication which ensures proof of origin and message integrity and message encryption which warrants the confidentiality. In classic cryptography, there is only one unconditionally secure method for encryption, namely the Vernam cipher or modulo 2 one-time pad, requiring keys as long as the message. For authentication, there are unconditionally secure message authentication codes of Wegman-Carter, requiring a pre-established key. This is also required for all other symmetric-cryptography based authentication methods. Accordingly, it is possible to extend QKD to an unconditionally secure communication system even secure against attacks by quantum computers, but at a certain price. However, only simple combinations of a QKD scheme and a classic one-time pad (or Vernam cipher) or authentication scheme are not always secure in spite of these employed schemes are unconditionally secure when they are independently employed, since an inadequate combination of two cryptographic modules might result in new security problems in itself.

Very powerful attacks to a single QKD link are the Man-in-the-middle attack and denial of service (DOS) attack. If a sender A and a receiver B would like to communicate with each other, but the adversary E changes the situation that A and E build up a secret key, and also E and B another one, then he acts like the Man in the middle of the communication. Quantum cryptography alone is not able to resist this attack. As in classical considerations, only if A and B use a pre-shared secret to authenticate some needed messages in the quantum protocol before a new secret can be established, then the adversary E is unable to perform this Man-in-the-middle attack. On the other hand, this attack leads to a reduction of this pre-shared secret and the adversary could continue his attack until no secret is left. The stations A and B could not restart the quantum link any longer. This "denial of service attack" for that link is impossible in quantum networks, if there is more than one possible connection between A and B. The stations A and B would be able to exchange a new shared secret between them over the remaining network that has not been tampered by the adversary. But in the two-party communication with a single link, the DOS attack is available in the quantum private communication. Of course, one could adopt the classic approaches to solve this problem.

References

[1] Schneier B (1994) Applied cryptography: protocols, algorithms, and source code in C. Wiley, New York

[2] Corndorf E, Barbosa G, Liang C, et al (2003) High-speed data encryption over 25 km of fiber by two-mode coherent-state quantum cryptography. Optics Letters, 28(21): 2040 – 2042

[3] Townsend P D (1997) Quantum cryptography on multi-user optical fibre networks. Nature, 385: 47 – 49

[4] Townsend P D (1998) Experimental investigation of the performance limits for first telecommunications-window quantum cryptography systems. IEEE Photonics Technology Letters, 10:(7) 1048 – 1050

[5] Stucki D, Gisin N, Guinnard O, et al (2002) Quantum key distribution over 67 km with a plug&play system. New Journal of Physics, 41(4):1 – 8

[6] Gordon K J, Fernandez V, Townsend P D, et al (2004) A short wavelength gigahertz clocked fiber-optic quantum key distribution system. IEEE Journal of Quantum Electronics, 40: 900 – 908

[7] Gobby C, Yuan Z L, Shields A J (2004) Quantum key distribution over 122 km of standard telecom fiber. Applied Physics Letters, 84: 3762 – 3764

[8] Tang X, Ma L, Mink A, et al (2006) Experimental study of high speed polarization-coding quantum key distribution with sifted-key rates over Mbit/s. Optics Express, 14: 2062 – 2070

[9] Fernandez V, Collins R J, Gordon K J, et al (2007) Passive Optical Network Approach to GigaHertz-Clocked Multiuser Quantum Key Distribution. IEEE Journal of Quantum Electronics, 43(2): 1 – 9

[10] Rarity J, Tapster P, Gorman P (2001) Secure free-space key exchange to 1.9 km and beyond. Journal of Modern Optics, 48: 1887

[11] Rarity J G, Tapster P R, Gorman P M, et al (2002) Ground to satellite secure key exchange using quantum cryptography. New Journal of Physics, 4: 82

[12] Hughes R J, Nordholt J E, Derkacs D, et al (2002) Practical free-space quantum key distribution over 10 km in daylight and at night. New Journal of Physics, 4: 43

[13] Kurtsiefer C, Zarda P, Halder M, et al (2002) A step towards global key distribution. Nature, 419: 450

[14] Aspelmeyer M, Jennewein T, Pfennigbauer M, et al (2003) Long-distance quantum communication with entangled photons using satellites. IEEE Journal of Selection Topics on Quantum Electron, 9: 1541

[15] Aspelmeyer M, Böhm H R, Gyatso T, et al (2003) Long-distance free-space distribution of quantum entanglement. Science, 301: 621 – 623

[16] Resch K, Lindenthal M, Blauensteiner B, et al (2005) Distributing entanglement and single photons through an intra-city, free-space quantum channel. Optics Express, 13: 202 – 209

[17] Peng C Z, Yang T, Bao X, et al (2005) Experimental free-space distribution of entangled photon pairs over 13 km: towards satellite-based global quantum communication. Physical Review Letters, 94: 150501

