

UNIVERSITY OF OKLAHOMA

GRADUATE COLLEGE

FAST CONVERGENT AND SECURE KEY DISTRIBUTION PROTOCOLS

USING A DUAL-QUANTUM CHANNEL

A DISSERTATION

SUBMITTED TO THE GRADUATE FACULTY

in partial fulfillment of the requirements for the

Degree of

DOCTOR OF PHILOSOPHY

By

DI JIN

Norman, Oklahoma

2008

FAST CONVERGENT AND SECURE KEY DISTRIBUTION PROTOCOLS
USING A DUAL-QUANTUM CHANNEL

A DISSERTATION APPROVED FOR THE
SCHOOL OF ELECTRICAL AND COMPUTER ENGINEERING

BY

Dr. Stamatios V. Kartalopoulos, Co-Chair

Dr. Pramode K. Verma, Co-Chair

Dr. Samuel Cheng

Dr. William O. Ray

Dr. James J. Sluss, Jr.

© Copyright by DI JIN 2008
All Rights Reserved.

Dedication

To my family.

Acknowledgements

I would like to sincerely thank my co-advisors, Dr. Stamatios V. Kartalopoulos and Dr. Pramode K. Verma for their guidance and encourage throughout my doctoral study. Without their help, I would not have been able to complete my Ph.D.

I am very grateful to the respected members of my doctoral committee, Dr. Samuel Cheng, Dr. William O. Ray, and Dr. James J. Sluss, Jr. for their valuable comments and suggestions.

I also want to express my special thank to Ms. Renee Wagenblatt for her warmhearted help in improving my English in the past three years, as well as my officemate Christella Chavez, and all the other people at OU-Tulsa who have ever helped me.

Finally, I would like to thank my wife, my parents, my parents-in-law, and my brother, for their constant support, encourage, and understanding. It is because of them that I have been so successful.

Table of Contents

| | |
|--|-----------|
| Dedication..... | vii |
| Acknowledgements | iv |
| Table of Contents | v |
| List of Tables | xi |
| List of Figures..... | xii |
| Abstract..... | xiv |
| Chapter 1 Introduction | 1 |
| 1.1 A Brief History of Cryptography | 2 |
| 1.2 Information Security Becomes a Crucial Concern | 6 |
| 1.3 Quantum Computers and Quantum Algorithms..... | 8 |
| 1.4 Contributions of this Dissertation..... | 9 |
| 1.5 Organization of this Dissertation..... | 11 |
| Chapter 2 Conventional Cryptography..... | 14 |
| 2.1 Symmetric Cryptography | 15 |
| 2.1.1 Data Encryption Standard..... | 16 |
| 2.1.2 Advanced Encryption Standard..... | 17 |
| 2.1.3 RC4 Algorithm | 18 |
| 2.1.4 One-Time Pad..... | 19 |
| 2.2 Asymmetric Cryptography | 20 |
| 2.2.1 RSA Algorithm..... | 21 |

| | |
|---|-----------|
| 2.2.2 Elliptic Curve Cryptography | 23 |
| 2.2.3 Diffie-Hellman Key Exchange | 24 |
| 2.3 Conditional Security of Conventional Cryptography..... | 25 |
| 2.4 Summary..... | 27 |
| Chapter 3 Quantum Cryptography and Quantum Key Distribution | 28 |
| 3.1 Introduction | 28 |
| 3.1.1 Polarization of Light..... | 29 |
| 3.1.2 Classical Bit and Quantum Bit | 31 |
| 3.2 Basis of Quantum Cryptography | 33 |
| 3.2.1 Heisenberg Uncertainty Principle..... | 33 |
| 3.2.2 No-Cloning Theorem..... | 34 |
| 3.2.3 Quantum Measurement | 36 |
| 3.2.4 Quantum Entanglement | 38 |
| 3.3 Unconditional Security of Quantum Cryptography | 39 |
| 3.4 Major Quantum Key Distribution Protocols | 41 |
| 3.4.1 Polarization-Based Quantum Key Distribution Protocol | 41 |
| 3.4.1.1 Four Polarization States of a Photon | 42 |
| 3.4.1.2 Rectilinear Basis and Diagonal Basis..... | 42 |
| 3.4.1.3 Measuring Polarized Single Photons with a Polarizing Beam Splitter | 43 |
| 3.4.1.4 Representation of Classical Bits by Polarized Single Photons... | 47 |

| | |
|--|-----------|
| 3.4.1.5 Schematic Diagram of the Structure of the BB84 Protocol | 48 |
| 3.4.1.6 Assumptions of the BB84 Protocol | 49 |
| 3.4.1.7 Steps to Share a Raw Key in the BB84 Protocol..... | 50 |
| 3.4.1.8 Information Reconciliation and Privacy Amplification Procedures | 53 |
| 3.4.1.9 Weaknesses of the BB84 protocol..... | 55 |
| 3.4.2 Entanglement-Based Quantum Key Distribution Protocol | 57 |
| 3.4.3 Other Major Quantum Key Distribution Protocols | 59 |
| 3.5 Quantum Key Distribution in Practices..... | 60 |
| 3.6 Summary..... | 61 |
| Chapter 4 Key Distribution Using a Dual-Quantum Channel..... | 63 |
| 4.1 Introduction | 63 |
| 4.2 Dual-Quantum Channel Structure | 63 |
| 4.3 Complementary Measuring Bases | 64 |
| 4.4 The Proposed Protocol | 66 |
| 4.5 Raw Key Efficiency, Final Key Efficiency, and Raw Key Error Rate | 69 |
| 4.6 Raw Key Efficiency and Raw Key Error Rate in Different Scenarios with or without the Presence of Eve..... | 70 |
| 4.6.1 Eve is not Present on Either of the Two Quantum Channels | 71 |
| 4.6.2 Eve is Present on One of the Two Quantum Channels | 72 |
| 4.6.3 Eve is Present on Both of the Two Quantum Channels | 74 |

| | |
|--|-----------|
| 4.7 Making Use of the Difference between the Two Raw Key Error Rates on the Two Quantum Channels to Speed up the Key Distribution Process and Frustrate Eve..... | 75 |
| 4.8 Making Use of an Initialization Vector Shared between Alice and Bob to Improve the Convergence Speed of the Final Key and Frustrate Eve..... | 77 |
| 4.9 Security Analysis and Solutions..... | 79 |
| 4.10 Comparison to the BB84 Protocol..... | 83 |
| 4.10.1 Differences between the Proposed Protocol and the BB84 Protocol | 83 |
| 4.10.2 Performance Comparison between the Proposed Protocol and the BB84 Protocol | 84 |
| 4.11 Conclusion..... | 85 |
| Chapter 5 Quantum Key Distribution Using a Novel Basis Selection Rule | 87 |
| 5.1 Introduction | 87 |
| 5.2 A Novel Basis Selection Rule on the Dual-Quantum Channel | 88 |
| 5.3 The Proposed Protocol | 89 |
| 5.4 Raw Key Efficiency | 91 |
| 5.5 Raw Key Error Rate | 92 |
| 5.5.1 Eve is not Present on either of the Two Quantum Channels..... | 93 |
| 5.5.2 Eve is Present on One of the Two Quantum Channels | 93 |
| 5.5.3 Eve is Present on both of the Two Quantum Channels..... | 93 |

| | |
|--|------------|
| 5.6 Three Ways to Obtain the Final Key | 94 |
| 5.7 Two Ways to Frustrate Eve’s Attack..... | 97 |
| 5.9 Conclusion..... | 98 |
| Chapter 6 Quantum Key Distribution without Basis Information Exchange and the Usage of the Conventional Channel | 100 |
| 6.1 Introduction | 100 |
| 6.2 Roles of the Conventional Channel..... | 100 |
| 6.3 The Proposed Protocol | 103 |
| 6.4 Raw Key Efficiency and Raw Key Error Rate..... | 106 |
| 6.5 Four Ways to Obtain the Final Key..... | 108 |
| 6.6 Two Ways to Frustrate Eve’s Attack..... | 109 |
| 6.7 Real-Time Detection Mechanisms of Eve’s Presence during the Key Distribution Process..... | 110 |
| 6.8 Eliminating the Basis Information Exchange between Alice and Bob on the Conventional Channel | 113 |
| 6.9 Eliminating the Necessity of the Conventional Channel in the Structure | 114 |
| 6.10 Conclusion..... | 115 |
| Chapter 7 Defense Mechanisms to Eve’s Attack..... | 117 |
| 7.1 Introduction | 117 |
| 7.2 Several Techniques to Frustrate Eve’s Attack..... | 118 |

| | |
|--|------------|
| 7.2.1 Changing the Representation of Bits by Polarized Single Photons. | 118 |
| 7.2.2 Using the Decoy Quantum Channel to Transmit Fake Information | 119 |
| 7.2.3 Locating the Two Quantum Channels in Different Optical Fibers or Optical Fiber Cables | 120 |
| 7.2.4 Assigning the Two Quantum Channels with Different Wavelengths | 121 |
| 7.2.5 Using the Initialization Vector Shared between Alice and Bob | 123 |
| 7.2.6 Transmitting the Initialization Vector in a Random Manner | 123 |
| 7.2.7 Introducing a Random Delay between the Transmissions on the Two Quantum Channels | 124 |
| 7.3 Integrated Defense Mechanism to Eve’s Attack | 124 |
| 7.4 Conclusion | 125 |
| Chapter 8 Conclusions and Future Work | 126 |
| 8.1 Conclusions | 126 |
| 8.2 Future Work..... | 131 |
| Bibliography | 133 |
| Appendix | 142 |
| List of Publications..... | 142 |

List of Tables

| | |
|---|-----|
| Table 1.1 Security incident reports received by CERT | 7 |
| Table 3.1 Representation of classical bits by polarized single photons | 48 |
| Table 3.2 An example of the BB84 protocol | 51 |
| Table 4.1 Bob's complementary measuring bases used on the dual-quantum channel | 65 |
| Table 4.2 An example of the proposed protocol | 69 |
| Table 4.3 The maximal raw key error rate Eve can bring into the raw key is 25% when Eve eavesdrops on all the qubits transmitted on a quantum channel | 73 |
| Table 4.4 Comparison of the raw key error rate in different scenarios between the BB84 protocol and the proposed protocol | 85 |
| Table 5.1 Basis selection on the dual-quantum channel according to the value of the initialization vector shared between Alice and Bob | 89 |
| Table 5.2 An example of the proposed protocol | 91 |
| Table 6.1 Selection of bases on the two quantum channels according to the bit value of the initialization vector shared between Alice and Bob | 104 |
| Table 6.2 An example of the proposed protocol | 106 |
| Table 7.1 Four different representations of bits by polarized single photons | 119 |

List of Figures

| | |
|---|----|
| Figure 1.1 The Mesopotamian clay tablet and envelope | 3 |
| Figure 1.2 A scytale | 4 |
| Figure 2.1 The structure of conventional cryptosystems | 15 |
| Figure 3.1 Polarization of light | 30 |
| Figure 3.2 Four polarization states of a photon | 31 |
| Figure 3.3 A general quantum state | 33 |
| Figure 3.4 Measuring a 45° polarization state along the horizontal or vertical direction | 37 |
| Figure 3.5 Four basic polarization states of a single photon | 42 |
| Figure 3.6 Rectilinear basis and diagonal basis | 43 |
| Figure 3.7 Measuring a vertically polarized single photon and a horizontally polarized single photon using a PBS with a vertical polarization axis | 44 |
| Figure 3.8 Measuring a 45° polarized single photon using a PBS with a vertical polarization axis | 45 |
| Figure 3.9 Measuring a qubit with a 45° or 135° polarization state with a PBS with a vertical polarization axis (with the aid of a 45° polarization rotator) | 46 |
| Figure 3.10 Schematic diagram of the structure of the BB84 protocol | 48 |
| Figure 3.11 Schematic diagram of the structure of the E91 protocol | 58 |
| Figure 4.1 Schematic diagram of the structure of the proposed protocol | 64 |

| | |
|---|-----|
| Figure 4.2 Transmitting decoy information on the quantum channel on which Eve is actively eavesdropping while sending real information on the other quantum channel on which Eve is not eavesdropping | 77 |
| Figure 4.3 Obtaining the final key by XORing the sifted key with the initialization vector shared between Alice and Bob | 78 |
| Figure 4.4 Comparing the raw key error rate with the preset threshold to decide whether a raw key should be kept or discarded | 81 |
| Figure 5.1 Schematic diagram of the structure of the proposed protocol | 87 |
| Figure 5.2 Distilling the final key from the raw key by going through the information reconciliation and privacy amplification procedures | 94 |
| Figure 5.3 Comparing the difference between the two raw key error rates on the two quantum channels and picking the raw key with a lower error rate to obtain the final key | 95 |
| Figure 6.1 Schematic diagram of the structure of the proposed protocol | 103 |
| Figure 6.2 Comparing the measurement results on the two quantum channel to detect whether Eve is eavesdropping | 111 |
| Figure 6.3 Alice transmitting the initialization vector to Bob and Bob comparing the measurement results with the initialization vector to detect whether Eve is eavesdropping | 112 |
| Figure 7.1 Changing the locations of the two quantum channels | 121 |
| Figure 7.2 Assigning different wavelengths to the two quantum channels | 122 |

Abstract

Information security is a crucial concern of modern communication. With the help of cryptography, information can be concealed from undesired people. However, conventional cryptography only provides conditional security, which tends to be broken by the increasing computational power people can get nowadays.

Quantum key distribution was invented in response to the need of unconditional security. It is based on the unbreakable laws of quantum mechanics, which offers the ability to detect the eavesdropper (Eve) during the key distribution process, thus it provides unconditional security.

As the most important quantum key distribution protocol, the BB84 protocol suggested an effective way to establish a secret key between two communicating entities (Alice and Bob); however, it experiences some inherent weaknesses. It has a very low efficiency in getting a raw key and a final key; it takes a long time and much communication and computation overheads to get a short final key; it does not have effective defense mechanisms to defend against Eve; and the conventional channel in the structure indicates a high communication overhead as well as security vulnerabilities.

Aiming at the weaknesses of the BB84 protocol, this dissertation proposes three novel quantum key distribution protocols to improve the efficiency of the key distribution process. By making use of a dual-quantum channel and a novel

basis selection rule, the raw key efficiency is improved from 50% to 100%, which means all the random bits generated by Alice are included into the raw key. The proposed protocols take advantage of the channel diversity brought by the dual-quantum channel to get the final key much faster from the quantum channel with a significantly lower raw key error rate or the eavesdropping-free quantum channel. Eve's attack can be effectively frustrated by sending decoy information on the quantum channel on which Eve is actively eavesdropping. By XORing the sifted key with the initialization vector shared between Alice and Bob, the proposed protocols obtain the final key in a much faster and securer way, and the length of the final key is kept longest possible. This dissertation also presents three real-time detection mechanisms of Eve's presence, which greatly help Alice and Bob defend against Eve's attack. A protocol proposed in this dissertation removes the basis information exchange between Alice and Bob, and further eliminates the necessity of the conventional channel in the structure, which not only reduces the communication overhead and cost dramatically, but also makes the structure all-quantum, presenting less vulnerability to the eavesdropping attack. In addition, the integrated defense mechanism presented in this dissertation provides an effective countermeasure to frustrate Eve's attack.

Chapter 1 Introduction

Ever since the time that people started keeping their own secrets from being public, there had been security concerns. At that time, the secrets were saved in one's brain or written on a material, such as a piece of paper, and then hidden in a secret place. When computers were invented, and especially after the Internet started prevailing in the 1990's, the way people kept their secrets was changed dramatically. Nowadays, secrets are everywhere, flowing on the Internet, through computers, cell phones, telephones, and so on, and literally people are surrounded by secrets all day long. However, most of the secrets do not exist in the form of characters on a piece of paper any more, in which case as long as the physical security of that piece of paper can be guaranteed, the information carried by that piece of paper is secure; instead, the secrets are represented by 0's and 1's, in a digital form, which are later transmitted from place to place. Since the secrets are represented digitally and transmitted between digital devices, how to keep them safe and prevent them from being revealed becomes a big concern, which is the security concern. In the digital age we are living right now, people managed to create many effective security mechanisms to keep secrets secure, and for a period of time those mechanisms worked very well. However, nobody wins all the time in the war of keeping secrets. With currently available and yet developing technologies, those people who are

interested in revealing secrets have gradually gained the ability to achieve their goals. Those security mechanisms that used to be effective at a time are losing their confidence in protecting secrets. However, on the other hand, those people who want to keep the secrecy of the secrets are also working hard to realize their goals. Many researchers have contributed tremendously in every aspect of the field of information security, and many advanced security mechanisms have been proposed and applied. For the past several decades, researchers have been proposing security mechanisms that provide adequate but conditional security suited for the current technologies and people's current needs, while at the same time searching for security mechanisms that can provide unconditional security. In this dissertation, the author is dedicated to providing unconditional communication security and presents the latest research results that will help build unconditional security mechanisms for the future.

1.1 A Brief History of Cryptography

Information security has always been a concern. About 1500 BC ago, the Mesopotamian people wrote a secret recipe in non-standard characters on a clay tablet and enclosed it in a clay envelope [1], Figure 1.1 [2]. If the recipient noticed that the clay envelope was broken when he got it, he knew that somebody had read the clay tablet. However since the information on that clay

tablet was written in some rare, unusual characters, the person who intercepted the clay tablet was not able to read it. This way, the secret of the recipe was kept secure.



Figure 1.1 The Mesopotamian clay tablet and envelope

The ancient Greeks, and the Spartans in particular, are said to have used the “scytale” to communicate during campaigns [3]. A scytale is a tool used to transpose the letters in a message so that people who intercept it can not read it. It consists of a cylinder with a strip of leather wound around it and the message is written on the strip of leather, Figure 1.2 [3]. When people want to deliver a message, they deliver the strip of leather. Because the letters in the message are transposed, it is not intelligible to the enemies. Only the person who has the

cylinder with the same radius can read the message, when he winds the strip of leather around his cylinder.



Figure 1.2 A scytale

Different from the scytale transposition cipher used by the Greeks, which used one of the two core techniques of modern symmetric cryptography, i.e., permutation, Julius Caesar used the other technique, namely, substitution, to encrypt a message. He used the letter that is three positions down in the alphabet to replace a letter in the message, so that the message after encryption is unintelligible to others [4].

During the development of the cryptography, many cryptographic algorithms making use of permutation, substitution, and a single key for encryption have been proposed, such as Monoalphabetic Cipher, Playfair Cipher, Hill Cipher, Polyalphabetic Cipher, One-Time Pad, Data Encryption Standard (DES), Triple

Data Encryption Standard (3DES), Advanced Encryption Standard (AES), RC4, and so on [5]. All these cryptographic algorithms are referred to as the symmetric cryptography, since only one key is used for both encryption and decryption.

Permutation and substitution remained as the core techniques for the symmetric cryptography until the invention of the asymmetric cryptography in 1977 by Ron Rivest, Adi Shamir, and Len Adleman [5], whose algorithm was named RSA [6]. The RSA algorithm was the result of responding to the challenge proposed by Whitfield Diffie and Martin Hellman to invent public-key systems [7]. As an asymmetric cryptography, the RSA algorithm makes use of two keys, one public key and one private key, to encrypt and decrypt messages. The security offered by asymmetric cryptography relies on the infeasibility of currently available computers solving a very difficult mathematical problem within polynomial time, which actually only provides conditional security. With the increasing computational power people can get nowadays, the asymmetric cryptography tends to be broken more easily than before.

The symmetric and asymmetric cryptography are referred to as the conventional cryptography, whose security is computational-difficulty-based. Due to the increasing security breaches, there is an urgent need for a cryptography that can provide unconditional security. In 1984, Charles Bennett and Gilles Brassard invented the first quantum key distribution protocol, the

BB84 protocol [8], which opened the door for the research of quantum cryptography and quantum key distribution. Since then, many researchers have contributed tremendously in this field, and the research of quantum cryptography and quantum key distribution has become a hot topic.

1.2 Information Security Becomes a Crucial Concern

With the popularity of the Internet and the extensive usage of computers for business and personal purposes, a great deal of sensitive information is flowing over the Internet every second. That sensitive information may include business information, trade secrets, social security numbers, credit card numbers, bank accounts, and so on, and the loss of any of which to others would bring very serious aftermaths. Businesses with stolen information may bear extremely expensive losses, which can cause great reductions of revenue, losing competitions to the rivals, and even bankruptcies. The stolen personal information can be used to fake IDs, steal money, commit crimes, and so forth. So it is a very important issue to protect information security.

During the past years, security incidents and breaches have increased dramatically, and more and more people are affected. According to the data recorded by the Computer Emergency Response Team (CERT), the reported

security incidents increased from only 6 times in 1988 to 138 thousand times in 2003, Table 1.1 [9].

Table 1.1 Security incident reports received by CERT

| | | | | | | | | |
|---------------------------|------|------|------|------|------|------|------|------|
| Year | 1988 | 1989 | 1990 | 1991 | 1992 | 1993 | 1994 | 1995 |
| Incident Reports Received | 6 | 132 | 252 | 406 | 773 | 1334 | 2340 | 2412 |
| Year | 1996 | 1997 | 1998 | 1999 | 2000 | 2001 | 2002 | 2003 |
| Incident Reports Received | 2573 | 2134 | 3734 | 9859 | 22k | 53k | 82k | 138k |

According to the reports by the Identity Theft Resource Center (ITRC), in 2005, there were 158 incidents, affecting more than 64.8 million people [10]. In 2006, the number of security breaches increased to 312, affecting nearly 20 million individuals. About 29% of the security breaches were reported by government/military agencies, 28% by educational institutions, 22% by general businesses, 13% by health care facilities/companies, and 8% by banking/credit/financial services entities [11]. In 2007, 446 security breaches were reported, which exposed almost 128 million pieces of records [12].

Information security is becoming a crucial concern, due to the increasing number and severity of the security breaches. People are trying to cope with the security breaches, and are actively seeking effective security mechanisms to

provide better information security. Although many achievements have been accomplished, there is still a long way to dealing with all kinds of security breaches in which more sophisticated attacking techniques are being used.

1.3 Quantum Computers and Quantum Algorithms

People are looking for better security mechanisms; however, at the same time people are searching for more powerful computational machines. A quantum computer [13, 14] is a powerful computational machine to which people have been dedicated for a while. A quantum computer has extremely powerful parallel computational capabilities, and it is considered to be able to break all the computational-difficulty-based conventional cryptographic algorithms. For example, it takes the classical computer $O(N)$ time to solve the unsorted database search problem, however, with Grover's quantum database search algorithm [15], it only takes $O(\sqrt{N})$ time, where N is the number of the entries in the unsorted database. The factorization problem of a very large composite number is extremely difficult to solve using a classical computer. The best known classical algorithm, the General Number Field Sieve Algorithm [16], works in exponential time $O(2^{(\log N)^{1/3}})$, where N is the composite number. In 1994, Peter Shor from AT&T discovered a quantum algorithm that could

factorize a very large composite number N in polynomial time $O((\log N)^3)$ [17], which is exponentially faster than the best known classical algorithm.

The development of quantum computers and quantum algorithms indicates that when people can build quantum computers and have quantum algorithms running on them, breaking the conventional cryptography would be very easy. In this situation, in order to keep information secure, we really need an advanced cryptography, which is not based on computational difficulty, but is based on a totally different idea, which provides unconditional security, and about which even a quantum computer can do nothing. That advanced cryptography is quantum cryptography.

1.4 Contributions of this Dissertation

In this dissertation, the author is dedicated to the research of quantum key distribution. Aiming at the low-efficiency problem of currently available quantum key distribution protocols, the author conducted a lot of research and achieved significant results. The contributions of this dissertation are as follows:

1. The author proposed a dual-quantum channel structure for the quantum key distribution process, which improved the efficiency of sharing the raw key. And due to the channel diversity brought by the dual-quantum

channel structure, the final key was established in a faster way, and the eavesdropper's (Eve's) attack was effectively thwarted.

2. The author presented a novel basis selection rule to improve the raw key efficiency and deter the eavesdropper. When combined with the dual-quantum channel, the raw key efficiency was greatly improved, and subsequently the convergence speed of the final key was much faster.
3. With the aid of an initialization vector shared between the two communicating entities (Alice and Bob) and known to only themselves, the eavesdropper's attack was effectively frustrated, and the final key was obtained in a much faster and efficient way.
4. The author proposed three real-time detection mechanisms of Eve's presence during the key distribution process. The proposed mechanisms enabled the Alice and Bob to detect whether Eve was eavesdropping or not in real time, which provided an effective method to avoid and counter Eve's attack.
5. This dissertation presented a quantum key distribution protocol that removed the basis information exchange on the conventional channel, and further eliminated the necessity of the conventional channel in the structure, which greatly reduced the communication overhead and cost. In addition, the elimination of the conventional channel made the structure of the proposed protocol all-quantum. This all-quantum

structure presented less vulnerability than the hybrid structure with classical elements (for example, a conventional channel) in it.

6. In order to better frustrate Eve's attack, this dissertation incorporated several effective defense mechanisms making use of the idea of introducing more randomnesses and unpredictabilities into the structure. The integration of those countermeasures made Eve unable to launch successful attacks to the key distribution process.

1.5 Organization of this Dissertation

The organization of this dissertation is as follows:

Chapter 1 is an instruction, which includes a brief history of cryptography, the increasing security breaches, and the development of quantum computers and quantum algorithms. It also summaries the contributions and organization of this dissertation;

Chapter 2 introduces the conventional cryptography, including the symmetric cryptography, asymmetric cryptography, and several popular cryptographic algorithms. It points out the ineffectiveness of the conventional cryptography to defend against future security attacks, due to the fact that the conventional cryptography is only able to provide conditional security;

In Chapter 3, we introduce the theoretical basis of quantum cryptography, several major quantum key distribution protocols, and the applications of quantum key distribution in practices. We also discuss the unconditional security offered by quantum key distribution, as well as the weaknesses of the BB84 protocol;

In Chapter 4, we present a quantum key distribution protocol making use of a dual-quantum channel structure and complementary measuring bases on the two quantum channels; we analyze the raw key efficiency and raw key error rate in different scenarios; and we propose several methods to speed up the convergence speed of the final key while at the same time effectively frustrate Eve's attack. We compare the proposed protocol with the BB84 protocol, and show the superiority of the proposed protocol;

In Chapter 5, we propose a novel basis selection rule with the aid of an initialization vector shared between Alice and Bob. Together with the dual-quantum channel, the proposed protocol improves the efficiency of obtaining the raw key and the convergence speed of the final key, and meanwhile offers much better performance in frustrating Eve's attack than that of the BB84 protocol;

In Chapter 6, we analyze how to reduce the communication overhead on the conventional channel by deploying the dual-quantum channel structure, the basis selection rule on the two quantum channels, and the initialization vector shared between Alice and Bob. Our proposed protocol eliminates the basis information

exchange between the two communicating entities, and further eliminates the necessity of the conventional channel in the structure. We also present three real-time detection mechanisms of Eve's presence during the key distribution process, which help Alice and Bob to detect, avoid, and frustrate Eve's attack. It is proved that the proposed protocol presents many advantages in reducing the communication overhead, the cost, and defending against Eve's attack;

In Chapter 7, several defense mechanisms that can confuse, fool and counter Eve's attack are addressed. The basic idea behind these defense mechanisms is to import more randomnesses and unpredictabilities into the key distribution process. The integration of these techniques increases the difficulty of Eve to launch a successful eavesdropping attack, and as a result, Eve's attack is effectively frustrated; and

Chapter 8 concludes the entire dissertation and points out some future research directions.

Chapter 2 Conventional Cryptography

Cryptography is an art of concealing information. It converts intelligible information into unintelligible or meaningless information, which nobody can read without properly decrypting. This is how the secret information can be kept secret. The secret information that people want to hide and transmit is called plaintext, while the unintelligible message after encryption is called ciphertext. The process of converting plaintext into ciphertext is called encryption, and the reverse process, which is restoring plaintext from ciphertext is called decryption. In order to be able to encrypt and decrypt messages, the two communicating entities, Alice and Bob, need to share some kind of initial secret between them ahead of time, which is later used in the encryption and decryption processes. That initial secret is called an encryption/decryption key. According to whether the keys used for encryption and decryption are the same, conventional cryptography is categorized into two classes: symmetric cryptography and asymmetric cryptography. In symmetric cryptography, the encryption and decryption processes make use of the same key, while in asymmetric cryptography, encryption and decryption use two different keys. The general encryption and decryption processes of a cryptosystem are shown in Figure 2.1.

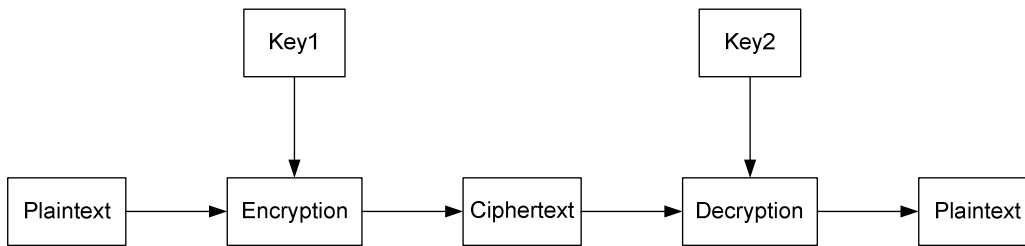


Figure 2.1 The structure of conventional cryptosystems

2.1 Symmetric Cryptography

In symmetric cryptography, Alice and Bob use the same key for both encryption and decryption. That key is referred to as a secret key and thus symmetric cryptography is also called secret key cryptography, or single-key encryption [5]. The core techniques of symmetric cryptography are permutation and substitution, and the security of the symmetric cryptography relies on the secrecy of the secret key. Permutation is the process of transposing the bits in a message, and substitution is the process of replacing a bit in a message by another bit. In the following sections, we will give a brief introduction to some of the most popular symmetric cryptographic algorithms that are widely being used for secure communication.

2.1.1 Data Encryption Standard

Data Encryption Standard (DES) algorithm is the most widely used encryption scheme adopted in 1977 by the National Institute of Standards and Technology (NIST) as the Federal Information Processing Standard 46 (FIPS PUB 46) [5]. FIPS PUB 46-3 is the latest version of the standard [18]. The DES is a symmetric cryptographic algorithm making use of a 56-bit secret key to encrypt a message that is divided into a sequence of 64-bit blocks. It deploys a structure called the Feistel structure [19], which has the following features:

1. It has a certain number of rounds of processing, and all the rounds of processing are identical;
2. In each round, the message is divided into two halves, a substitution is performed on one half of the message, followed by a permutation of the two halves; and
3. Each round of processing uses different keys that are derived from the original secret key.

The DES algorithm consists of 16 rounds of processing. The invention of the DES was mainly contributed by the researchers at IBM in 1970's, with the help of some people outside IBM. The DES had been the most popular cryptographic algorithm until the end of last century. In 1999 NIST suggested that DES should only be used for legacy systems and triple DES (3DES) should be used as a substitute [18]. The DES algorithm is pretty strong against a variety of attacks;

however, due to the small size of the encryption key (56 bits) and the increasing computational power people can get, it is easy to be broken nowadays. For example, the DES algorithm was broken in 22 hours and 15 minutes by the Electronic Frontier Foundation's "Deep Crack" in a combined effort with "distributed.net" in 1999 [20]. Triple DES uses two or three different keys to encrypt a message, whose total key size reaches 112 bits or 168 bits, providing much stronger security compared to the DES.

2.1.2 Advanced Encryption Standard

Advanced Encryption Standard (AES) is aiming at replacing DES and 3DES in the long run. In 1997, NIST called for a new cryptographic algorithm to replace the DES algorithm. In 2001, an algorithm named Rijindael, whose inventors are Dr. Joan Daemen and Dr. Vincent Rijimen [5], was selected as the AES algorithm and published in FIPS PUB 197 [21]. The AES algorithm does not adopt the Feistel structure as the DES; it uses a 128-bit message block and a key size of 128, 192, or 256 bits; and the AES deploys 10 rounds of processing, 9 out of 10 are identical, consisting of four procedures, Substitute Bytes, Shift Rows, Mix Columns, and Add Round Key, and the last round contains only three procedures, Substitute Bytes, Shift Rows, and Add Round Key. Due to the

bigger key size, the AES provides much stronger security than the DES. So far there is still no affordable ways to break the AES.

2.1.3 RC4 Algorithm

The two cryptographic algorithms we just introduced above are both block ciphers, since the message is divided into fix-size blocks (64 or 128 bits) and each block is treated as a single element when being encrypted. The RC4 algorithm is a stream cipher designed by Ron Rivest for RSA Security in 1987 [5]. In a stream cipher, the message is encrypted either byte by byte or bit by bit instead of block by block in a block cipher. The RC4 algorithm uses a variable key size, such as 128 bits, 192 bits, or even longer. The key is used as the input of a pseudorandom number generator, which produces pseudorandom numbers. The pseudorandom numbers is then XORed with the message to be encrypted byte by byte, and the results of the XOR operation form the ciphertext. The security of the RC4 algorithm is very strong, and there is no practical attack against the algorithm with a reasonably long key size. The primary advantage of the RC4 algorithm is that it has a very fast encryption speed so that it runs very quickly in software. The RC4 is widely used between web browsers and web servers, and in wireless communications as well. The SSL/TLS (Secure Sockets

Layer/Transport Layer Security) and WEP (Wired Equivalent Privacy) algorithms also make use of the RC4 algorithm as the encryption mechanism.

2.1.4 One-Time Pad

None of the abovementioned cryptographic algorithms is able to provide unconditional security. In conventional cryptography, the only cryptographic algorithm that can provide theatrically unbreakable security is the one-time pad. The one-time pad was proposed by a U.S. Army Signal Corps officer, Joseph Mauborgne, as an improvement to the Verman cipher invented by an AT&T engineer named Gibert Vernam [5]. In the one-time pad algorithm, Mauborgne proposed that a message should be encrypted by a key that has the same length as the message and at the same time is a random number. The key is only used once, and then it is discarded. For the next message, a new key of the same length as the message is used. Theoretically, one-time pad is unbreakable; however, in practice, it is impossible to produce truly random numbers without any repetition in the long run. Thus the one-time pad is difficult to be deployed in practical situations.

2.2 Asymmetric Cryptography

Different from the symmetric cryptography, where there is only one key that is used for both encryption and decryption of a message, in the asymmetric cryptography, the encryption and decryption processes make use of two different keys. The two different keys are referred to as a public key and a private key, respectively. The asymmetric cryptography is also called the public key cryptography, since one of the two keys can be public. In the asymmetric cryptography, both of the public key and the private key can be used for encryption and decryption. For example, if the public key is used for encryption, then the private key is used for decryption, or if the private key is used for encryption, then the public key is used for decryption. The asymmetric cryptography can provide confidentiality, authentication, and non-repudiation features at the same time. The confidentiality feature is realized by encrypting the message with the other person's public key. Since only the other person has his private key, he is the only one who can decrypt the message and read it. This way the confidentiality is achieved. The authentication and non-repudiation features are realized by encrypting the message with your own private key. Since you are the only one who has your own private key, the encrypted message must have come from you, and you can not deny that you have encrypted the message, which provides the authentication and non-repudiation features at the same time. The symmetric cryptography can provide

confidentiality and authentication between the two communicating entities, but it does not offer the non-repudiation feature, since both of the two communicating entities share the same key and they can both claim that a message is from the other person. We will briefly introduce several major asymmetric cryptographic algorithms that are widely being used.

2.2.1 RSA Algorithm

The RSA algorithm [6] is the most widely used asymmetric cryptographic algorithm invented by Ron Rivest, Adi Shamir, and Len Adleman in 1977. It is a block cipher, whose block size is a number between 1 and typically 1024 bits (or 309 decimal digits). Its security relies on the fact that it is infeasible to factorize a huge composite number (309 decimal digits) in a practical time at an acceptable cost with currently available technologies. The algorithm is briefly shown as follows:

1. Select two secret large prime numbers p and q , $p \neq q$;
2. Calculate $n = p \times q$ and release n to the public, where n is a number of 1024 bits;
3. Calculate $\phi(n) = (p-1) \times (q-1)$, where $\phi(n)$ is called Euler's Totient Function, and $\phi(n)$ is kept secret;

4. Select an integer e , which is relatively prime to $\phi(n)$, $1 < e < \phi(n)$, and then release e ;
5. Calculate $d \equiv e^{-1} \pmod{\phi(n)}$, and keep d secret;

Till now, we have produced the public key $PU = \{e, n\}$ and the private key $PR = \{d, n\}$.

6. Calculate the ciphertext $C = M^e \pmod{n}$, where M is the plaintext, and $M < n$; and
7. The plaintext can be restored by $M = C^d \pmod{n}$.

The RSA algorithm is very strong against a variety of security attacks, such as the brute force attack, mathematical attack, timing attack, chosen ciphertext attack, and so on. According to the report by the RSA Laboratories, it will take about 55 years on a single 2.2 GHz Opteron CPU to solve the factorization problem of a 663-bit composite number, but it will only take about 3 months on a cluster of 80 2.2 GHz Opteron CPUs [22] to finish the factorization. However, the effort of factorizing a 1024-bit number would be millions of times harder than that of the 663-bit number, which makes it infeasible for currently available classical computers to solve the problem.

2.2.2 Elliptic Curve Cryptography

Although the RSA algorithm is still the most popular asymmetric cryptographic algorithm being used so far, the Elliptic Curve Cryptography (ECC) starts to challenge it. The RSA algorithm requires a lot of computational effort, thus it has a slow processing speed, which is one of the RSA algorithm's drawbacks. For example, in order to provide confidentiality and authentication at the same time, a message needs to be encrypted by the sender's private key and then encrypted again by the receiver's public key, which requires the sender to run the RSA algorithm twice. When decrypting the encrypted message, first the receiver's private key is used, and then the sender's public key is needed. Since for each message to be transmitted, the RSA algorithm needs to run four times, the entire process becomes very sluggish and effort-consuming. Elliptic Curve Cryptography, on the other hand, is considered to be able to provide the same level of security using a considerable smaller key size, and hence requiring much less computational efforts than the RSA algorithm.

Elliptic Curve Cryptography is a public key cryptography based on the usage of elliptic curves over finite fields. The use of elliptic curves in cryptography was suggested by Neal Koblitz [23] and Victor S. Miller [24] independently in 1985. Just like the RSA algorithm, it also has a very difficult mathematical problem serving as the bastion of its security, which is referred to as the elliptic

curve logarithm problem. The mathematics involved in the algorithm is very complicated, and we simply omit it in the dissertation.

2.2.3 Diffie-Hellman Key Exchange

The Diffie-Hellman key exchange algorithm was the first public key algorithm that was proposed by Whitfield Diffie and Martin Hellman in 1976 [7]. In that seminal paper, Whitfield Diffie and Martin Hellman defined the public key cryptography, and proposed a way to establish a secret key between the two communicating entities using their public and private keys. The security of this key exchange algorithm is based on the ineffectiveness of solving the so-called discrete logarithm problem. In the following, we will briefly introduce the steps of exchanging a secret key between the two communicating entities, Alice and Bob:

1. Alice and Bob select a prime number q and a primitive root of q , which is $\alpha, \alpha < q$;
2. Alice selects a private key $PR_A < q$, calculates her public key $PU_A = \alpha^{PR_A} \bmod q$, and transmits PU_A to Bob;
3. Bob selects a private key $PR_B < q$, calculates his public key $PU_B = \alpha^{PR_B} \bmod q$, and transmits PU_B to Alice; and

4. Alice calculates the secret key by $K = PU_B^{PR_A} \bmod q$, and Bob calculates the secret key by $K = PU_A^{PR_B} \bmod q$.

Since $PU_B^{PR_A} \bmod q = PU_A^{PR_B} \bmod q$, Alice and Bob share the same secret key K . The discrete logarithm problem is to get $PR_A = d \log_{\alpha, q}(PU_A)$, which is considered infeasible by using currently available computers. However the Diffie-Hellman key exchange algorithm is subject to the Man-in-the-Middle attack, where an attacker Eve communicates to Alice as if she was Bob, and then communicates to Bob as if she was Alice, to share a secret key with Alice and another secret key with Bob respectively without Alice's and Bob's notices. Alice and Bob still think that they are communicating to each other; however, they are actually communicating to Eve, instead.

2.3 Conditional Security of Conventional Cryptography

The conventional cryptography, including the symmetric cryptography and asymmetric cryptography, is only conditionally secure, which means that they can only provide conditional security to the encrypted message. The conventional cryptography is vulnerable to many types of attacks. Despite of the many subtle attacks, the brute force attack has always been a serious one to the conventional cryptography. The idea of the brute force attack is to try to exhaust

all the possible decryption keys to search for a match between the ciphertext and the plaintext. The DES algorithm has been broken in 22 hours by the brute force attack using the technologies available in 1999. Even the widely used RSA algorithm, which is considered very secure, is being challenged due to the increasing computational power people can get. In fact, the security of the conventional cryptography is based on the hope that the attacker either cannot break the ciphertext within the message's validation time, or the effort needed to break the ciphertext is more expensive than the value of the message itself, so that the attacker would not bother to attack. This does not necessarily mean that the attacker cannot break the ciphertext, it only means that the attacker is not willing to do that due to lack of motivations.

With the fast development of the computer technologies, people are getting more computational power at a much faster pace. Each year people are closer to breaking the conventional cryptography. In addition, people can work in a cooperative way to break the conventional cryptography by using distributed computing techniques. As we mentioned earlier, it will take about 55 years for a single 2.2 GHz Opteron CPU to solve the factorization problem of a 663-bit number; however, it will only take about 3 months to solve the same problem if 80 2.2 GHz Opteron CPUs are used at the same time [22].

Quantum computer is a fast emerging research area. It uses a totally different idea to compute, and it provides extremely powerful parallel computing

capabilities. The realization of quantum computers will exponentially speed up the solving of the factorization problem, which will make not only the RSA algorithm, but also all the other computational-difficulty-based conventional cryptographic algorithms not secure at all.

2.4 Summary

In this chapter, we talked about the conventional cryptography, including the symmetric cryptography and asymmetric cryptography. In the symmetric cryptography, we briefly introduced two block ciphers, the DES and AES algorithms, and two stream ciphers, the RC4 and one-time pad algorithms. In the asymmetric cryptography, we introduced the widely used RSA algorithm, and the emerging ECC algorithm, as well as the first public key distribution protocol, namely, the Diffie-Hellman key exchange algorithm. We also discussed the conditional security provided by the conventional cryptography, the challenge it is facing to the exponentially increasing computational power people can get with the fast development of the computer technologies. The discussion showed that the conventional cryptography is not secure enough for the future.

Chapter 3 Quantum Cryptography and Quantum Key Distribution

3.1 Introduction

Compared to the conventional cryptography introduced in Chapter 2, quantum cryptography is a very different cryptography that is based on a totally different idea. Quantum cryptography is based on the laws of quantum mechanics, which enable the detection of an eavesdropper's eavesdropping activity during the key distribution process, and thus provide unconditional security. The terms Quantum Cryptography (QC) and Quantum Key Distribution (QKD) are usually exchangeable. Although quantum cryptography may be understood as a method of encryption, it is actually a technique to distribute a secret key between two communicating entities, so it is better described as quantum key distribution.

The idea of using quantum mechanics for cryptography was implicitly proposed as early as 1969 by Stefan Wiesner in his manuscript; however, the manuscript was not published until 1983 [25]. The first quantum key distribution protocol was proposed by Charles Bennett and Gilles Brassard in their seminal paper [8] in 1984, which is referred to as the BB84 protocol. The BB84 protocol opened the door of the quantum key distribution research. Since then many quantum key distribution protocols have been proposed [26-60], and some of them have been implemented in experiments and practices [61-74]. Despite of

the numerous quantum key protocols proposed with many variations and enhanced features, most of them are based on several major quantum key distribution protocols [8, 26-30]. References [75-80] give a more complete introduction to quantum cryptography and quantum key distribution.