[18] Ursin R, Tiefenbacher F, Schmitt-Manderbach T, et al (2007) Free-space distribution of entanglement and single photons over 144 km. Nature Physcs, 3: 481 – 486

[19] Pfennigbauer M, Aspelmeyer M, Leeb W R, et al (2005) Satellite-based quantum communication terminal employing state-of-the-art technology. Journal of Optics Networking, 4: 549 – 560

[20] Elliott C (2002) Building the quantum network. New Journal of Physics, 4: 46.1 – 46.12

[21] Curcic T, Filipkowski M E, Chtchelkanova A, et.al (2004) Quantum networks: From quantum cryptography to quantum architecture. ACM SIGCOMM Computer Communication Review, 34(5): 3 – 8

[22] Rass S, Sfaxi M A, Hélie S G, et al (2008) Secure message relay over networks with QKD-Links. Second International Conference on Quantum, IEEE Nano and Micro Technologies, Sainte Luce, Martinique, 10 – 15 February, pp 10 – 15

[23] SECOQC—Development of a global network for secure communication based on quantum cryptography. EU Sixth Framework Programme. http://www.secoqc.net/. Accessed 10 August 2009

[24] Marhoefer M, Wimberger I, Poppe A. Applicability of quantum cryptography for securing Mobile communication networks. http://citeseerx.ist.psu.edu/. Accessed 1 August 2009

[25] Bennett C H, Bessette F, Brassard G, et al (1992) Experimental quantum cryptography. Journal of Cryptology, 5: 3 – 28

[26] Idquantique. www. idquantique. com. Accessed 1 August 2009

[27] Takesue H, Nam S W, Zhang Q, et al (2007) Quantum key distribution over a 40-dB channel loss using superconducting single photon detectors. Nature Photonics, 1: 343 – 368

[28] Villoresi P, Jennewein T, Tamburini F, et al (2008) Experimental verification of the feasibility of a quantum channel between space and Earth. New Journal of Physics, 10: 1 – 12

[29] Shields A, Yuan Z (2007) Key to the quantum industry. Physics World, March: 24 – 29

[30] MagiQ Company. www.magiqtech.com. Accessed 1 August 2009

[31] SmartQuantum. http://www.smartquantum.com/. Accessed 1 August 2009

[32] Neumann E G (1988) Single-mode fibers. Springer, New York

[33] Imoto N, Yoshizawa N, Sakai J, et al (1980) Birefringence in single-mode optical fiber due to elliptical core deformation and stress anisotropy. IEEE Journal of Quantum Electronics, 16(11): 1267 – 1271

[34] Foschini G J, Poole C D (1991) Statistical theory of polarization dispersion in single mode fibers. Journal of Lightwave Technology, 9(11): 1439 – 1456

[35] Gisin N (1995) Statistics of polarization dependent losses. Optics Communications, 114 (5): 399 – 405

[36] Rothman L S, Rinsland C P, Goldman A, et al (1998) The HITRAN molecular spectroscopic database and HAWKS. Journal of Quantitative Spectroscopy & Radiative Transfer, 60: 665 – 710

[37] Fante R L (1975) Electromagnetic beam propagation in turbulent media. Proceedings of the IEEE, 63(12): 1669 – 1692

[38] Boroson D M (1993) Overview of lincoln laboratory development of lasercom technologies for space. Proceedings of SPIE, 1866: 30 – 39

[39] Corndorf E, Liang C, Kanter G S, et al (2004) Quantumnoise — protected data encryption for WDM fiberoptic networks. ACM SIGCOMM Computer Communications Review, 34(5): 21 – 30

[40] Acín A, Cirac J I, Lewenstein M (2007) Entanglement percolation in quantumnetworks. Nature Physics, 3: 256 – 259

[41] Kumavor P D, Beal A C, Yelin S (2005) et al. Comparison of Four Multi-User Quantum Key Distribution Schemes Over Passive Optical Networks. Journal of Lightwave Technology, 23(1): 268 – 276

[42] Nishioka T, Ishizuka H, Hasegawa T, et al (2002) "Circular type" quantum key distribution. IEEE Photonic Technology Letters, 14(4): 576 – 578

[43] Giovannetti V, Lloyd S, Maccone L (2001) Quantum-enhanced positioning and clock synchronization. Nature, 412(26): 417 – 419

[44] Strohbehn J W (1978) Laser beam propagation in the atmosphere. Spinger, Heidelberg, pp 45 – 106

[45] Driscoll W G, Vaughan W (1978) Handbook of optics. McGraw-Hill, New York

[46] Huang X, Sharma D (2009) An agent-oriented quantum key distribution for Wi-Fi network security. Lecture Notes in Computer Science (LNCS), Springer, Heidelberg, 5179: 227 – 235

[47] Nguyen T M T, Sfaxi M A (2006) Ghernaouti-Hélie S. 802.11i Encryption key distribution using quantum cryptography. Journal of Networks, 1(5): 9 – 20

Index

R

S

T

U

V

W

X