3.1.1 Polarization of Light

Although all the particles that manifest quantum mechanics properties can be used for quantum key distribution, for example, photons, electrons, ions, and so on, photons are the most popular carrier of quantum key distribution. Most of the quantum key distribution protocols available so far make the most use of the polarization states of photons to realize the key distribution. Now we will briefly introduce the concept of polarization of light.

Light is an electromagnetic wave that is composed of photons. It is described by the electric field and magnetic field that are perpendicular and proportional to each other. When considering the polarization state of light, we only need to consider either the electric field or the magnetic field, since the two fields are correlated and knowing one equals to knowing the other. Usually the electric field is chosen when talking about the polarization state of light.

Light can be polarized or not polarized at all. According to the projection of the electric field vector on the plane perpendicular to the travel direction of the

light, polarized light can be linearly polarized, circularly polarized, or elliptically polarized, Figure 3.1.

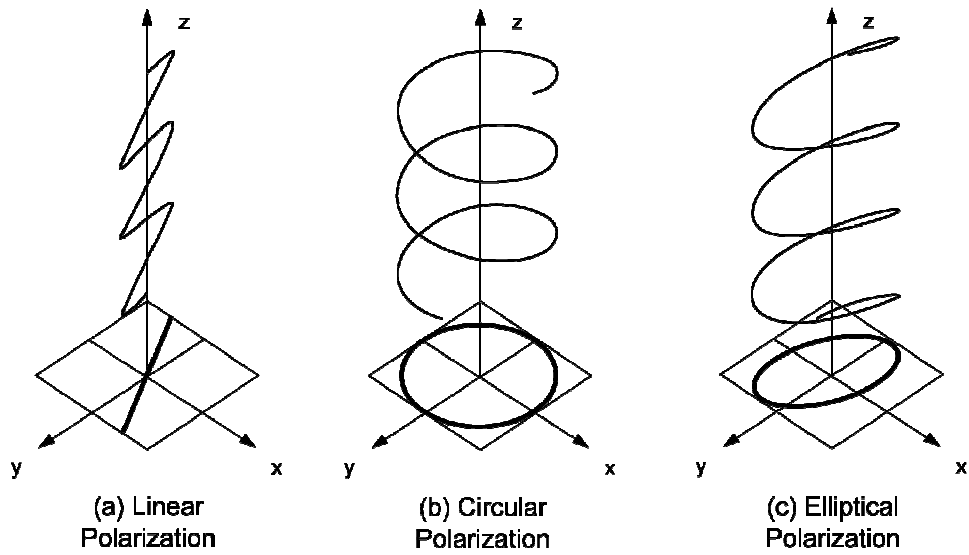


Figure 3.1 Polarization of light

In quantum key distribution protocols, the linear polarization state is mostly used. Within the linear polarization state, there are four special polarization states that are of particular interest: vertical (90°) polarization, horizontal (0°) polarization, 45° polarization, and 135° polarization, which are shown in Figure 3.2.

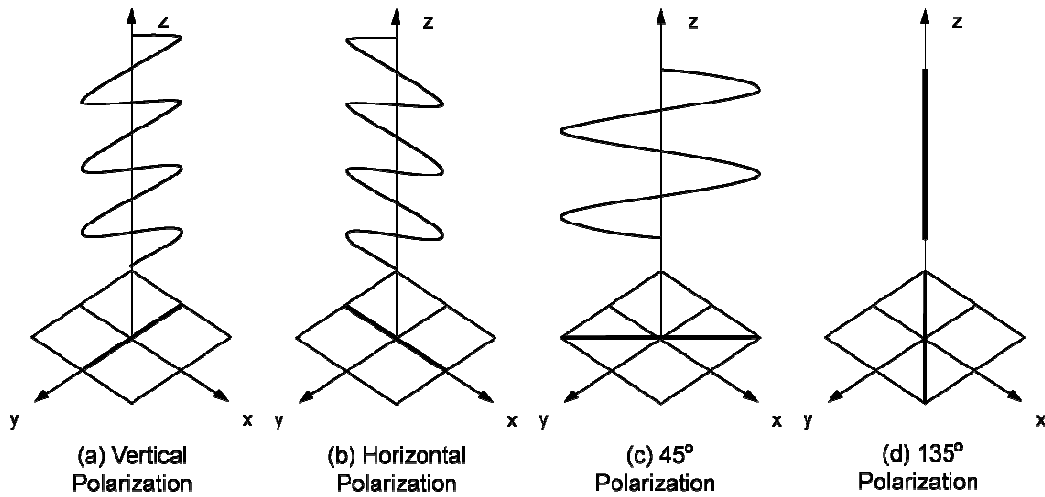


Figure 3.2 Four polarization states of a photon

3.1.2 Classical Bit and Quantum Bit

In the classical world, the value of a classical bit can only have two options, either 0 or 1, which are represented by the presence or absence of a voltage in analog systems. It is obvious that a classical bit can not be both 0 and 1 at the same time, since a voltage can not be both present and absent at the same time.

In order to distinguish the bit in the quantum world from the bit in the classical world, we call the bit in the quantum world a quantum bit, or a Qubit for short. A qubit has a totally different story when it comes to its value. A qubit can have numerous values, compared to the classical bit, which can only have one of the two options. Mathematically, a qubit is represented by a vector

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (3.1)$$

where $\alpha, \beta \in C, |\alpha|^2 + |\beta|^2 = 1$, and $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

The definition of a qubit: A qubit is a quantum system Q whose state lies in a two-dimensional Hilbert space H [77]. Here we consider a 2-state quantum system, where there are only two possible results in experiments, for example, the vertical polarization and horizontal polarization states. A general quantum state is a linear complex combination of the two basic polarization states, the vertical and horizontal polarization states. We denote the vertical polarization state by $|\uparrow\rangle$, the horizontal polarization state by $|\rightarrow\rangle$, and then a general quantum state can be represented by

$$|\varphi\rangle = \alpha|\rightarrow\rangle + \beta|\uparrow\rangle, \quad (3.2)$$

where $\alpha, \beta \in C, |\alpha|^2 + |\beta|^2 = 1$, and $|\rightarrow\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |\uparrow\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

Figure 3.3 provides a straightforward view of the relationship between a general quantum state and the two basic states.

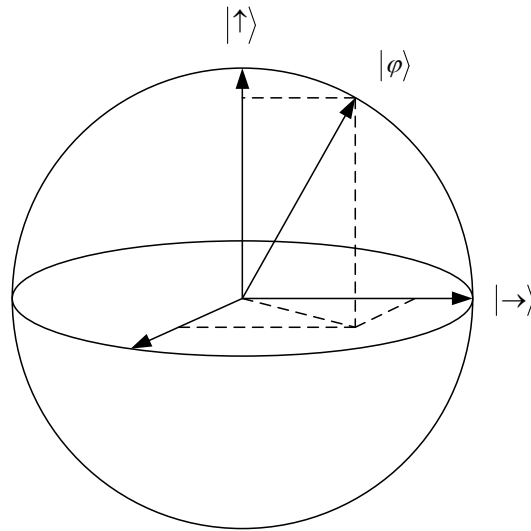


Figure 3.3 A general quantum state

3.2 Basis of Quantum Cryptography

3.2.1 Heisenberg Uncertainty Principle

The Heisenberg Uncertainty Principle is one of the most important theorems on which quantum cryptography is based. It is formulated by Werner Heisenberg in the 1920's and developed with other people's contribution [81].

The Heisenberg Uncertainty Principle can be interpreted as follows: It is impossible to get the precise position and velocity of a particle simultaneously. For example, if you increase the accuracy of measuring the position of a particle, then you inevitably reduce the accuracy of measuring the velocity of that particle at the same time, and vice versa. The Heisenberg Uncertainty Principle

not only applies to the position and velocity of a particle, but also to other quantum properties that do not commute to each other. Here “do not commute”, mathematically, means $AB \neq BA$, where A and B represent two quantum properties. In quantum cryptography, the polarization state of a photon is often used, and the Heisenberg Uncertainty Principle tells us that it is impossible to get a precise measurement result of an unknown polarization state along two different polarization axes. We will see examples of the application of the Heisenberg Uncertainty Principle in the BB84 protocol to be addressed later on.

3.2.2 No-Cloning Theorem

The No-Cloning Theorem is another most important theorem on which quantum cryptography is based. It was discovered by William Wootters, Wojciech Zurek, and Dennis Dieks in 1982 [82, 83].

The No-Cloning Theorem tells us that it is impossible to create an identical copy of an arbitrary unknown quantum state. For example, if you want to copy a quantum state on a qubit but you do not know the quantum state on that qubit in the first place, you will not be able to get a faithful copy of that quantum state. There are two reasons causing this impossibility of identically copying an unknown quantum state, which are as follows:

1. If you copy an unknown quantum state on a qubit, the quantum state changes as soon as you try to copy it, and the quantum state you get is different from the original quantum state. In addition, when you copy the quantum state, the qubit (polarized single photon) bearing the quantum state is also destroyed; and
2. You can make a faithful copy of a quantum state on a qubit only if you know the quantum state already. If you do not know the quantum state, then you will not be able to get an identical copy of it. This is like a deadlock, where you are required to know the quantum state before making a copy; however, not knowing the quantum state is the motivation of this copying action, which obviously conflicts to each other and cannot be solved anyway.

In quantum cryptography, the reason that the two communicating entities are able to detect whether an eavesdropper has eavesdropped on the message or not is due to the No-Cloning Theorem, which guarantees that if an eavesdropper eavesdrops on the message, then the receiver of the message will get a different message from what the sender has sent, so that later on after comparing their messages, the sender and receiver will notice the conflicts in the messages, from which they can deduce that the eavesdropper has eavesdropped on the message. The reason that the receiver will get a different message is that as soon as the

eavesdropper copies the quantum state, it is changed to another state that is different from the quantum state sent by the sender.

3.2.3 Quantum Measurement

In a 2-state quantum system, although a quantum state can be a combined state $|\varphi\rangle = \alpha|\rightarrow\rangle + \beta|\uparrow\rangle$, when a quantum state is measured, there are only two possible results, either the horizontal polarization state or the vertical polarization state, with a certain probability, respectively. To be more concrete, after measuring a general quantum state $|\varphi\rangle$, the possibility of getting a horizontal polarization state ($|\rightarrow\rangle$) is $|\alpha|^2$, and the possibility of getting a vertical polarization state ($|\uparrow\rangle$) is $|\beta|^2$, where $|\alpha|^2 + |\beta|^2 = 1$.

For example, the 45° polarization state ($|45^\circ\rangle$) can be represented as

$$|45^\circ\rangle = \frac{1}{\sqrt{2}}|\rightarrow\rangle + \frac{1}{\sqrt{2}}|\uparrow\rangle, \quad (3.3)$$

which is illustrated in Figure 3.4. If you use an optical filter that has a polarization axis along the horizontal direction, then the filter will get a

horizontal polarization state $|\alpha|^2 = \left(\frac{1}{\sqrt{2}}\right)^2 = 0.5$ of the time; on the other hand, if

you use an optical filter that has a polarization axis along the vertical direction,

then the filter will get a vertical polarization state $|\beta|^2 = \left(\frac{1}{\sqrt{2}}\right)^2 = 0.5$ of the time.

In this case, no matter whether you use an optical filter with a horizontal polarization axis or a vertical polarization axis, you can not get an assured measurement result, since both results happen with 50% probability. The only way that you can get a correct measurement result all the time is to use an optical filter with a 45° polarization axis (there is no such a filter naturally, but we can manage to get one with the help of additional components, and we will talk about this in detail later on).

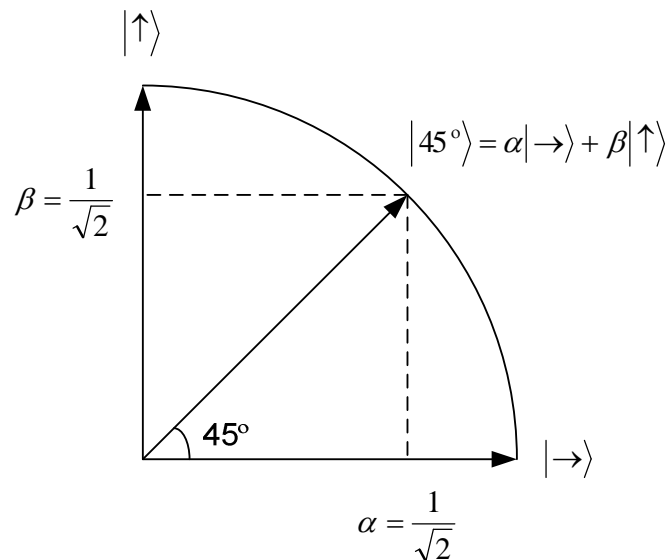


Figure 3.4 Measuring a 45° polarization state along the horizontal or vertical direction

3.2.4 Quantum Entanglement

Quantum entanglement [26, 84, 85] is a very astonishing quantum property that happens exclusively in the quantum world. There is no counterpart of this phenomenon in the classical world. Quantum entanglement is a correlation between two quantum systems A and B , in which when quantum system A is measured, the state of quantum system B is changed instantaneously, and the correlation between the two quantum systems is broken as soon as a measurement is made. The measurement results from the fact that two quantum systems can be the same, or the opposite, which are referred to as correlated and anti-correlated, respectively.

Let us take the anti-correlated entanglement for example to explain the properties of quantum entanglement. Suppose you have two qubits, and you know the initial quantum states on them in the first place, for example, a vertical polarization state and a 45° polarization state. Through some specific procedures, somehow the two qubits become entangled. As soon as the two qubits become entangled, the states on them change to some uncertain states that nobody knows. The two qubits do not need to stay together to maintain the entanglement between them. They can be separated for an arbitrarily long distance and yet will remain entangled. But as soon as one qubit is measured, the quantum state on the other qubit is changed instantaneously, and the entanglement between the two qubits is broken. If the first person Alice uses a specific measurement and

gets a measurement result 1, then the other person Bob must get a 0, which is the opposite of 1, if he uses the same measurement as Alice. If Alice gets a 0, then Bob has to get a 1. This is called the anti-correlated quantum entanglement of the two quantum systems.

The special characteristic of quantum entanglement can be used for quantum cryptography to distribute a key with unconditional security. The first quantum key distribution protocol making use of quantum entanglement was proposed by Artur Ekert in 1991, and the protocol is referred to as the E91 protocol [26].

3.3 Unconditional Security of Quantum Cryptography

The essential reason that quantum cryptography can provide unconditional security is that it is able to detect whether the eavesdropper has eavesdropped on the message or not during the key distribution process, while the conventional cryptography does not offer this feature.

The eavesdropping activity of the eavesdropper inevitably brings disturbances to the quantum system, which are treated as noises, and represented by the errors in the raw key shared between the two communicating entities. After Alice generates a qubit with a certain quantum state and sends it to Bob, Eve, who is the eavesdropper in between, intercepts the qubit and performs a copying activity. At the moment when Eve tries to copy the quantum state on the qubit,

due to the No-Cloning Theorem, she is not able to get a correct copy of that quantum state, if she does not know the quantum state beforehand. According to the Heisenberg Uncertainty Principle, after measuring the qubit sent by Alice, the quantum state on that qubit collapses to one of the two possible states, for example, the vertical polarization state or horizontal polarization state; however, neither of which happens with 100% probability, unless the original quantum state happens to be a vertical or horizontal polarization. This indicates that after the measurement, the quantum state on a qubit is changed to another state that is different from the original one. Now, when Bob receives the qubit with a different quantum state from the original one and measures it, he will get a different measurement result from the original information Alice wanted to transmit. Later on, Alice and Bob compare their measurement results, if they find a conflict between them, then they can deduce that Eve has been present and eavesdropped on the message, so that they discard the message and start the key distribution protocol all over again until they can conclude Eve is not eavesdropping on the message. This is how quantum cryptography can detect the eavesdropping activity of an eavesdropper and provide unconditional security.

On the other hand, let us check the conventional cryptography. Alice sends a string of classical bits to Bob; and Eve, who is in between, intercepts or copies the classical data. The classical data sent by Alice would not change to other

values due to Eve's eavesdropping activity. After Eve's copying, the original classical data remains the same, and Eve can get the exact value of that original data. Then Bob receives the data sent by Alice and eavesdropped on by Eve already, and he will still get the same data as Alice. So eventually, Alice, Bob, and Eve will all get the same data. Since Alice and Bob get the same data, there is no way for them to tell whether the eavesdropper has eavesdropped on the data or not. Thus the conventional cryptography is not able to provide unconditional security as the quantum cryptography does.

3.4 Major Quantum Key Distribution Protocols

3.4.1 Polarization-Based Quantum Key Distribution Protocol

The BB84 protocol is the first quantum key distribution protocol and also the most important one. It makes use of the polarization state of a single photon to represent a classical bit and then distributes that bit of information from one communicating entity to the other.

3.4.1.1 Four Polarization States of a Photon

In this protocol, four polarization states of a photon are used, i.e., vertical polarization, horizontal polarization, 45° polarization, and 135° polarization, Figure 3.5.

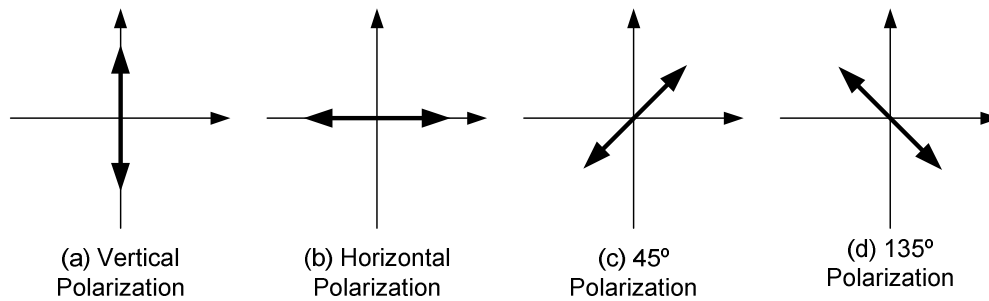


Figure 3.5 Four basic polarization states of a single photon

3.4.1.2 Rectilinear Basis and Diagonal Basis

Two bases are defined in this protocol: the rectilinear basis, denoted by $+$; and the diagonal basis, denoted by \times . The rectilinear basis represents a coordinate system, in which the two axes point to the horizontal and vertical directions (Figure 3.6 (a)); and the diagonal basis represents another coordinate system, in which the two axes point to the 45° and 135° directions (Figure 3.6 (b)).

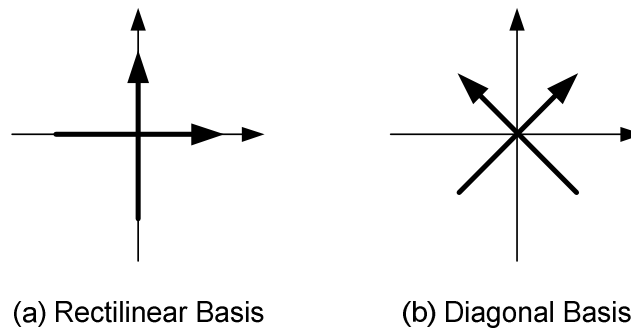


Figure 3.6 Rectilinear basis and diagonal basis

3.4.1.3 Measuring Polarized Single Photons with a Polarizing Beam Splitter

In terms of measuring a qubit with a certain polarization state on it, the physical meaning of a rectilinear basis is an optical filter with either a vertical polarization axis or a horizontal polarization axis that allows a qubit to pass along either the vertical direction or the horizontal direction; and the physical meaning of a diagonal basis is an optical filter with either a 45° polarization axis or a 135° polarization axis (there is no such optical filter by nature, but it can be made with the aid of a 45° polarization rotator) that allows a qubit to pass along either the 45° direction or the 135° direction.

A Polarizing Beam Splitter (PBS) is a good representation of the two bases. Let us take the polarizing beam splitter with a vertical polarization axis for example to illustrate the measurement of a qubit, Figure 3.7.

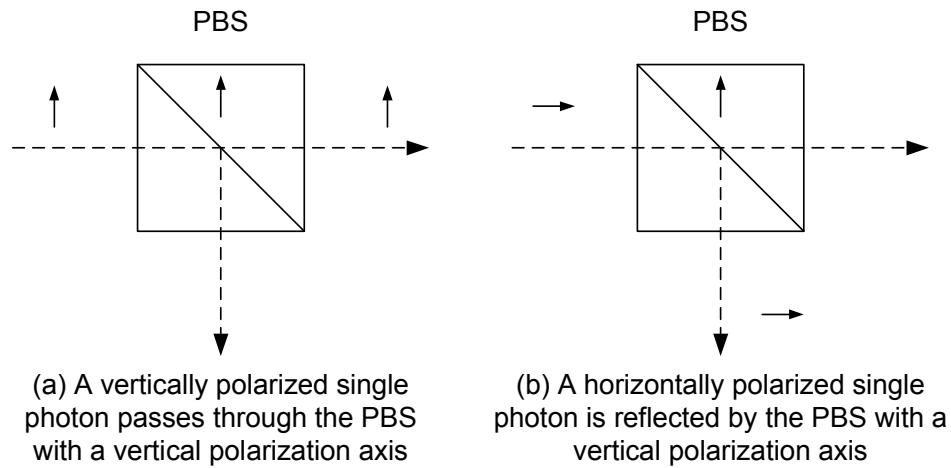


Figure 3.7 Measuring a vertically polarized single photon and a horizontally polarized single photon using a PBS with a vertical polarization axis

A qubit with a vertical polarization state on it passes the PBS with a vertical polarization axis with 100% probability. A qubit with a horizontal polarization state on it is reflected by the PBS with a vertical polarization axis with 100% probability. The probability of passing or being reflected by a PBS with a vertical polarization axis is decided by the coefficients of the vector representation of the qubit, i.e., α and β . According to the vector representation of a qubit, $|\varphi\rangle = \alpha|\rightarrow\rangle + \beta|\uparrow\rangle$, a qubit passes the PBS with a vertical polarization axis with the probability of $|\beta|^2$, and it is reflected by the same PBS with the probability of $|\alpha|^2$. A qubit with a 45° polarization state on it passes or is reflected by a PBS with a vertical polarization axis with equal probabilities, both

50%, Figure 3.8, which is why using a PBS with a vertical polarization axis to measure a qubit with a 45° or 135° polarization state on it totally randomizes the measurement result. On the other hand, if you use a PBS with a 45° polarization axis to measure a qubit with a vertical or horizontal polarization state on it, the measurement result you can get is also totally random.

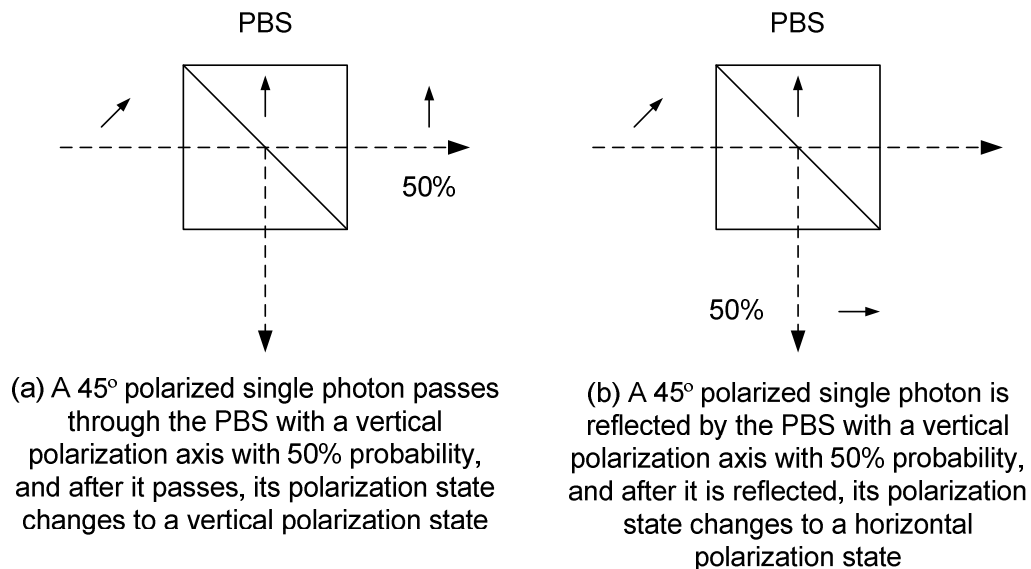


Figure 3.8 Measuring a 45° polarized single photon using a PBS with a vertical polarization axis

Since naturally there is no PBS with a 45° polarization axis, in order to be able to measure the polarization states in the diagonal basis, i.e., 45° and 135° polarization states, a 45° Polarization Rotator (PR) is needed before the 45° and 135° polarized single photons enter the PBS, Figure 3.9.

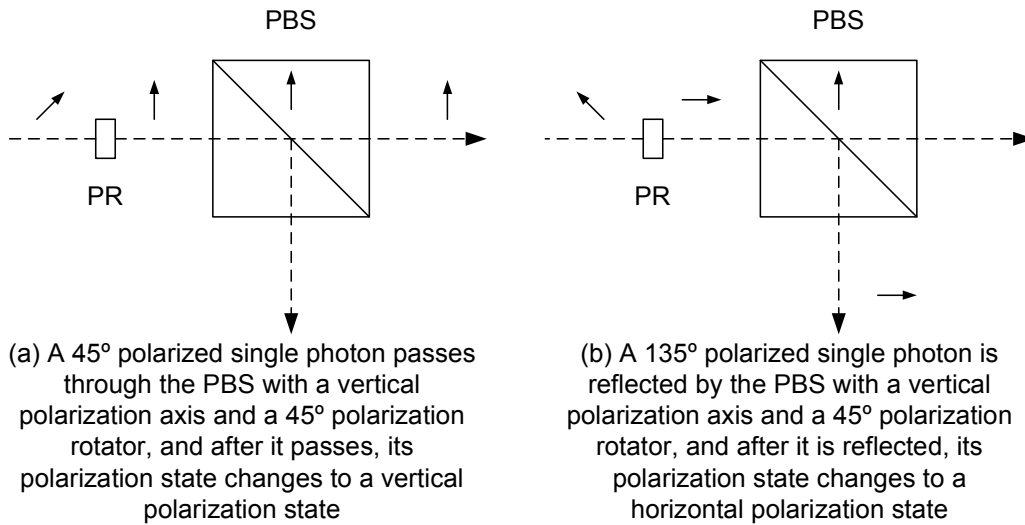


Figure 3.9 Measuring a qubit with a 45° or 135° polarization state with a PBS with a vertical polarization axis (with the aid of a 45° polarization rotator)

After a 45° polarized single photon passing through a 45° polarization rotator, it is changed to 90° polarized, which is a vertically polarized single photon. Then this vertically polarized single photon passes the PBS with a vertical polarization axis with 100% probability. If a single photon detector down the passing path detects a click, then it knows that a vertically polarized single photon just passed and the original polarization state of that polarized single photon is $90^\circ - 45^\circ = 45^\circ$ polarization. Similar thing happens to a 135° polarized single photon. After the 45° polarization rotator, the 135° polarized single photon is changed to a 180° polarized single photon, which is horizontally polarized. Then it is reflected by the PBS to the reflecting path, and a single







photon detector down the reflecting path clicks. After subtracting 45° , the photon detector can get the result of the original polarized single photon, which is a $180^\circ - 45^\circ = 135^\circ$ polarized single photon. This explains how to measure polarized single photons in the diagonal basis using a PBS that has a polarization axis in the rectilinear basis.

3.4.1.4 Representation of Classical Bits by Polarized Single Photons

Two binary values, the classical bits 0 and 1 are used in this protocol, and they are represented by polarized single photons according to Table 3.1. For example, the binary value 0 can be presented by either a horizontally polarized single photon in the rectilinear basis or a 45° polarized single photon in the diagonal basis, and it depends on which basis is chosen (either the rectilinear basis or the diagonal basis) to decide which polarized single photon to choose. If you choose the rectilinear basis, then the classical bit 0 is represented by a horizontally polarized single photon; and if you choose the diagonal basis, then it is represented by a 45° polarized single photon. The combinations in Table 3.1 can be changed to other forms, for example, one can choose to use a vertically polarized single photon to represent 0 in the rectilinear basis and still use the 45° polarized single photon to represent 0 in the diagonal basis. No matter which

form is chosen, the two communicating entities should keep synchronized and both be aware of the content of the table.

Table 3.1 Representation of classical bits by polarized single photons

| Classical Bit | Basis | |
|---------------|---|--|
| |  |  |
| 0 |  |  |
| 1 |  |  |

3.4.1.5 Schematic Diagram of the Structure of the BB84 Protocol

The schematic diagram of the structure of the BB84 protocol is shown in Figure 3.10.

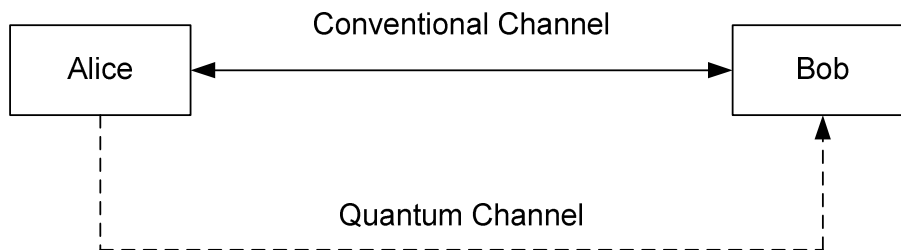


Figure 3.10 Schematic diagram of the structure of the BB84 protocol

As we can see from Figure 3.10, the two communicating entities, Alice and Bob, who wish to establish a secret key between them, are connected by two channels, one conventional channel and one quantum channel. The conventional channel is a regular telecommunication channel, on which Alice and Bob exchange classical information. The quantum channel is an optical fiber, on which qubits (polarized single photons) are transmitted from Alice to Bob.

3.4.1.6 Assumptions of the BB84 Protocol

The assumptions of the BB84 protocol are the following:

1. Alice and Bob have already authenticated each other somehow before the protocol starts;
2. Eve has access to the conventional channel. She can listen to the conventional channel and get the information flowing on it; however, she is not able to change the information on the conventional channel. Eve can listen to the quantum channel, intercept a qubit and resend another qubit to Bob; and
3. Eve's goal is to eavesdrop on the information transmitted between Alice and Bob as much as possible without being noticed. To stop Alice and Bob from communicating, for example, by cutting off the conventional channel or the quantum channel, is not the goal of the eavesdropper.

Otherwise no communication system could work as long as somebody keeps destroying the equipment physically.

3.4.1.7 Steps to Share a Raw Key in the BB84 Protocol

The two communicating entities, Alice and Bob, need to take the following steps to share a raw key between them:

1. Alice generates a sequence of random 0's and 1's;
2. Alice randomly selects one of the two possible bases (+ or \times) for each of the bits generated in the first step;
3. Alice represents the bits generated in the first step using polarized single photons according to Table 3.1, and transmits them through the quantum channel;
4. At Bob's measuring side, he randomly selects one of the two possible bases (+ or \times) for each of the qubits received on the quantum channel and measures it;
5. If Bob selects the same basis as Alice, then he will get the same data as Alice's; and if he selects a different basis from Alice's, then he will get the same data as Alice's only half of the time;

6. Bob communicates with Alice through the conventional channel about which bases he used to measure the qubits, and Alice tells Bob for which qubits he used the wrong bases; and
7. Alice and Bob delete all the bits for which they used different bases and save the rest of the bits as a sequence, which is the raw key shared between them.

Table 3.2 gives us a complete view of the 7 steps of sharing a raw key between Alice and Bob.

Table 3.2 An example of the BB84 protocol

| | | | | | | | | | |
|---------------|--------|---|--------|--------|---|--------|---|---|--------|
| Alice | Step 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |
| | Step 2 | | | | | | | | |
| | Step 3 | | | | | | | | |
| Bob | Step 4 | | | | | | | | |
| | Step 5 | | 0 or 1 | 0 or 1 | | 0 or 1 | | | 0 or 1 |
| Alice and Bob | Step 6 | Alice and Bob exchange basis information through the conventional channel | | | | | | | |
| | Step 7 | 1 | | | 0 | | 0 | 1 | |

: Correct basis or bit

Comments on step 5: As explained in Section 3.4.1.3, if Bob uses a rectilinear basis (a PBS with a vertical polarization axis) to measure a polarized single

photon (45° or 135° polarized) made in a diagonal basis, he will get 0 or 1 with equal probability, which is 50%. The same conclusion applies if Bob uses a diagonal basis (a PBS with a vertical polarization axis and a 45° polarization rotator in front of it) to measure a polarized single photon (vertically or horizontally polarized) made in a rectilinear basis, he will also get 0 or 1 with equal probability, which is 50%. Because Bob is not sure about the measurement result, he and Alice have to discard this bit of information on which they used different bases.

Comments on step 6: Alice's and Bob's publicly communicating to each other on the conventional channel will not release any information about the random bits generated by Alice in the first step or the raw key. The information Alice and Bob exchange through the conventional channel is the basis information, which explains which bases Bob has used to measure the qubits, and which bases Bob has used the same bases as Alice. Since each basis, either the rectilinear basis or the diagonal basis, can be used to represent 0 or 1 with equal probability, Eve is not able to figure out which bit a certain basis is representing. It is equivalent to ask Eve to guess a random number, which she can not guess correctly for sure.

Comments on step 7: The key shared between Alice and Bob is called a raw key. If Eve did not eavesdrop on the qubits transmitted by Alice, and the transmission of the qubits on the optical fiber was perfect, then there would be

no error in the raw key, and this raw key could be used directly as the final key shared between Alice and Bob to encrypt messages. If Eve did eavesdrop on the qubits, then there would be some errors in the raw key, which means the raw key in Alice's possession is not exactly the same as the raw key in Bob's possession. In this situation, in order to share an identical key between Alice and Bob, about which Eve has an arbitrarily low level of knowledge, they need to adopt the information reconciliation and privacy amplification procedures to remove the errors in the raw key and distill a final key out of the raw key. In the following, we are going to introduce the two procedures briefly, omitting their details.

3.4.1.8 Information Reconciliation and Privacy Amplification Procedures

When there are errors in the raw key due to Eve's eavesdropping or the imperfection of the optical fiber (we do not consider the imperfection of the optical fiber in this dissertation), the raw key can not be used until the errors have been removed and the secrecy of the raw key has been enhanced.

The information reconciliation procedure is basically an error correction process, through which all the errors in the raw key can be removed. The raw key with all the errors removed is called a sifted key, or we may call it an error-free raw key occasionally.

The privacy amplification procedure is basically a hash function, through which a final key is distilled from the sifted key. It is used to reduce Eve's knowledge about the final key to an arbitrarily low level to enhance the secrecy of the final key.

The information reconciliation and privacy amplification procedures are very time-consuming and effort-consuming. The information reconciliation procedure requires a lot of communication overhead between Alice and Bob on the conventional channel, as well as a lot of computation overhead at each side. Although the privacy amplification is a very important procedure to obtain the final key; however, it reduces the length of the final key dramatically, which indicates a very low efficiency. For example, a 1000-bit raw key, after removing 150 errors in it, the length of the sifted key becomes 850 bits. After going through the privacy amplification procedure, the length of the final key may be only 25 bits. It depends on the strength of the hash function algorithm you use that how many bits can be left in the final key. For example, the Secure Hash Algorithm (SHA) can reduce a sifted key with the length of up to $(2^{64} - 1)$ bits to a final key with a fixed length of 160 bits [5], which can maximally reduce the length of the final key to 1.15^{-17} of the length of the sifted key.

3.4.1.9 Weaknesses of the BB84 protocol

Although the BB84 protocol can provide unconditional security to the key distribution process, it has some drawbacks as well. The biggest drawback is that its efficiency of sharing a raw key and a final key is very low. In the BB84 protocol, Bob can guess the bases used by Alice correctly only half of the time, so that only half of the bits generated by Alice can be included into the raw key, which makes the efficiency of sharing a raw key 50%.

Since there may be errors in the raw key, Alice and Bob need to employ the information reconciliation procedure to remove all the errors, which is a communication- and computation-consuming process that produces a lot of communication overhead and takes a long time to finish. In order to enhance the secrecy of the final key, the privacy amplification procedure has to be performed. The privacy amplification procedure is a length-devastating process that reduces the length of the final key dramatically, which is not desirable.

Another drawback is the conventional channel used in the structure. A conventional channel means two things in terms of drawbacks:

1. If there is a conventional channel, then the conventional communication is needed, which generates a communication overhead as well as the cost; and
2. The conventional channel presents vulnerabilities in the structure, since it can be eavesdropped on by Eve without being noticed by Alice and

Bob, while the quantum channel does not present this vulnerability. In addition, one of the assumptions of the BB84 protocol is that the information exchange between Alice and Bob on the conventional channel can not be changed, which puts a strong requirement on the application of the BB84 protocol.

One more drawback is that the BB84 protocol assumes that Alice and Bob have already authenticated each other before the protocol starts, which leaves the protocol an incomplete one with a strong restriction.

In addition, the BB84 protocol does not have effective mechanisms to defend against Eve's eavesdropping attack. All it has is a passive way to detect Eve's presence during the key distribution process after the protocol has finished running once.

Aiming at the weaknesses of the BB84 protocol, we should improve the protocol in the following aspects:

1. Improving the efficiency of sharing a raw key and a final key, in terms of a faster convergence speed of the keys and a lower communication and computation overheads;
2. Introducing effective detection mechanisms of Eve's eavesdropping activity, and further proposing effective defense mechanisms to frustrate Eve's attack;

3. Removing the basis information exchange between Alice and Bob on the conventional channel, and further eliminating the necessity of the conventional channel in the structure, so that the communication overhead and cost are reduced, and the vulnerability coming from the conventional channel as a classical element is removed; and
4. Providing authentication for the two communicating entities at the beginning of the protocol.

3.4.2 Entanglement-Based Quantum Key Distribution Protocol

In 1991 Artur Ekert proposed the first quantum key distribution protocol making use of the phenomenon of quantum entanglement [26], and the protocol is referred to as the E91 protocol. The basic idea behind this entanglement-based quantum key distribution protocol is that if Alice and Bob use the same way to measure the entangled photon pair, then they will get exactly the opposite measurement results, so that they can share a secret key.

Figure 3.11 shows the schematic diagram of the structure of the E91 protocol. Alice and Bob are connected by two channels, one conventional channel, on which classical information is exchanged, and one quantum channel, on which one of the two photons in an entangled photon pair is transmitted to Bob. The entangled photon pair generator is used to generate entangled photon pairs, and

one photon in an entangled photon pair is transmitted to Alice and the other transmitted to Bob.

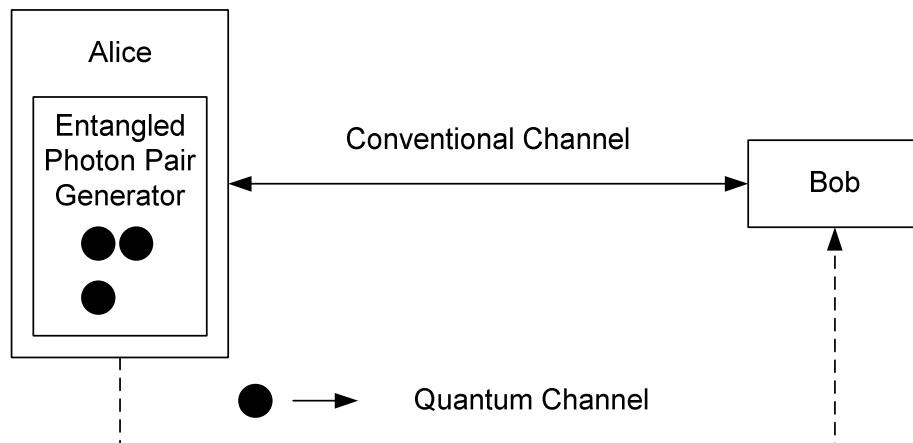


Figure 3.11 Schematic diagram of the structure of the E91 protocol

Alice and Bob need to take the following steps to share a raw key:

1. Alice generates an entangled photon pair, keeps one of the two photons in the pair with her and transmits the other photon to Bob through the quantum channel;
2. Alice randomly selects one of the two possible bases (+ or \times) to measure her qubit, and saves the measurement result;
3. Bob randomly selects one of the two possible bases (+ or \times) to measure his qubit, and saves the measurement result;

4. If Alice and Bob select the same bases, then they will have exactly the opposite measurement results; if Bob selects a different basis from Alice's, then the measurement result he gets is totally random, and later on that measurement result will be discarded;
5. Bob communicates with Alice through the conventional channel about which basis he used to measure his qubit, and Alice tells Bob whether he has used the same basis as she;
6. Alice and Bob discard all the bits on which they used different bases, and save the rest of the bits in a sequence, respectively; and
7. Bob reverses the bit value of his sequence, after which his sequence is the same as Alice's, and that sequence is the raw key shared between Alice and Bob.

After Alice and Bob share the raw key, they need to go through the information reconciliation and privacy amplification procedures to get a final key. From there on, the E91 protocol shares the same procedures as the BB84 protocol.

3.4.3 Other Major Quantum Key Distribution Protocols

In 1991 Charles Bennett proposed a quantum key distribution protocol that made use of two arbitrary nonorthogonal quantum states to distribute a key [27].

Charles Bennett, Gilles Brassard, and David Mermin presented a quantum key distribution protocol making use of the quantum entanglement without Bell's Theorem in 1992 [28], which is simpler than the E91 protocol and equivalent to the BB84 protocol. Instead of using either the polarization state of a photon or an entangled photon pair to distribute a key, Kyo Inoue, Edo Waks, and Yoshihisa Yamamoto used the phase difference between two pulses of a photon to carry a bit information and distribute a key, which is more suitable for the transmission in fibers [29]. In 2006, Subhash Kak proposed a three-stage quantum cryptography protocol to distribute a key, in which the communication remains quantum in each stage [30]. Some discussions on the Kak's three-stage protocol are available in references [86-90].

3.5 Quantum Key Distribution in Practices

Quantum key distribution techniques have evolved very fast recently. On April 21, 2004, the world's first bank transfer using entanglement-based quantum key distribution took place in Vienna [65]. The Mayor of the Vienna City sent an online wire transfer from the Vienna City Hall to the headquarter of Bank-Austria Creditanstalt. The record of free-space quantum key distribution was achieved in 2006 between the Canary Islands of La Palma and Tenerife via a satellite based optical free-space link, and an entangled photon pair was

transmitted over a distance of 144 km [91]. The longest fiber quantum key distribution was accomplished by Los Alamos National Laboratory and National Institute of Standards and Technology together in 2006. They were able to transmit a photon using phase-coding quantum key distribution method over 148.7 km [92].

Commercial products of quantum key distribution are available on the market already, which so far are used more in military than in business. The four companies that are offering quantum key distribution products are: a Swiss company called “id Quantique” [93], a U.S. company named “MagiQ Technologies” [94], a French company “SmartQuantum” [95], and an Australian company “QuintessenceLabs Pty Ltd” [96].

3.6 Summary

In this chapter we introduced the basis of quantum cryptography, including the polarization state of light, qubits, the two primary theorems on which quantum cryptography is based, i.e., the Heisenberg Uncertainty Principle and the No-Cloning Theorem, and the very astonishing quantum property – quantum entanglement. We explained the unconditional security provided by quantum cryptography, and introduced several major quantum key distribution protocols, with the emphasis on the first quantum key distribution protocol, the BB84

protocol, and the first entanglement-base quantum key distribution protocol – the E91 protocol, followed by the achievements of quantum key distribution techniques in practices. Within the introduction of the BB84 protocol, we elaborated the details in many aspects, including the two bases used in the protocol, namely, the rectilinear basis and the diagonal basis, the representation of classical bits by polarized single photons, how to measure polarized single photons using a polarizing beam splitter, the structure of the protocol, the assumptions it requires, the steps to share a raw key and obtain a final key, the weaknesses of the protocol, and what should be done to improve the efficiency of the BB84 protocol as well.

Chapter 4 Key Distribution Using a Dual-Quantum Channel

4.1 Introduction

As we discussed in Chapter 3, the BB84 protocol has a very low efficiency in getting a raw key and a final key, and it does not have effective defense mechanisms against Eve's eavesdropping attack. Here the "low efficiency" means that it takes a long time, a high communication overhead and computation overhead to only get a short final key. Aiming at the low efficiency problem of the BB84 protocol, in this chapter, we present a method to speed up the convergence process of the final key at a lower cost and yet provide a better defense mechanism against Eve, making use of a dual-quantum channel structure and a complementary measuring basis selection rule.

4.2 Dual-Quantum Channel Structure

The schematic diagram of the structure of the quantum key distribution protocol to be presented in this chapter is shown in Figure 4.1.

In the proposed structure, two communicating entities, Alice and Bob, who wish to establish a secret key between them, are connected by three channels, one of which is a conventional channel, and the other two of which are two quantum channels. The two quantum channels are referred to as a dual-quantum

channel. The conventional channel is just a regular telecommunication channel, which is used to exchange classical information between Alice and Bob. The dual-quantum channel is composed of two optical fibers, on which qubits are transmitted from Alice to Bob.

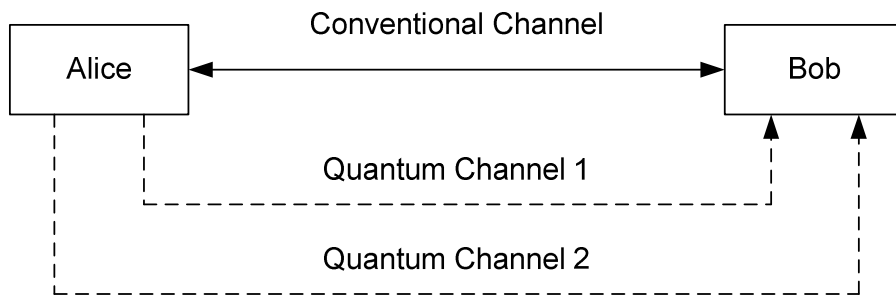


Figure 4.1 Schematic diagram of the structure of the proposed protocol

4.3 Complementary Measuring Bases

In the BB84 protocol, at Bob’s measuring side, he randomly chooses one of the two possible bases (+ or \times) for each of the qubits received on the quantum channel. In this protocol, we have two quantum channels, and how to take advantage of the channel diversity offered by the dual-quantum channel and choose bases for the dual-quantum channel becomes a critical issue. In this section, we introduce a technique called “complementary measuring basis selection rule”.

Since the two bases used in this protocol cover all the four polarization states of a photon, with each basis covering two orthogonal polarization states, these two bases are said to be complementary to each other. Instead of using randomly selected measuring bases on both of the two quantum channels, which makes the two quantum channels independent of each other, we use randomly chosen bases on one quantum channel, and use the complementary bases on the other quantum channel on purpose. In doing so, the two independent quantum channels correlate to each other and form a dual-quantum channel. An example of the complementary bases used by Bob on the dual-quantum channel is shown in Table 4.1.

Table 4.1 Bob's complementary measuring bases used on the dual-quantum channel

| | | | | | | | | |
|-----|---|---|---|---|---|---|---|---|
| QC1 | + | + | × | × | × | + | × | + |
| QC2 | × | × | + | + | + | × | + | × |

QC1, 2: Quantum Channel 1, 2

For example, if Bob randomly chooses the rectilinear basis (+) for the first qubit on quantum channel 1, then he uses, on purpose, the complementary basis, i.e., the diagonal basis (×) for the first qubit on quantum channel 2, and so forth.

4.4 The Proposed Protocol

In the proposed protocol, the definitions of the bases and the representation of classical bits by polarized single photons remain the same as in the BB84 protocol. Alice and Bob need to take the following steps to share a raw key between them:

1. Alice generates a sequence of random 0's and 1's;
2. Alice randomly chooses one of the two possible bases (+ or \times) for each of the bits generated in step 1;
3. According to the basis selected, Alice represents each of the random bits by two polarized single photons with identical polarization states according to Table 3.1 and sends each of the polarized single photons on one of the two quantum channels. For example, for a bit 1 and a rectilinear basis, Alice generates two vertically polarized single photons and transmits one photon on quantum channel 1 and the other on quantum channel 2;
4. At Bob's measuring side, he adopts the complementary measuring basis selection rule to select bases and measure the qubits received on the two quantum channels. He randomly selects one of the two possible bases (+ or \times) to measure the polarized single photon received on quantum channel 1, and for the corresponding polarized single photon received on

quantum channel 2, he uses, on purpose, the complementary basis of the basis used on quantum channel 1 to measure it;

5. Bob communicates with Alice through the conventional channel about which basis he used to measure each of the polarized single photons on quantum channel 1, and Alice tells Bob for which qubit he used the same basis as she; for those qubits Bob used different bases from Alice's on quantum channel 1, he knows that on quantum channel 2 he must have used the same bases as Alice, since he chose the complementary bases on quantum channel 2. For example, if Bob chooses the diagonal basis (\times) to measure the polarized single photon on quantum channel 1, and he is told by Alice that the diagonal basis is different from hers, then he can deduce that the complementary basis, i.e., the rectilinear basis ($+$) used by him on quantum channel 2 must coincide with Alice's basis; and
6. Bob saves the measurement results of the qubits on which he used the same bases as Alice on the two quantum channels, and discards the rest of the measurement results on which he used different bases from Alice's. The saved measurement results form a sequence, which is the raw key shared between Alice and Bob.

As explained before, if Alice and Bob use different bases on a bit/qubit, then they will share the same information only half of the time, which is why this bit of information can not be included into the raw key and has to be discarded.

Only the qubit on which they use the same bases can yield the same bit of information for both Alice and Bob, and only in this situation can the bit of information be saved into the raw key.

So far, Alice and Bob finish the process of sharing a raw key. If the eavesdropper, Eve, was not present during the key distribution process, then the raw keys shared between Alice and Bob would be exactly the same; however, if Eve was present during the key distribution process, then the raw keys shared between Alice and Bob would not be exactly the same, with some of the bits differing from each other. In this case, the information reconciliation and privacy amplification procedures need to be adopted to distill a final key from the raw key, about which Eve has an arbitrarily low level knowledge. An example of the proposed protocol is shown in Table 4.2.

Table 4.2 An example of the proposed protocol

| | | | | | | | | | |
|-------|----------------|--------|--------|--------|--------|--------|--------|--------|--------|
| Alice | Step 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |
| | Step 2 | + | × | + | × | + | + | × | × |
| | Step 3/ QC1 | ↑ | ↖ | → | ↗ | ↑ | → | ↖ | ↗ |
| | Step 3/ QC2 | ↑ | ↖ | → | ↗ | ↑ | → | ↖ | ↗ |
| Bob | Step 4/ QC1 | × | ⊗ | ⊕ | + | ⊕ | × | + | ⊗ |
| | Step 4/ QC2 | ⊕ | + | × | ⊗ | × | ⊕ | ⊗ | + |
| | Step 5/ QC1 | 0 or 1 | 1 | 0 | 0 or 1 | 1 | 0 or 1 | 0 or 1 | 0 |
| | Step 5/ QC2 | 1 | 0 or 1 | 0 or 1 | 0 | 0 or 1 | 0 | 1 | 0 or 1 |
| | Step 6 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |

QC1, 2: Quantum Channel 1, 2; ○ : Correct basis or bit

4.5 Raw Key Efficiency, Final Key Efficiency, and Raw Key Error Rate

In order to evaluate how efficiently a protocol can obtain a raw key and a final key from the original random bits generated by Alice, we define two parameters, raw key efficiency and final key efficiency. Raw key efficiency is defined as the length of the raw key shared by Alice and Bob divided by the length of the original random bits generated by Alice. Final key efficiency is defined as the

length of the final secret key (after all necessary procedures) divided by the length of the original random bits generated by Alice.

In order to describe how well the raw key in Alice's possession accords with the raw key in Bob's possession, we extend the definition of "error rate" in the circumstance of the raw key. The raw key error rate is defined as the length of the erroneous bits (those bits in the raw keys that are different between Alice and Bob) in the raw key divided by the length of the raw key. The erroneous bits in the raw key could be caused by the imperfection of the quantum channel, or the eavesdropping activity of the eavesdropper. In this dissertation we mainly consider the impact caused by Eve's eavesdropping activity.

4.6 Raw Key Efficiency and Raw Key Error Rate in Different Scenarios with or without the Presence of Eve

In the following, we are going to analyze the raw key efficiency and raw key error rate under several different scenarios classified according to whether Eve is present or not, on either or both of the two quantum channels. Three different scenarios apply:

1. Eve is not present on either of the two quantum channels;
2. Eve is present on one of the two quantum channels; and
3. Eve is present on both of the two quantum channels.

4.6.1 Eve is not Present on Either of the Two Quantum Channels

In this case, we can break down the entire key distribution process into two parts, with each part being one quantum channel, and analyze them one by one.

On quantum channel 1, for a bit transmitted by Alice, Bob randomly chooses one of the two bases to measure that qubit, and he has 50% of the probability of choosing the same basis as Alice and getting the same bit as Alice's. On average, on quantum channel 1, Alice and Bob end up with sharing 50% of the original random bits as their raw key.

On quantum channel 2, because Bob uses the complementary bases to measure the qubits, for those qubits which he did not choose the same bases as Alice on quantum channel 1, he would choose the same bases as Alice on quantum channel 2. This includes the remaining 50% of the original random bits generated by Alice into the raw key. So totally, from the two quantum channels, Alice and Bob end up with sharing 100% of the original random bits as their raw key, with each quantum channel contributing to 50% of the final raw key, which makes the raw key efficiency 100%.

Regarding the raw key error rate, if Eve is not present on either of the two quantum channels, then there would be no errors in the raw key, thus the raw key error rate is 0%.

4.6.2 Eve is Present on One of the Two Quantum Channels

When Eve is present during the key distribution process, she may have access to only one quantum channel or she may choose to eavesdrop on only one quantum channel to avoid being detected by Alice and Bob. Let us suppose Eve is eavesdropping on quantum channel 2.

According to the analysis in Section 4.6.1, if Eve is not present on quantum channel 1, then Alice and Bob will end up with sharing 50% of the original random bits as their raw key from quantum channel 1, and there will be no error in that part of raw key obtained from quantum channel 1 due to the absence of Eve. So the raw key efficiency and raw key error rate on quantum channel 1 are 50% and 0%, respectively.

Now let us consider the situation that Eve is present on quantum channel 2. The fact that Bob's bases on quantum channel 2 will still coincide with Alice's for the other 50% of the original random bits, no matter whether Eve is present or not, is not changed. What is changed is the raw key error rate due to Eve's presence, since her eavesdropping activity can bring errors into the raw key obtained from quantum channel 2. The maximal raw key error rate Eve can bring into the raw key obtained from quantum channel 2 is 25%, if she eavesdrops on all the other 50% of the original random bits on quantum channel 2, which is explained in Table 4.3.

Table 4.3 The maximal raw key error rate Eve can bring into the raw key is 25% when Eve eavesdrops on all the qubits transmitted on a quantum channel

| | | | | | |
|--------------------------|-----|-------|-------|-------|-------|
| Alice's random bit | 1 | | | | |
| Alice's random basis | + | | | | |
| Qubit generated by Alice | ↑ | | | | |
| Eve's random basis | + | × | | | |
| Eve's measurement result | ↑ | ↗ | | ↖ | |
| Qubit resent by Eve | ↑ | ↗ | | ↖ | |
| Bob's random basis | + | | | | |
| Bob's measurement result | ↑ | → | ↑ | → | ↑ |
| Bob's bit | 1 | 0 | 1 | 0 | 1 |
| Probability | 50% | 12.5% | 12.5% | 12.5% | 12.5% |
| Error rate | 0% | 12.5% | 0% | 12.5% | 0% |

For a bit of the raw key obtained from quantum channel 2, Eve has 50% probability of choosing the same basis as Alice and Bob, and in this case, Eve does not bring any error into the raw key. However, since Eve also has another 50% probability of choosing a different basis from Alice's and Bob's, after she measures and resends her qubit to Bob, Bob measures it with a different basis and gets either a 0 or 1 with 50% probability, respectively. This means with a

different basis, Bob gets a 0 or 1 randomly. Eventually, from Table 4.3 we can figure out that the probability that Bob gets a 0 instead of the supposed 1 is 25%, and that is the maximal error rate Eve can bring into a raw key by her eavesdropping activity. So the maximal raw key error rate on quantum channel 2 is 25%.

When combining the two quantum channels together and considering them as a whole, the raw key efficiency becomes $50\%+50\%=100\%$ and the average raw key error rate is equal to $0\%*50\%+25\%*50\%=(0\%+25\%)/2=12.5\%$.

4.6.3 Eve is Present on Both of the Two Quantum Channels

When Eve is present on quantum channel 1, according to the analysis in Section 4.6.2, the raw key efficiency and maximal raw key error rate are 50% and 25%, respectively. It is the same on quantum channel 2 when Eve is present, with the raw key efficiency and maximal raw key error rate being 50% and 25%, respectively. So in all, when Eve is present on both of the two quantum channels, the raw key efficiency is $50\%+50\%=100\%$, and the maximal raw key error rate is $25\%*50\%+25\%*50\%=(25\%+25\%)/2=25\%$.

4.7 Making Use of the Difference between the Two Raw Key Error Rates on the Two Quantum Channels to Speed up the Key Distribution Process and Frustrate Eve

We can take advantage of the channel diversity brought by the dual-quantum channel structure to speed up the process of obtaining the final key and better frustrate Eve.

If Eve is not present during the key distribution process at all, then there would be no errors in the raw key, and hence this raw key can be used directly as the final key to encrypt messages. Sometimes, Eve may be eavesdropping on both of the two quantum channels, bringing a maximum of 25% errors into the raw key. In this case, the information reconciliation and privacy amplification procedures need to be adopted to remove the errors in the raw key and distill a final key from the raw key. However, as analyzed before, this process is very effort-consuming and has very low efficiency. Only a very small size of the final key can be obtained after the information reconciliation and privacy amplification procedures.

Sometimes Eve may not have access to both of the two quantum channels, so she only eavesdrops on one quantum channel, or she may choose to eavesdrop on only one quantum channel to try to avoid being detected by Alice and Bob. If Alice and Bob could find out that, during a certain period of time, the raw key

error rate on one quantum channel is significantly lower (it is also possible that the raw key error rate is 0%, which gives Alice and Bob an even greater advantage) than that on the other quantum channel, then they can take advantage of this situation by using the measurement results only on the quantum channel where the raw key error rate is lower (or 0%), and keep sending decoy information on the other quantum channel where there is a higher raw key error rate and Eve is actively eavesdropping. By doing so, Alice and Bob can have the benefit that the processing time of obtaining the sifted key through the information reconciliation procedure is much shorter by using a raw key with a lower error rate. The reason is simply that less work is needed by the information reconciliation procedure when dealing with a raw key with a lower error rate. Ideally, if the raw key error rate on one quantum channel is 0%, which means that Eve does not eavesdrop on that channel at all, then all the measurement results from that quantum channel can be used directly as the final key, without even going through the tedious information reconciliation and privacy amplification procedures. In this case, the final key can be achieved in a much faster way, and the length of the final key is much longer than if the privacy amplification procedure is deployed. At the same time, Alice and Bob keep sending decoy information on the other quantum channel on which Eve is focusing on eavesdropping, so that Eve's attention is drawn to the decoy quantum channel instead of the quantum channel that is actually transmitting the

real information, Figure 4.2. As a result, Eve’s eavesdropping attempt is restricted within the decoy quantum channel and her eavesdropping attack is effectively frustrated.

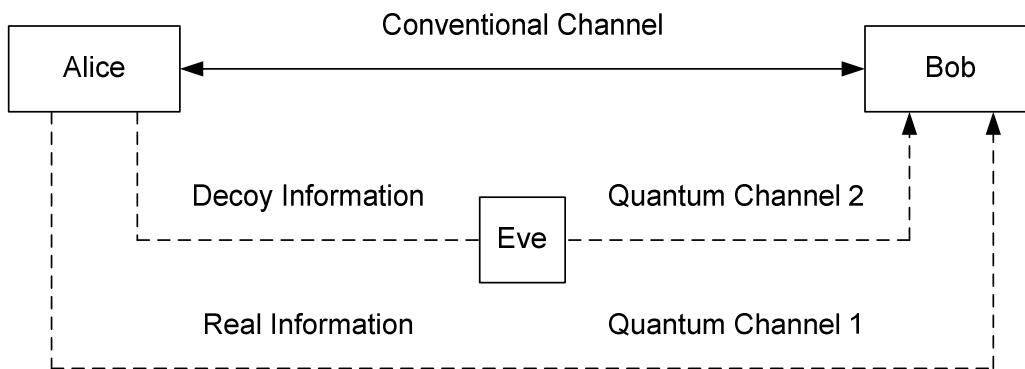


Figure 4.2 Transmitting decoy information on the quantum channel on which Eve is actively eavesdropping while sending real information on the other quantum channel on which Eve is not eavesdropping

4.8 Making Use of an Initialization Vector Shared between Alice and Bob to Improve the Convergence Speed of the Final Key and Frustrate Eve

We introduce an initialization vector (IV) shared between Alice and Bob to help speed up the key distribution process as well as deter Eve. We show that, with

the aid of an initialization vector, Alice and Bob can obtain the final key in a much faster way and have a better defense against Eve's attacks.

The raw key error rate can be calculated either as an average of the two quantum channels or separately as described in Section 4.7. It does not matter how the raw key error rate is calculated. After Alice and Bob get the raw key, they adopt the information reconciliation procedure to obtain a sifted key. After getting the sifted key, instead of proceeding to the next step as usual, i.e., the privacy amplification procedure, Alice and Bob simply XOR the sifted key with the initialization vector shared between them, and the result of the XOR operation is the final key, Figure 4.3.

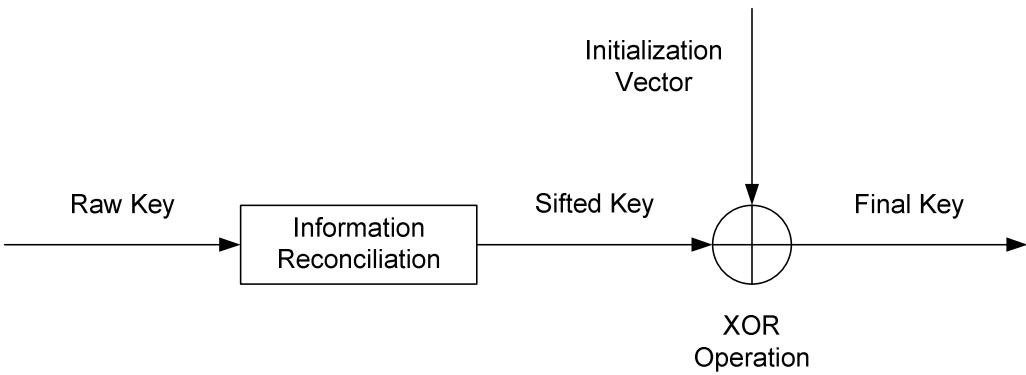


Figure 4.3 Obtaining the final key by XORing the sifted key with the initialization vector shared between Alice and Bob

As we know, the privacy amplification procedure is a very tedious process that reduces the length of the final key dramatically. Since it is not deployed here, the length of the final key obtained is the same as the length of the sifted key, which is usually a little shorter than the length of the raw key, however, may be hundreds of times, if not thousands, longer than that of the final key if the privacy amplification procedure is deployed. And since the privacy amplification procedure is not deployed, the final key can be obtained much faster. Further, since Eve has absolutely no knowledge about the initialization vector shared between Alice and Bob, she would not have any knowledge about the final key either. This way, Eve is effectively frustrated.

4.9 Security Analysis and Solutions

Just like the BB84 protocol and all the other quantum key distribution protocols, the proposed protocol is also subject to the eavesdropping attack. During the eavesdropping attack, Eve not only brings errors into the raw key, but also gains some information about the raw key. In order to reduce or even eliminate Eve's knowledge about the raw key, several methods can be adopted.

First, we can set up a threshold for the error rate of the raw key shared between Alice and Bob. From previous analysis we notice that if Eve is present on only one quantum channel, then she will bring a maximum of 12.5% errors to

the raw key. Thus we may set the threshold at 12.5%. If Alice and Bob find out that 12.5% or more of the raw key is in error after comparison, they discard the raw key and start the proposed protocol all over again until they get a raw key with an error rate that is lower than the threshold, Figure 4.4. This way, Alice and Bob can detect Eve's presence and prevent Eve from knowing too much information about the raw key. In practice, when we consider the imperfection of the transmission of the qubits on the quantum channels, we need to set the threshold to a lower value to compensate the impact on the raw key error rate that is caused by the imperfect transmission, since the error rate we really want to deal with is the one caused by Eve's eavesdropping activity, not the one caused by the imperfect transmission.

If the raw key passes the threshold test, then Alice and Bob are pretty sure that either Eve was not present on the quantum channels, or she only eavesdropped on a part of the bits transmitted by Alice during her presence. In this case, we know that Eve may get partial knowledge of the raw key, but not to a significant extent. Even so, we still want to further reduce Eve's knowledge about the raw key to an even lower level to provide higher confidence. In order to achieve this goal, Alice and Bob need to adopt the information reconciliation and privacy amplification procedures to distill a final key out of the raw key, about which Eve does not have any knowledge.

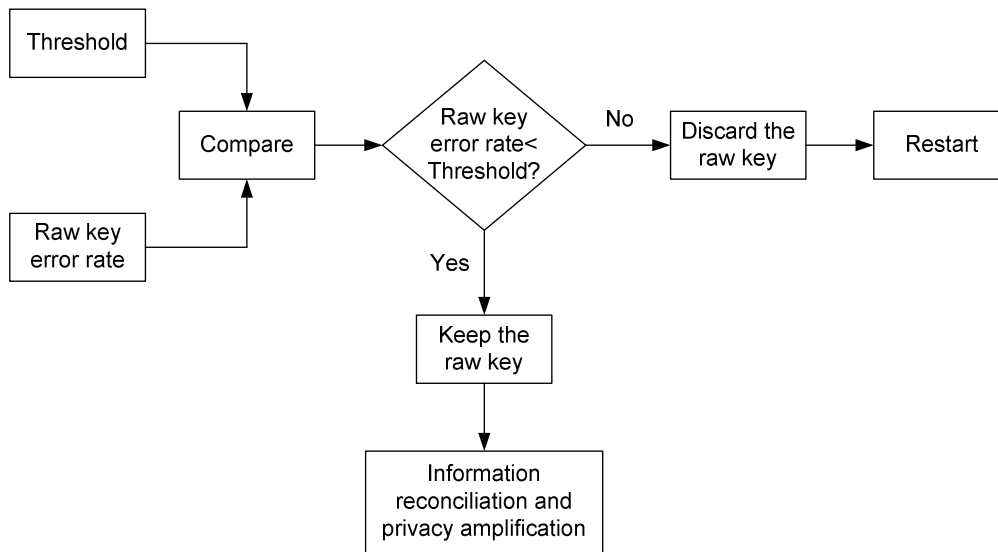


Figure 4.4 Comparing the raw key error rate with the preset threshold to decide whether a raw key should be kept or discarded

Since there are two quantum channels in the proposed protocol, Eve may not have access to both of the two quantum channels at a certain time or she may choose to eavesdrop on only one quantum channel instead of two to avoid being detected by Alice and Bob. If Eve is eavesdropping on only one quantum channel and leaves the other one intact, then by comparing the raw key error rates on the two quantum channels, Alice and Bob can figure out on which quantum channel Eve is eavesdropping and on which she is not eavesdropping. In this situation, Alice and Bob can keep sending decoy information on the quantum channel that is being eavesdropped on by Eve to attract her attention,

and sending real information on the other quantum channel, on which Eve is not eavesdropping. By doing so, Eve's eavesdropping attack can be easily frustrated.

Compared to deploying the privacy amplification procedure to eliminate Eve's knowledge about the final key, Alice and Bob can adopt a better solution, which is to make use of the initialization vector shared between them to obtain the final key in a much faster, and much more efficient way, while at the same time frustrate Eve's eavesdropping attack effectively. After getting the raw key, Alice and Bob perform the information reconciliation procedure to remove the errors in the raw key and get the sifted key, then they simply XOR the sifted key with the initialization vector to obtain the final key. Since the initialization vector is shared and known to only Alice and Bob, about which Eve does not have any knowledge, she would not be able to get any knowledge about the final key either. This way, the tedious and length-devastating privacy amplification procedure is skipped, which not only results in a faster and securer way to obtain the final key, but also increases the length of the final key dramatically. In other words, the convergence speed as well as the efficiency of obtaining the final key is greatly improved.

4.10 Comparison to the BB84 Protocol

4.10.1 Differences between the Proposed Protocol and the BB84 Protocol

The proposed protocol differs from the BB84 protocol in the following aspects:

1. The proposed protocol uses two quantum channels (a dual-quantum channel) to transmit qubits, while the BB84 protocol uses only one quantum channel;
2. In the proposed protocol, for each of the random bits generated by Alice, she uses two polarized single photons with identical polarization states, each transmitted through one of the two quantum channels, while in the BB84 protocol, only one polarized single photon is used for each bit; and
3. In the proposed protocol, at Bob's measuring side, he performs two complementary measurements on the two quantum channels using two complementary measuring bases, while in the BB84 protocol, only one random measuring basis is used on the only quantum channel.

Due to the special structure and the diversity brought by the dual-quantum channel, the proposed protocol offers a much better performance than the BB84 protocol, in terms of the efficiency of getting the final key, and the ability to counter Eve's attack.

4.10.2 Performance Comparison between the Proposed Protocol and the BB84 Protocol

In the BB84 protocol, Bob chooses the same bases as Alice only half of the time, which results in that only 50% of the bits generated by Alice are included into the raw key, making the raw key efficiency 50%. While in the proposed protocol, with the aid of the dual-quantum channel structure and the complementary measuring basis selection rule on the two quantum channels, all the bits generated by Alice can be included into the raw key, making the raw key efficiency 100%, which is twice as much as that of the BB84 protocol.

As for the raw key error rate, the maximal raw key error rate of the BB84 protocol, due to Eve's presence, is 25%, while the maximal raw key error rate of the proposed protocol can be 12.5% or 25%, according to how many channels Eve is eavesdropping on. In general, the proposed protocol has a lower raw key error rate than that of the BB84 protocol. Table 4.4 gives a clear comparison about the raw key error rates of the two protocols in different situations.

Compared to the BB84 protocol, the proposed protocol obtains the final key in a much faster and securer manner, and the length of the final key is much longer. In addition, the proposed protocol has the ability to effectively defend against Eve and frustrate her attacks. The techniques we use in the proposed protocol are the following: comparing the raw key error rates on the two quantum channels and using the one with a lower rate key error rate to distill a

final key; sending decoy information on the quantum channel on which Eve is eavesdropping to fool her, while getting the final key directly from the other eavesdropping-free quantum channel; and XORing the sifted key with the initialization vector shared between Alice and Bob to obtain a secure final key, about which Eve does not have any knowledge. All these features offered by the proposed protocol are not available to the BB84 protocol.

Table 4.4 Comparison of the raw key error rate in different scenarios between the BB84 protocol and the proposed protocol

| QC | BB84 protocol | QC1 | QC2 | Proposed protocol |
|----|---------------|-----|-----|-------------------|
| 0 | 0% | 0 | 0 | 0% |
| 1 | 25% | 0 | 1 | 12.5% |
| | | 1 | 0 | |
| | | 1 | 1 | 25% |

QC – Quantum Channel; 0 – Eve is not present; 1 – Eve is present

4.11 Conclusion

The BB84 protocol has a low raw key efficiency, a very low final key efficiency and a high raw key error rate. In this chapter we presented a new quantum key

distribution protocol using a dual-quantum channel and a complementary measuring basis selection rule to improve the raw key efficiency, the final key efficiency, and reduce the raw key error rate. It was proved that the proposed protocol offers a much higher raw key efficiency and a lower raw key error rate than those of the BB84 protocol. We analyzed different scenarios according to whether Eve is present or not during the key distribution process. We proposed several techniques to eliminate Eve's knowledge about the raw key and the final key to frustrate her attacks. With the techniques presented in this chapter, Alice and Bob share a much longer final key in a much faster, securer way than the BB84 protocol; while at the same time frustrate Eve's attack effectively.

Chapter 5 Quantum Key Distribution Using a Novel Basis

Selection Rule

5.1 Introduction

In Chapter 4 we introduced the dual-quantum channel structure and complementary measuring bases used by Bob on the two quantum channels to improve the efficiency of the key distribution process. In this chapter, we will present a new quantum key distribution protocol to improve the convergence speed of the final key and effectively deter Eve by using a novel basis selection rule on the dual-quantum channel with the aid of an initialization vector shared between Alice and Bob. The structure of this protocol follows the one presented in Chapter 4, but in addition to that, Alice and Bob are required to have an Initialization Vector (IV) shared between them, Figure 5.1.

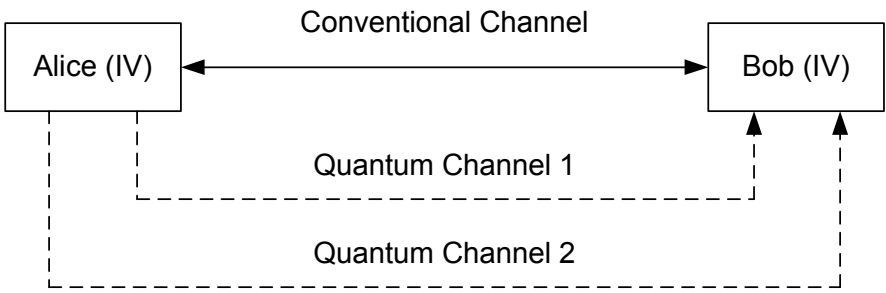


Figure 5.1 Schematic diagram of the structure of the proposed protocol

5.2 A Novel Basis Selection Rule on the Dual-Quantum Channel

With the aid of an initialization vector shared between them, Alice and Bob make a prior agreement about how to select bases on the two quantum channels. Alice and Bob can agree that for the bit 1 in the initialization vector, Alice would randomly choose one of the two possible bases for each of the bits on quantum channel 1, and use the same random basis on quantum channel 2; and Bob would randomly choose a basis for each of the polarized single photons received on quantum channel 1, and use the complementary basis on quantum channel 2. The basis selection for the bit 0 in the initialization vector is the opposite of bit 1 on the two quantum channels, which is as follows: Alice would randomly choose one of the two possible bases for each of the bits on quantum channel 1, and use the complementary basis on quantum channel 2; and Bob would randomly choose a basis for each of the polarized single photons received on quantum channel 1, and use the same random basis on quantum channel 2. The basis selection on the two quantum channels according to the value of the initialization vector is summarized in Table 5.1.

Table 5.1 Basis selection on the dual-quantum channel according to the value of the initialization vector shared between Alice and Bob

| Initialization Vector | Alice | | Bob | |
|-----------------------|--------------|---------------------|--------------|---------------------|
| | QC1 | QC2 | QC1 | QC2 |
| 1 | Random basis | Same random basis | Random basis | Complementary basis |
| 0 | Random basis | Complementary basis | Random basis | Same random basis |

5.3 The Proposed Protocol

Alice and Bob need to take the following steps to share a raw key, making use of the basis selection rule with the aid of an initialization vector shared between them:

1. Alice generates a sequence of random 0's and 1's;
2. For each of the bits generated in the first step, Alice selects two bases, one for quantum channel 1, and the other for quantum channel 2, according to the corresponding bit value in the initialization vector (Table 5.1);
3. Alice represents each of the bits by two polarized single photons according to the bases selected in the second step and the representation of bits by polarized single photons as introduced in Table 3.1, and sends

one polarized single photon on quantum channel 1, and the other on quantum channel 2;

4. Bob selects a measuring basis for each of the qubits received on quantum channel 1 and quantum channel 2, respectively, according to the corresponding bit value in the initialization vector (Table 5.1), and measures the polarized single photons;
5. Bob communicates with Alice through the conventional channel about which basis he used to measure each of the polarized single photons on quantum channel 1, and Alice tells Bob for which qubits he used the same basis as she; and Bob can deduce, for which qubits on quantum channel 2 he has selected the same basis as Alice, according to the bit values of the initialization vector; and
6. Bob saves all the measurement results for which he used the same bases as Alice on the two quantum channels in a sequence, and that sequence is the raw key shared between them.

An example of the proposed protocol is shown in Table 5.2.

Table 5.2 An example of the proposed protocol

| Initialization Vector | | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 |
|-----------------------|----------------|--------|--------|--------|--------|--------|--------|--------|--------|
| Alice | Step 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |
| | Step 2/ QC1 | + | ⊗ | × | ⊕ | × | + | ⊗ | ⊕ |
| | Step 2/ QC2 | ⊕ | + | ⊗ | × | ⊕ | ⊗ | × | + |
| | Step 3/ QC1 | ↑ | ↖ | ↗ | → | ↖ | → | ↖ | → |
| | Step 3/ QC2 | ↑ | ↑ | ↗ | ↗ | ↑ | ↗ | ↖ | → |
| Bob | Step 4/ QC1 | × | ⊗ | + | ⊕ | + | × | ⊗ | ⊕ |
| | Step 4/ QC2 | ⊕ | × | ⊗ | + | ⊕ | ⊗ | + | × |
| | Step 5/ QC1 | 0 or 1 | 1 | 0 or 1 | 0 | 0 or 1 | 0 or 1 | 1 | 0 |
| | Step 5/ QC2 | 1 | 0 or 1 | 0 | 0 or 1 | 1 | 0 | 0 or 1 | 0 or 1 |
| Step 6 | | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |

QC1, 2: Quantum Channel 1, 2; ○ : Correct basis or bit

5.4 Raw Key Efficiency

The raw key efficiency of this protocol is 100%. It is guaranteed in this protocol that all of the random bits generated by Alice are included into the raw key, with each of the two quantum channels contributing to half of the raw key. This is realized by the novel selection rule of the bases on the two quantum channels. From Table 5.2 we can find out that, no matter what the bit value of the initialization vector is, it is ensured that on one of the two quantum channels,

there is one pair of bases, and only one pair, that will coincide. For example, if the bit value of the initialization vector is 1, Alice randomly selects the rectilinear basis (+) for quantum channel 1 and uses the same random basis, which is the rectilinear basis (+), for quantum channel 2, and Bob randomly selects the diagonal basis (\times) for quantum channel 1 and uses the complementary basis, which is the rectilinear basis (+), for quantum channels 2, then there is a coincidence on quantum channel 2, since both of them select the rectilinear basis. This way, there has to be a basis coincidence for each bit, happening either on quantum channel 1 or on quantum channel 2, which guarantees the 100% raw key efficiency.

5.5 Raw Key Error Rate

According to whether Eve is present or not, on either or both of the two quantum channels, there are three different scenarios that determine the raw key error rate:

1. Eve is not present on either of the two quantum channels;
2. Eve is present on one of the two quantum channels; and
3. Eve is present on both of the two quantum channels.

In the following, we are going to analyze the three scenarios one by one.

5.5.1 Eve is not Present on either of the Two Quantum Channels

If Eve is not present during the key distribution process, then there would be no error in the raw key, hence the raw key error rate is 0%.

5.5.2 Eve is Present on One of the Two Quantum Channels

When Eve is present on one of the two quantum channels, for example, on quantum channel 1, her presence would bring a maximum of 25% errors into the part of the raw key obtained from quantum channel 1. Since Eve is not present on quantum channel 2, that part of the raw key obtained from quantum channel 2 is error-free. Because each quantum channel contributes to half of the final raw key, on average, Eve's presence on one quantum channel would bring a maximum of $25\% * 50\% + 0\% * 50\% = (25\% + 0\%) / 2 = 12.5\%$ errors into the final raw key, which results in a 12.5% raw key error rate.

5.5.3 Eve is Present on both of the Two Quantum Channels

When Eve is present on both of the two quantum channels, the maximal raw key error rate on each quantum channel is 25%, thus the average raw key error rate on the two quantum channels is 25%, maximally.

5.6 Three Ways to Obtain the Final Key

In this protocol, there are three ways to obtain the final key:

1. Distilling the final key from the raw key by going through the information reconciliation and privacy amplification procedures, Figure 5.2;

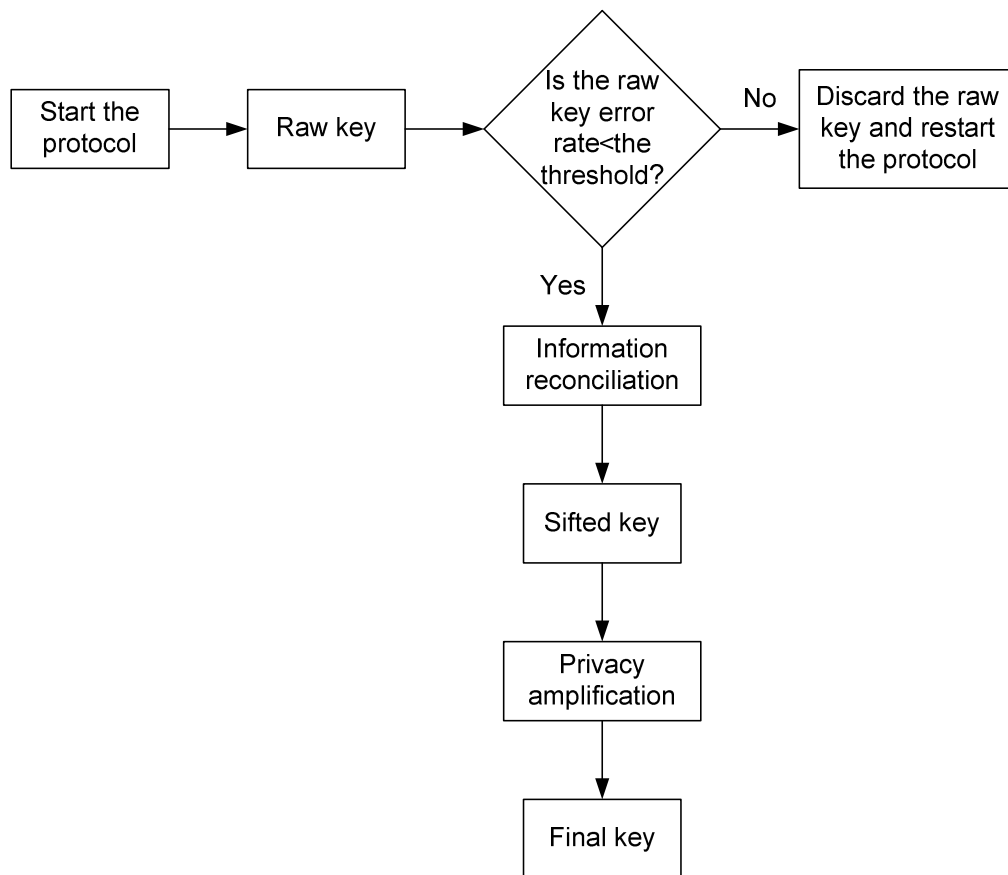


Figure 5.2 Distilling the final key from the raw key by going through the information reconciliation and privacy amplification procedures

2. Figuring out on which quantum channel Eve is not eavesdropping by looking into the raw key error rates on the two quantum channels, and getting the final key directly from the eavesdropping-free quantum channel (previously shown in Figure 4.2);
3. Comparing the difference between the two raw key error rates on the two quantum channels, and getting the final key from the quantum channel with a significantly lower raw key error rate by adopting the information reconciliation and privacy amplification procedures, Figure 5.3; and

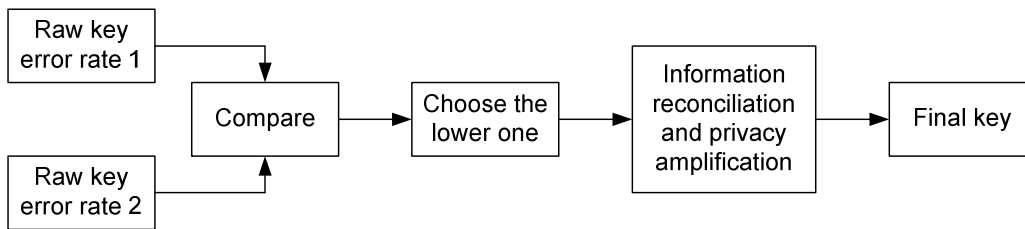


Figure 5.3 Comparing the difference between the two raw key error rates on the two quantum channels and picking the raw key with a lower error rate to obtain the final key

4. XORing the sifted key with the initialization vector shared between Alice and Bob to obtain the final key (previously shown in Figure 4.3).

The first way is the standard method used to obtain the final key after Alice and Bob get the raw key from the two quantum channels. Usually this method

takes a long time and much effort to obtain the final key, and the length of the final key is very small. Thus this method is a low efficiency solution of getting the final key.

Since this protocol provides channel diversity between Alice and Bob, they can use the second and the third method to obtain the final key in a faster manner. If Eve is present on only one of the two quantum channels, then the part of raw key obtained from the quantum channel on which Eve is not present is error-free and can be used directly as the final key. This can be realized by calculating the raw key error rates on the two quantum channels respectively and finding out on which quantum channel Eve is not eavesdropping. If the information reconciliation and privacy amplification procedure are not used to get the final key, the speed of getting the final key will be much faster, and the effort needed to get the final key is much smaller as well. Even if Eve is present on both of the two quantum channels, using the standard method to distill the final key from the quantum channel with a significantly lower raw key error rate is still much faster than in the normal situation, because less error-correcting work is needed for a raw key with a significant lower error rate.

In the fourth way, Alice and Bob can take advantage of the initialization vector shared between them to obtain the final key in a much faster and securer manner. After Alice and Bob get the raw key, they perform the information reconciliation procedure to remove the errors in the raw key and get the sifted

key, and then they XOR the sifted key with the initialization vector to obtain the final key. Since the privacy amplification procedure is not adopted, the convergence speed of the final key is improved, and the length of the final key is kept the same as the length of the sifted key, which is much longer than that of the final key if the privacy amplification procedure is adopted. Since Eve does not have any knowledge about the initialization vector shared between Alice and Bob, she is not able to get any knowledge about the final key either. Thus, by using this method, Alice and Bob can get a longer, securer final key in much a faster way, while Eve can be effectively frustrated at the same time.

5.7 Two Ways to Frustrate Eve's Attack

The proposed protocol offers two effective methods to frustrate Eve's attack, which are realized by the usage of a decoy quantum channel, and an initialization vector shared between Alice and Bob.

Since sometimes Eve may not be able to eavesdrop on both of the two quantum channels, or she may choose to eavesdrop on only one quantum channel strategically, Alice and Bob can figure out on which quantum channel Eve is actively eavesdropping by comparing the raw key error rates on the two quantum channels. After finding out on which quantum channel Eve is actively eavesdropping, Alice and Bob keep sending decoy information on that quantum

channel and switch the real information on the other quantum channel on which she is not tampering with. This way, the information Eve gets is just some fake information, the real information is protected, and Eve's attack is countered.

As we mentioned before, the final key can be achieved by XORing the sifted key with the initialization vector shared between Alice and Bob. Since Eve does not have any knowledge about the initialization vector, she would not have any knowledge about the final key either. This way, Eve's attempt to get the final key is effectively frustrated.

5.9 Conclusion

In this chapter, we introduced a new quantum key distribution protocol that takes advantage of a novel basis selection rule on the two quantum channels with the aid of an initialization vector shared between Alice and Bob and the dual-quantum channel structure to improve the efficiency of the key distribution process, the security of the final key, and effectively frustrate Eve. The basis selection rule and the dual-quantum channel structure make sure that all the random bits generated by Alice in the first step are included into the raw key, which makes the raw key efficiency 100%. The final key is obtained in a much faster and securer way by using the initialization vector shared between Alice and Bob. Eve's attack can be effectively defeated in this protocol by using the

stratagem of fooling Eve with a decoy quantum channel and the initialization vector shared between Alice and Bob.

Chapter 6 Quantum Key Distribution without Basis Information Exchange and the Usage of the Conventional Channel

6.1 Introduction

As we know the conventional channel has been an indispensable component of all the quantum key distribution protocols that have ever been proposed so far, on which classical information regarding the bases used by Alice and Bob and the error correction process of the raw key is transmitted. In this chapter, we are going to introduce a new quantum key distribution protocol in which the basis information exchange on the conventional channel is removed, and further the necessity of the conventional channel in the structure is eliminated. In doing so, the communication overhead is avoided, and the entire structure of the proposed protocol becomes all-quantum, presenting less vulnerability than the traditional structure with a classical element (the conventional channel) in it.

6.2 Roles of the Conventional Channel

In quantum key distribution protocols, the conventional channel is used for the following two purposes:

1. The conventional channel is used to exchange basis information between Alice and Bob. After Bob finishes measuring the qubits received on the

two quantum channels, he needs to tell Alice which basis he used to measure each of the qubits on the two quantum channels through the conventional channel, and then through the same conventional channel, Alice tells Bob which bases he used are the same as hers. After this communication on the conventional channel, both Alice and Bob know exactly for which qubits they have used the same basis, so that they can save those bits as the raw key and delete the rest of the bits for which they have used different bases; and

2. After Alice and Bob share the raw key, they need to check whether Eve has eavesdropped on the raw key during the key distribution process. This is realized by checking if there are any errors in the raw key. If there are errors in the raw key, then they can conclude that Eve was present during the key distribution process. And according to how high the raw key error rate is, they decide whether to keep this raw key or discard it. Basically what they need to do is to send to each other a small portion of the raw key in each person's possession, for example, the first 50 bits of the raw key, and compare the portion received from the other person with their own to see if there is any inconsistency. If there is an inconsistency in the raw key, namely, error, they conclude that Eve has eavesdropped on the raw key. Then they make an estimation of the raw key error rate by calculating the error rate of the portion they exchanged,

and compare the value of the estimated raw key error rate with the threshold set up beforehand to decide whether they should discard or keep the raw key. If the raw key error rate is lower than the threshold, then they keep the raw key and go through the error correction process to remove all the errors in the remaining portion of the raw key, which also needs the conventional channel to transmit classical information between them. After they remove all the errors in the raw key, they do not need the conventional channel any more, since the privacy amplification procedure can be finished on their own without exchanging any information.

The benefit of the elimination of the basis information exchange on the conventional channel is obvious. Since the basis information exchange is not needed, the communication overhead is reduced greatly. And the further elimination of the necessity of the conventional channel in the structure not only totally removes the communication overhead, but also makes the entire structure all-quantum, which are very beneficial to Alice and Bob. That is because only the quantum structure is able to detect Eve's eavesdropping activity, while the classical structure can not, so that the all-quantum structure is less vulnerable to the eavesdropping attack than the hybrid structure (structure with both classical and quantum elements in it).

6.3 The Proposed Protocol

In this section we are going to present a new quantum key distribution protocol in which the basis information exchange is not needed during the key distribution process, and further we will discuss the elimination of the necessity of the conventional channel in the structure.

The basic structure of the proposed protocol follows the previous structure, Figure 6.1. Since the conventional channel is eliminable, we use the bold dashed line to represent the dispensable conventional channel.

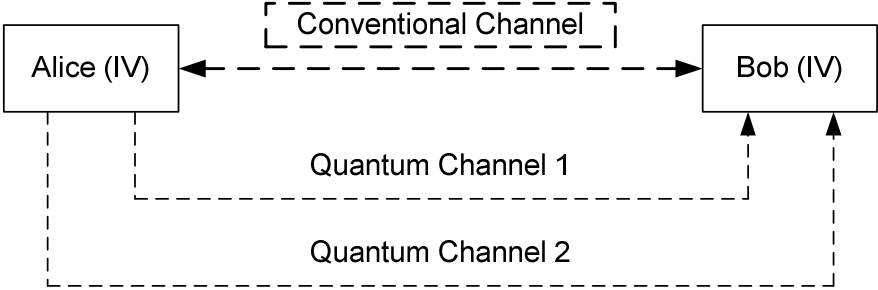


Figure 6.1 Schematic diagram of the structure of the proposed protocol

Before the protocol starts, Alice and Bob need to make an agreement on the selection of the bases on the two quantum channels according to the bit value of the initialization vector shared between them. For example, they may agree that for the bit 1 in the initialization vector, they choose the rectilinear basis for quantum channel 1 and the diagonal basis for quantum channel 2; and for the bit

0 in the initialization vector, they choose the diagonal basis for quantum channel 1 and the rectilinear basis for quantum channel 2. Since Alice and Bob share the same initialization vector, they know exactly which bases the other person uses on the two quantum channels. The selection of bases used on the two quantum channels according to the bit value of the initialization vector is summarized in Table 6.1.

Table 6.1 Selection of bases on the two quantum channels according to the bit value of the initialization vector shared between Alice and Bob

| Initialization Vector | Basis | |
|-----------------------|-------|-----|
| | QC1 | QC2 |
| 1 | + | × |
| 0 | × | + |

Alice and Bob need to take the following steps to share a raw key:

1. Alice generates a sequence of random 0's and 1's;
2. Alice chooses the bases for each of the bits generated in the first step for the two quantum channels according to the value of the corresponding bit in the initialization vector (Table 6.1);

3. According to the representation of bits by polarized single photons (Table 3.1), Alice generates two polarized single photons for each of the bits generated in the first step using the bases selected in the second step and transmits the polarized single photons through quantum channel 1 and quantum channel 2, respectively;
4. At Bob's measuring side, he chooses the basis for each of the qubits received on the two quantum channels according to the value of the corresponding bit in the initialization vector (Table 6.1); and since Bob shares the same initialization vector with Alice, he uses exactly the same bases as Alice on both of the two quantum channels;
5. Bob uses the bases selected in step 4 to measure the polarized single photons received on the two quantum channels; and
6. Bob saves the measurement results in a sequence as the raw key.

An example of the proposed protocol is shown in Table 6.2.

So far the conventional channel has not been used yet. Since Alice and Bob know exactly which bases the other person uses, the basis information exchange between them is not necessary. The conventional channel is also used for the error correction of the raw key, and we will show how to eliminate the error correction procedure and further eliminate the usage of the conventional channel in the structure later on.

Table 6.2 An example of the proposed protocol

| Initialization Vector | | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 |
|-----------------------|----------------|---|---|---|---|---|---|---|---|
| Alice | Step 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |
| | Step 2/ QC1 | + | × | + | × | × | × | + | + |
| | Step 2/ QC2 | × | + | × | + | + | + | × | × |
| | Step 3/ QC1 | ↑ | ↖ | → | ↗ | ↖ | ↗ | ↑ | → |
| | Step 3/ QC2 | ↖ | ↑ | ↗ | → | ↑ | → | ↖ | ↗ |
| Bob | Step 4/ QC1 | ⊕ | ⊗ | ⊕ | ⊗ | ⊗ | ⊗ | ⊕ | ⊕ |
| | Step 4/ QC2 | ⊗ | ⊕ | ⊗ | ⊕ | ⊕ | ⊕ | ⊗ | ⊗ |
| | Step 5/ QC1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |
| | Step 5/ QC2 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |
| Step 6 | | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |

QC1, 2: Quantum Channel 1, 2; ○ : Correct basis or bit

6.4 Raw Key Efficiency and Raw Key Error Rate

The raw key efficiency of this protocol is 100%. The reason is that Alice and Bob both use exactly the same bases as the other person on the two quantum channels, thus all the bits generated by Alice are included into the raw key. Since Alice and Bob both know exactly which bases the other person uses, there is no need for them to exchange basis information through the conventional channel as usual.

Similar to the analyses in the previous chapters, during the key distribution process, Eve may or may not be present, on one or both of the two quantum channels. So three different scenarios apply:

1. Eve is not present during the key distribution process. If Eve is not present, then there would be no errors in the raw key, which makes the raw key error rate 0%, and the raw key automatically becomes the final key shared between Alice and Bob;
2. Eve is present on one quantum channel. If Eve is present on only one quantum channel, then the maximal raw key error rate she can bring into the raw key obtained from that quantum channel is 25%, and the error rate of the other raw key obtained from the other quantum channel on which Eve is not present is 0%. Since both Alice and Bob use exactly the same bases on the two quantum channels, there are two coincidences of basis on the two quantum channels, so that the two measurement results on the two quantum channels for a specific bit should be the same. However, due to Eve's eavesdropping, 25% of the bits in the two raw keys obtained from the two quantum channels are different. For those 25% bits that are different from each other, Bob has to pick up a bit from a quantum channel as the raw key, where he has 50% of probability picking up a wrong bit, which makes the maximal average raw key error rate on the two quantum channels $25% * 50% = 12.5%$; and

3. Eve is present on both of the two quantum channels. If Eve is present on both of the two quantum channels, then the maximal raw key error rates on the two quantum channels are both 25%. From the above analysis in Scenario 2, when the measurement results on the two quantum channels are different, Bob has 50% of probability of choosing the wrong bit. Now, suppose that in the 25% errors of the raw key obtained on quantum channel 1, there are $X\%$ that are the same as the 25% errors of the raw key obtained on quantum channel 2, where $0 \leq X \leq 25$, then the maximal average raw key error rate on the two quantum channels is

$$\frac{25\% - X\%}{2} + X\% + \frac{25\% - X\%}{2} = 25\% .$$

6.5 Four Ways to Obtain the Final Key

The three ways to obtain the final key introduced in the previous chapters can also be used in this protocol. Here we just summarize them briefly:

1. Using the standard information reconciliation and privacy amplification procedures to distill a final key out of the raw key;
2. Comparing the raw key error rates on the two quantum channels respectively, finding out the quantum channel with a significantly lower raw key error rate, and using the measurement results on that quantum

channel by going through the information reconciliation and privacy amplification procedures to distill a final key;

3. Figuring out on which quantum channel Eve is not eavesdropping by calculating the raw key error rates on the two quantum channels, and using the raw key from the eavesdropping-free quantum channel directly as the final key; and
4. XORing the sifted key with the initialization vector shared between Alice and Bob to obtain the final key.

The benefits of the four methods as introduced earlier still apply to this protocol, such as a faster convergence speed of the final key, a securer and longer final key, and effectively frustrating Eve's attacks.

6.6 Two Ways to Frustrate Eve's Attack

The two ways mentioned in Chapter 5 to frustrate Eve's attack can also be used in this protocol, which are as follows:

1. Transmitting decoy information on the quantum channel on which Eve is actively eavesdropping and sending real information on the other quantum channel on which Eve omits or chooses not to eavesdrop; and
2. XORing the sifted key with the initialization vector shared between Alice and Bob to get the final key and frustrate Eve.

6.7 Real-Time Detection Mechanisms of Eve's Presence during the Key Distribution Process

Besides the two ways to frustrate Eve's attack mentioned in Section 6.6, there are three additional detection mechanisms in this protocol that are able to detect Eve's presence in real time:

1. If Eve is present during the key distribution process, she would bring errors into Bob's measurement results on the two quantum channels, which generally will make the two corresponding measurement results on the two quantum channel differ from each other. Bob would notice the conflict between the two measurement results on the two quantum channels when he has to decide which one of the two measurement results to choose as the raw key. As soon as Bob notices this conflict, he knows Eve is present, Figure 6.2. For example, for a random bit 1 generated by Alice and transmitted on the two quantum channels as two polarized single photons, due to Eve's interference, Bob may get a 1 on quantum channel 1 and a 0 on quantum channel 2. If this situation happens, then Bob will not know which one of the measurement results should be chosen as the raw key, thus he can conclude that Eve is eavesdropping.

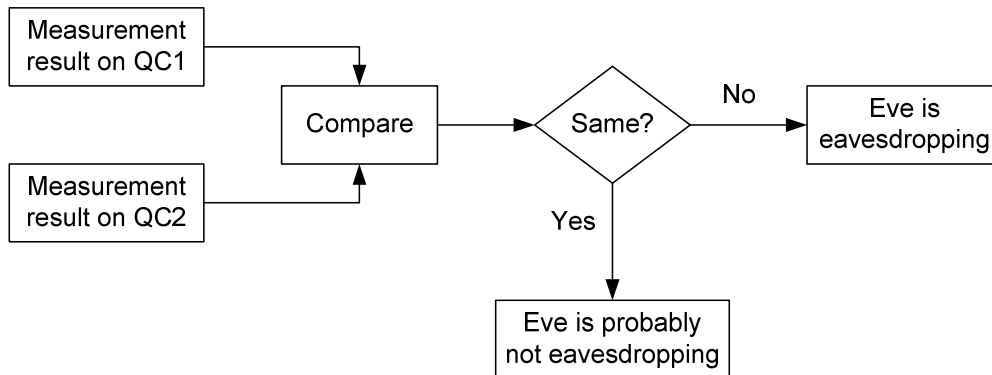


Figure 6.2 Comparing the measurement results on the two quantum channel to detect whether Eve is eavesdropping

2. The availability of an initialization vector shared between Alice and Bob leads to an easy way to detect whether Eve is present or not in real time. Instead of generating a sequence of random 0's and 1's in the first step, Alice uses the initialization vector shared between her and Bob as the random sequence, and then they follow the steps 2-6 as introduced above. As soon as Bob receives a qubit, measures it, and gets the measurement result, he compares it with the corresponding bit in the initialization vector, if he notices any conflict, the he knows Eve is present, Figure 6.3. Because he knows he is supposed to get a measurement result that is the same as the corresponding bit in the initialization vector, if he does not get it, the only reason is Eve's interference. So he can conclude that Eve is eavesdropping at that moment.

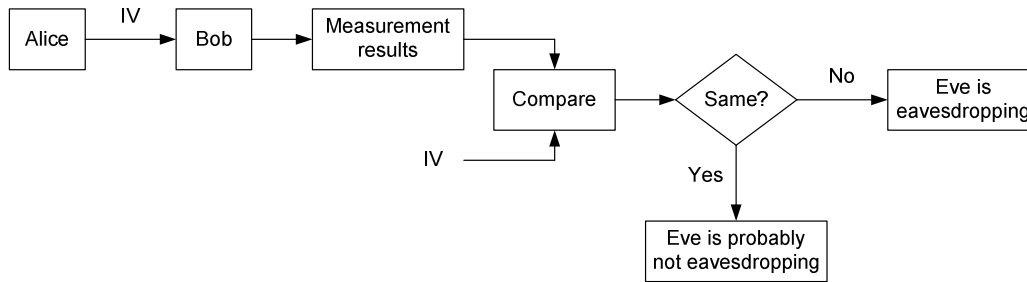


Figure 6.3 Alice transmitting the initialization vector to Bob and Bob comparing the measurement results with the initialization vector to detect whether Eve is eavesdropping

3. In order to make it even harder for Eve to guess when Alice and Bob are transmitting the initialization vector, they may choose to transmit it sporadically in a random order at random moments instead of transmitting the entire initialization vector in the normal order at the beginning. For example, Alice and Bob may transmit the bits of the initialization vector in a random order at random moments that are determined by a secret algorithm known to only themselves. Since there is no way for Eve to figure out at which moments and in which order Alice and Bob transmit the bits of the initialization vector, by no means she can avoid being detected if she is really eavesdropping. This mechanism provides a real-time detection of Eve's presence, because as soon as at a certain moment Bob finds a conflict between his

measurement results and the initialization vector, he knows Eve is present.

6.8 Eliminating the Basis Information Exchange between Alice and Bob on the Conventional Channel

It is a necessary step in all the quantum key distribution protocols proposed before this protocol for Alice and Bob to communicate with each other about the bases used by them on the two quantum channels, so that they can decide which bits should be discarded and which bits should be included into the raw key. However the basis information exchange is not needed in this protocol, which saves a great deal of communication overhead. This is realized by using the initialization vector shared between Alice and Bob and the basis selection rule adopted in this protocol. Since Alice and Bob share the initialization vector with each other, and they have a prior agreement on how to select the bases on the two quantum channels according to the bit value of the initialization vector, they know exactly which bases the other person uses on the two quantum channels, thus they do not need to communicate with each other about the basis information through the conventional channel as usual. This way, the basis information exchange on the conventional channel is removed.

6.9 Eliminating the Necessity of the Conventional Channel in the Structure

As introduced before, one of the purposes of the conventional channel is to exchange basis information between Alice and Bob, which we have proved its unnecessary in the proposed protocol; and the other purpose of the conventional channel is to figure out the error rate of the raw key and remove the errors in it. Now if Alice and Bob can figure it out that there is no error in the raw key, then the conventional channel can be eliminated. After eliminating the conventional channel, the structure of the proposed protocol becomes all-quantum, which means there is no classical element, such as a convention channel, in the structure. The all-quantum structure has the unique advantage over the hybrid structure with classical elements in term of security, because only the quantum structure can detect Eve's eavesdropping activity, while the classical structure cannot. So the all-quantum structure presents less vulnerabilities than the classical structure and the hybrid structure.

In order to eliminate the conventional channel, Alice and Bob need to be able to figure out that the raw key error rate is 0% during a period of time so that no error correction is needed through the communication on the conventional channel. The real-time detection mechanisms of Eve's presence presented in Section 6.7 give a very good preparation to achieve this goal. Since Alice and

Bob can detect Eve's presence in real time, they know exactly when Eve is not eavesdropping in real time. If Eve is not eavesdropping, then there is no error in the raw key, the error correction procedure on the conventional channel is not needed, so that the conventional channel can be eliminated. If there is no error in the raw key, then the raw key can be used directly as the final key to encrypt messages. In this case, the communication overhead is removed, the conventional channel is eliminated, the convergence speed of the final key is improved, and Eve's attack is effectively frustrated.

6.10 Conclusion

In this chapter, we introduced a new quantum key distribution protocol that makes use of the dual-quantum channel structure and the basis selection rule with the aid of an initialization vector shared between Alice and Bob. We showed that the basis information exchange on the conventional channel is not needed, which reduces the communication overhead greatly. In the proposed protocol we discussed four ways to obtain the final key, and two ways to frustrate Eve's eavesdropping attack. In addition to that, we presented three real-time detect mechanisms of Eve's presence during the key distribution process, which further enables the elimination of the necessity of the conventional channel in the structure. The proposed protocol removed the basis information

exchange between Alice and Bob, eliminated the usage of the conventional channel in the structure, and turned the structure of the proposed protocol into an all-quantum structure. The proposed protocol was able to obtain the final key in a much faster, securer way while at the same time frustrated Eve's attacks effectively without the communication overhead and the conventional channel in the structure at all.

Chapter 7 Defense Mechanisms to Eve's Attack

7.1 Introduction







The BB84 is a protocol to distribute a secret key from Alice to Bob, with the ability to detect whether Eve has eavesdropped or not during the key distribution process after the protocol has finished running once. It does not have a strong defense mechanism to frustrate Eve's attack rather than just passively detecting Eve's eavesdropping after a round of the running of the protocol. In this dissertation, we have presented several techniques that can be used to not only detect Eve's eavesdropping in real time, but also actively counter Eve's attack on Alice's and Bob's own initiative. In this chapter, we consider from the defender's perspective on how to thwart Eve's attack by adding more randomnesses and unpredictabilities into the proposed protocols, such as, time, location, wavelength, order, content, and so on. We address several techniques that can effectively deter Eve's attack, and together with previously presented techniques, the integrated defense mechanism offers a much stronger capability to actively and effectively frustrate Eve's attack, which enhances the security of the key distribution process.

7.2 Several Techniques to Frustrate Eve's Attack







7.2.1 Changing the Representation of Bits by Polarized Single Photons

Before a protocol starts, Alice and Bob need to make an agreement on the representation of bits by polarized single photons. The representation we use in this dissertation is shown in Table 7.1 (a). The agreement can be public to the eavesdropper, however in order to better frustrate Eve, Alice and Bob can make a secret agreement between them that is not publicized. There are totally four different forms to represent the classical bits by polarized single photons, Table 7.1. Now, instead of making use of only one publicly known representation, Alice and Bob can actually use the four secret representations in a random sequence for a random period of time, all decided by a secret algorithm known to only themselves. For example, Alice and Bob may use Table 7.1 (b) for 3 seconds, then use Table 7.1 (d) for 8.2 seconds, then switch to Table 7.1 (a) for 1.8 seconds, and then use Table 7.1 (c) for 15 seconds. Since Eve does not know the sequence of the representations, the content of the representation being used, as well as the duration of a certain representation, there is no way for Eve to figure out the meaning of her measurement results. To Eve, the measurement results do not mean anything but some random information. This way, Eve is effectively frustrated.







Table 7.1 Four different representations of bits by polarized single photons

| Classical Bit | Basis | |
|---------------|---|---|
| |  |  |
| 0 |  |  |
| 1 |  |  |







(a)

| Classical Bit | Basis | |
|---------------|---|---|
| |  |  |
| 0 |  |  |
| 1 |  |  |

(b)

| Classical Bit | Basis | |
|---------------|---|---|
| |  |  |
| 0 |  |  |
| 1 |  |  |

(c)

| Classical Bit | Basis | |
|---------------|---|---|
| |  |  |
| 0 |  |  |
| 1 |  |  |

(d)

7.2.2 Using the Decoy Quantum Channel to Transmit Fake Information

When Eve is eavesdropping during the key distribution process, she may be only present on one quantum channel while leave the other intact. In this situation, Alice and Bob can pretend to be transmitting real information on the quantum channel on which Eve is actively eavesdropping, however in fact transmit real information on the other quantum channel on which Eve is not eavesdropping.

The decoy information on the decoy quantum channel can draw Eve's attention and keep her focusing on the decoy quantum channel. This way Eve is fooled and the real information is protected. Alice and Bob can judge on which quantum channel Eve is eavesdropping by calculating and comparing the raw key error rates on the two quantum channels.

7.2.3 Locating the Two Quantum Channels in Different Optical Fibers or Optical Fiber Cables

The two quantum channels do not have to use one optical fiber or one optical fiber cable, although putting the two quantum channels in a single optical fiber cable is difficult enough already for Eve to locate the two quantum channels, since an optical fiber cable can have up to a thousand optical fibers in it. In order to better puzzle Eve, the two quantum channels can be located at different optical fiber cables, which makes it even more difficult for Eve to be able to locate the dual-quantum channel. If Eve can not locate the dual-quantum channel, then she can not launch successful attacks against them.

Further, if the situation with many optical fibers or optical fiber cables and a switch is available, then Alice and Bob can make use of the programmable switch to change the connections between fibers or cables, Figure 7.1. The connections inside the switch is decided by a secret algorithm shared and known

to only Alice and Bob, about which Eve does not have any knowledge. The connections in the switch change randomly and last for a random period of time. So Eve would not be able to find out which fiber (cable) is switched to which fiber (cable). For example, quantum channel 1 may be connected to fiber 3 (cable 3) for 5 seconds, and then it is switched to fiber 4 (cable 4) for 4 seconds, and so forth. Quantum channel 2 can also be switched to other fibers or cables randomly. Since Eve is not able to locate the two quantum channels, it is impossible for her to launch a successful attack against them.

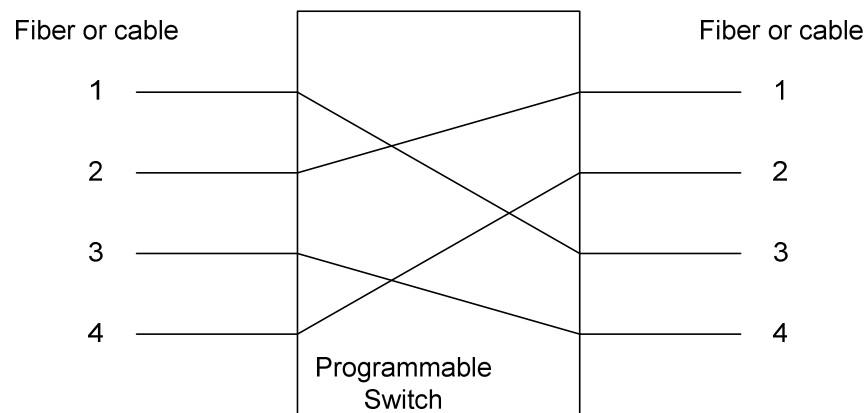


Figure 7.1 Changing the locations of the two quantum channels

7.2.4 Assigning the Two Quantum Channels with Different Wavelengths

By introducing the Wavelength Division Multiplexing (WDM) [97] technology into quantum key distribution, we can assign quantum channel 1 and quantum

channel 2 with two different wavelengths according to the secret algorithm shared and known to only Alice and Bob, Figure 7.2. For example, for a random period of time, wavelength w_2 may be assigned to quantum channel 1, and for another random period of time, wavelength w_4 may be assigned to quantum channel 1, and so on. Quantum channel 2 can be assigned with a random wavelength for a random period of time in the same way. Since there is no way for Eve to find out at a certain moment which wavelength is corresponding to which quantum channel, there is no way for her to launch a successful attack against the quantum channels.

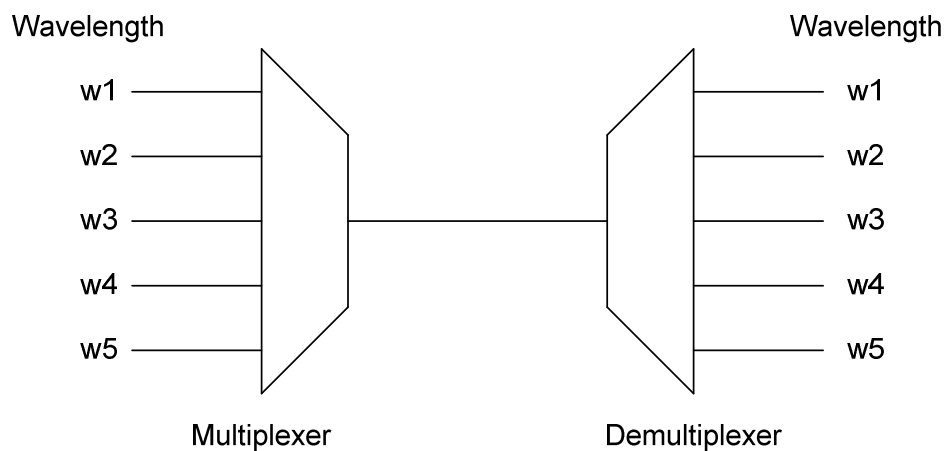


Figure 7.2 Assigning different wavelengths to the two quantum channels

7.2.5 Using the Initialization Vector Shared between Alice and Bob

In this dissertation, the initialization vector is used to XOR with the sifted key to obtain the final key, and to be transmitted instead of the randomly generated bits to detect Eve's presence in real time. Since the initialization vector is an initial secret shared and known to only Alice and Bob, about which Eve does not have any knowledge, any operations that are decided by the initialization is known to only Alice and Bob themselves. Eve is not able to get any information without knowing the initialization vector, thus her attack is effectively frustrated.

7.2.6 Transmitting the Initialization Vector in a Random Manner

In Chapter 6 we presented a method to detect Eve's presence in real time. Instead of transmitting the bits in the initialization vector in regular order, Alice and Bob can use the secret algorithm shared and known to only themselves to decide the sequence of the bits in the initialization vector to be sent, and the random moment to send a certain bit. Since the bits are sent at random moments in a random order, there is no way for Eve to figure out the situation. If Eve is really eavesdropping on the information transmitted between Alice and Bob, then there is no way for her to be able to avoid being detected by them. This way, Eve's eavesdropping activity is detected in real time, and Alice and Bob can adopt eluding or defending mechanisms to thwart her attack accordingly.

7.2.7 Introducing a Random Delay between the Transmissions on the Two Quantum Channels

Although as implied in the proposed protocols in this dissertation, the two polarized single photons that are corresponding to a certain random bit generated by Alice in the first step are transmitted at the same time on the two quantum channels, they can be transmitted at different moments, with a random delay between the transmissions on the two quantum channels. This enhances the security of the key distribution process.

If Eve does not know which two qubits are the two corresponding to a certain random bit generated by Alice, then she loses the opportunity to get additional information from the correlation of the two qubits, which is useful to launch a successful attack. For example, Alice may start transmitting a qubit on quantum channel 1 at a moment, while delay the transmission of the corresponding qubit on quantum channel 2 by a random period of time, for example, 6.2 seconds. This way, Eve can not figure out which two qubits are in a pair, so that she is not able to launch a successful attack against the two corresponding qubits.

7.3 Integrated Defense Mechanism to Eve's Attack

Each of the techniques mentioned above is a good mechanism to defend against Eve's attack. Additionally, these mechanisms can be used together to form an

integrated defense mechanism that provides a much stronger defending performance against Eve's attack. Several randomnesses and unpredictabilities are involved and combined together, such as time, location, wavelength, order, content, and so on, which make it extremely difficult for Eve to be able to figure out what is going on with the two quantum channels and the qubits transmitted on them. The secret algorithm shared between Alice and Bob can be just an algorithm that generates random values, and according to the random values generated, Alice and Bob choose how to manipulate time, location, wavelength, order, content, and so on.

7.4 Conclusion

In this chapter we presented several techniques that can effectively frustrate Eve's attack, and by using the integrated defense mechanism, it is even harder for Eve to be able to launch successful attacks. The idea behind these techniques is to introduce more randomnesses and unpredictabilities into the protocols, such that Eve can not figure out what is really happening between Alice and Bob on the two quantum channels, hence she is not able to launch successful attack against the key distribution process.

Chapter 8 Conclusions and Future Work

8.1 Conclusions

The BB84 protocol is a key distribution protocol that is able to provide unconditional security to the key distribution process. However this protocol is a very low efficient protocol in terms of sharing a raw key and the convergence speed of obtaining a final key. In addition, the BB84 protocol does not have an effective countermeasure to defend against Eve's attack except for passively detecting whether Eve has eavesdropped or not after one round of the running of the protocol. It is vulnerable to Eve's eavesdropping attack.

In this dissertation, we mainly focused on two things: How to improve the efficiency of sharing a raw key and a final key, and how to effectively frustrate Eve. Three protocols were proposed in this dissertation, offering much better performances than the BB84 protocol. They have a much higher raw key efficiency, they can obtain the final key in a much faster and securer way, they can keep the length of the final key the same as the length of the sifted key, which is much longer than what the BB84 protocol can obtain, and they can effectively deter Eve's attack. Overall, the proposed protocols provided a highly efficient and highly temper-resistant key distribution.

In the protocol proposed in Chapter 4, we introduced a dual-quantum channel structure and complementary measuring bases of Bob on the dual-quantum

channel. With the dual-quantum channel and the complementary measuring bases, the raw key efficiency is increased from 50% to 100%, which is a huge improvement over the BB84 protocol. The raw key error rate of this protocol is generally lower than that of the BB84 protocol, and according to whether Eve is present or not, on either or both of the two quantum channels, we analyzed three different scenarios with three different raw key error rates. Due to the channel diversity brought by the dual-quantum channel structure, the raw key error rates on the two quantum channels can be calculated respectively and compared afterwards, which offers an effective method to elude and frustrate Eve's eavesdropping attack. With this feature, Alice and Bob can figure out on which quantum channel Eve is actively eavesdropping and on which quantum channel Eve is not, so that they keep sending decoy information on the quantum channel on which Eve is actively eavesdropping to attract her attention, while at the same time sending real information on the other quantum channel on which Eve is not eavesdropping. This way, Eve is fooled, and all the information she gets is just some garbage information. Because Eve is not touching the other quantum channel, the raw key obtained from that quantum channel is error-free and can be used directly as the final key without going through the tedious information reconciliation and privacy amplification procedures, providing a much faster way to obtain the final key. In addition, by XORing the sifted key with the initialization vector shared between Alice and Bob and known only to

themselves, the final key can be achieved in a much faster, securer, and more efficient way. Since Eve does not have any knowledge about the initialization vector, she is not able to get any knowledge about the final key either, thus Eve is effectively frustrated.

In Chapter 5 we proposed a quantum key distribution protocol that adopted a novel basis selection rule with the aid of an initialization vector shared between Alice and Bob. According to the value of the bits in the initialization vector, Alice and Bob make a prior agreement on how to select the bases on the two quantum channels. This selection rule is formed in a way such that all the random bits generated by Alice in the first step of the protocol are included into the raw key, making the raw key efficiency 100%. Since it employed the same dual-quantum channel structure as the protocol presented in Chapter 4, the same scenarios regarding the raw key error rate applied. We presented four ways to obtain the final key in this protocol: going through the standard information reconciliation and privacy amplification procedures to obtain the final key, comparing the two raw key error rates on the two quantum channels and using the one with a significantly lower error rate to get the final key by going through the information reconciliation and privacy amplification procedures, using the raw key obtained from the eavesdropping-free quantum channel directly as the final key, and XORing the sifted key with the initialization vector shared between Alice and Bob to get the final key. We also proposed two ways to

frustrate Eve's attack in this protocol: sending decoy information on the quantum channel on which Eve is actively eavesdropping, and using the initialization vector to eliminate Eve's knowledge about the final key. Since Eve does not have any knowledge about the initialization vector shared between Alice and Bob, she does not have any knowledge about the final key either. Due to these reasons, Eve is not able to launch successful attacks, thus she is effectively deterred.

In Chapter 6 we proposed a quantum key distribution protocol in which the basis information exchange between Alice and Bob on the conventional channel is not needed, and further the necessity of the conventional channel in the structure is eliminated. In this protocol, the initialization vector shared between Alice and Bob is used to decide the bases used by Alice and Bob on the two quantum channels. Since Alice and Bob use exactly the same bases on the two quantum channels, they do not need to communicate with each other about the basis information through the conventional channel, which significantly reduces the communication overhead. The methods used to obtain the final key and frustrate Eve mentioned in Chapter 4 and Chapter 5 are also applicable to this protocol. Besides those methods, we introduced three detection mechanisms that are able to detect Eve's presence in real time in this protocol. With the help of the real-time detection mechanisms, Alice and Bob can respond to Eve's attack in a time-efficient manner so that they can better defend against Eve. Given the

ability of detecting Eve's presence in real time, this protocol eliminates the necessity of the conventional channel between Alice and Bob, which makes the entire structure all-quantum. This all-quantum structure not only means much lower communication overhead, but also indicates less vulnerabilities, since only the quantum structure is able to detect Eve's eavesdropping, while the classical structure and the hybrid structure are not able to do so.

In Chapter 7, we proposed several methods to import more randomnesses and unpredictabilities into the protocols to thwart Eve's attack. We introduced several the following techniques: randomizing the representation of bits by polarized single photons, using a decoy quantum channel to transmit fake information to Eve, changing the locations of the two quantum channels, assigning different wavelengths to the two quantum channels, making use of the initialization vector shared between Alice and Bob, randomizing the sequence and moments of the bits in the initialization vector to be transmitted to Bob, and employing a random delay between the transmissions on the two quantum channels. Each technique increases the difficulty for Eve to launch a successful attack, and with all the techniques combined together as an integrated defense mechanism, it is extremely difficult for Eve to be able to launch a successful attack, hence she is effectively frustrated.

8.2 Future Work

This dissertation has led to several thoughts for the future research work in quantum cryptography. First, the authentication problem in quantum key distribution is still an open problem. It is a universal assumption that before Alice and Bob start the key distribution protocol, they have already authenticated each other. In most of the time, the authentication between the two communicating entities is realized by physical means or conventional authenticating techniques, but some research has started focusing on finding a quantum way to authenticate Alice and Bob [42-60]. Quantum digital signature is another emerging direction to solve the authentication and non-repudiation problem in quantum key distribution [98, 99].

Second, another assumption in the quantum key distribution protocols is that although Eve can copy the classical information transmitted on the conventional channel, she is not able to modify the classical information. This indicates that where there is a classical element in the structure, there are vulnerabilities and restrictions. So fully eliminating all the classical elements in the key distribution process is a great idea to not only reduce communication overhead, but also more importantly, remove the restrictions and the vulnerabilities in the structure. Since the quantum structure is able to detect Eve's eavesdropping activity, an all-quantum structure is more robust in terms of resisting attacks. So fully

eliminating the convention channel and all the classical elements in the structure is another important research direction in the future.

In addition, other quantum key distribution protocols proposed prior to this dissertation also experience the low efficiency problem, and they are not able to defend against Eve effectively. Future research work should also focus on how to improve the efficiency of the key distribution process and the ability to defend against Eve for those protocols.

Bibliography

- [1] History of Cryptography, Wikipedia. (http://en.wikipedia.org/wiki/History_of_cryptography)
- [2] Jayne E. Shatz, *Ceramics of the Middle East: From the Middle Mesopotamian Period to the Modern Era*. (<http://www.jayneshatzpottery.com/MIDEASTCERAMICS.html>)
- [3] Scytale, Wikipedia. (<http://en.wikipedia.org/wiki/Scytale>)
- [4] Caesar Cipher, Wikipedia. (http://en.wikipedia.org/wiki/Caesar_cipher)
- [5] William Stallings, *Cryptography and Network Security - Principles and Practices (Fourth Edition)*, Pearson Prentice Hall, New Jersey, 2006.
- [6] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, February 1978.
- [7] Whitfield Diffie, and Martin E. Hellman, "Multiuser Cryptographic Techniques," *Proceedings of the AFIPS 1976 National Computer Conference*, Montvale, New Jersey, June 7-10, 1976, pp. 109-112.
- [8] Charles H. Bennett, and Gilles Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, December 10-12, 1984, pp. 175-179.
- [9] Historical Statistics, CERT. (<http://www.cert.org/stats/historical.html>)
- [10] 2005 Disclosures of U.S. Data Incidents, ITRC. (<http://idtheftmostwanted.org/ITRC%20Breach%20Report%202005.pdf>)
- [11] 2006 Disclosures of U.S. Data Incidents, ITRC. (<http://idtheftmostwanted.org/ITRC%20Breach%20Report%202006.pdf>)
- [12] 2007 Disclosures of U.S. Data Incidents, ITRC. (<http://idtheftmostwanted.org/ITRC%20Breach%20Report%202007.pdf>)
- [13] Daniel Stick, Jonathan D. Sterk, and Christopher Monroe, "The Trap Technique," *IEEE Spectrum*, vol. 44, no. 8, pp. 36-43, August 2007.

- [14] Lieven Vandersypen, "Dot-To-Dot Design," *IEEE Spectrum*, vol. 44, no. 9, pp. 42-47, September 2007.
- [15] Lov K. Grover, "A Fast Quantum Mechanical Algorithm for Database Search," *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing*, Philadelphia, PA, May 1996, pp. 212-219.
- [16] Carl Pomerance, "A Tale of Two Sieves," *Notices of the AMS*, vol. 43, no. 12, pp. 1473-1485, December 1996.
- [17] Peter W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, November 20-22, 1994, pp. 124-134.
- [18] Data Encryption Standard (DES), NIST, FIPS PUB 46-3, October 25, 1999. (<http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>)
- [19] Horst Feistel, "Cryptography and Computer Privacy," *Scientific American*, vol. 228, no. 5, pp. 15-23, May 1973.
- [20] RSA's DES Challenge III is solved in record time, RSA Laboratories, 1999. (<http://www.rsa.com/rsalabs/node.asp?id=2108>)
- [21] Advanced Encryption Standard (AES), NIST, FIPS PUB 197, November 26, 2001. (<http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>)
- [22] RSA-200 is factored, RSA Laboratories, 2005. (<http://www.rsa.com/rsalabs/node.asp?id=2879>)
- [23] Neal Koblitz, "Elliptic Curve Cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203-209, 1987.
- [24] Victor S. Miller, "Use of Elliptic Curves in Cryptography," *Lecture notes in computer sciences; vol. 218 on Advances in cryptology (CRYPTO 85)*, Santa Barbara, CA, pp. 417-426, 1986.
- [25] Stephen Wiesner, "Conjugate Coding," *ACM Sigact News*, vol. 15, no. 1, 1983, pp. 78-88; original manuscript written circa 1969.
- [26] Artur K. Ekert, "Quantum Cryptography Based on Bell's Theorem," *Physical Review Letters*, vol. 67, no. 6, pp. 661-663, 1991.

- [27] Charles H. Bennett, "Quantum Cryptography Using Any Two Nonorthogonal States," *Physical Review Letters*, vol. 68, no. 21, pp. 3121-3124, 1992.
- [28] Charles H. Bennett, Gilles Brassard, and N. David Mermin, "Quantum Cryptography without Bell's Theorem," *Physical Review Letters*, vol. 68, no. 5, pp. 557-559, 1992.
- [29] Kyo Inoue, Edo Waks, and Yoshihisa Yamamoto, "Differential Phase Shift Quantum Key Distribution," *Physical Review Letters*, vol. 89, no. 3, pp. 037902.1-037902.3, 2002.
- [30] Subhash Kak, "A Three-Stage Quantum Cryptography Protocol," *Foundations of Physics Letters*, vol. 19, pp. 293-296, 2006.
- [31] Tzonelih Hwang, Kuo-Chang Lee, and Chuan-Ming Li, "Provably Secure Three-Party Authenticated Quantum Key Distribution Protocols," *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no. 1, pp. 71-80, 2007.
- [32] Stamatios V. Kartalopoulos, "K08: A Generalized BB84 Protocol," submitted for publication, 2008.
- [33] Hoi-Kwong Lo, and H. F. Chau, "Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances," *Science*, vol. 283, no. 5410, pp. 2050-2056, 1999.
- [34] Di Jin, Pramode Verma, and Stamatios Kartalopoulos, "Key Distribution Using Dual Quantum Channels," *Proceedings of the Fourth International Conference on Information Assurance and Security*, Naples, Italy, September 8-10, 2008, pp. 327-332.
- [35] Di Jin, Pramode K. Verma, and Stamatios V. Kartalopoulos, "Fast Convergent Key Distribution Algorithms Using a Dual Quantum Channel," to be published by the *Wiley Journal of Security and Communication Networks*, 2008.
- [36] Almut Beige, Berthold-Georg Englert, Christian Kurtsiefer, and Harald Weinfurter, "Secure Communication with a Publicly Known Key," *Acta Physica Polonica A*, vol. 101, no. 3, pp. 357-368, 2002.

- [37] Hwayean Lee, Jongin Lim, and HyungJin Yang, “Quantum Authentication and Quantum Key Distribution Protocol,” arXiv:quant-ph/0510144v2, 2005.
- [38] Guihua Zeng, and Xinmei Wang, “Quantum Key Distribution with Authentication,” arXiv:quant-ph/9812022v2, 1998.
- [39] Bao-Sen Shi, Jian Li, Jin-Ming Liu, Xiao-Feng Fan, and Guang-Can Guo, “Quantum Key Distribution and Quantum Authentication Based on Entangled State,” *Physics Letters A*, vol. 281, no 2-3, pp. 83-87, March 2001.
- [40] H. Bechmann-Pasquinucci, and A. Pasquinucci, “Quantum Key Distribution with Trusted Quantum Relay,” arXiv:quant-ph/0505089v1, May 2005.
- [41] Yu Liu, Changqiang Wang, Fan Zhang, Guangxi Zhu, and Xiang Zhu, “A Discussion on a Quantum Key Remote Distribution Scheme not Based on the Quantum Entanglement State,” *Proceedings of the SPIE*, vol. 5282, Bellingham, WA, 2003, pp. 889-897.
- [42] Y. Kanamori, Seong-Moo Yoo, D. A. Gregory, and F. T. Sheldon, “On Quantum Authentication Protocols,” *IEEE Global Telecommunications Conference*, November 28-December 2, 2005, vol. 3, pp. 1650-1654.
- [43] Miloslav Dusek, Ondrej Haderka, Martin Hendrych, and Robert Myska, “Quantum Identification System,” *Physical Review A*, vol. 60, pp. 149-156, 1999.
- [44] Andrea Pasquinucci, “Authentication and Routing in Simple Quantum Key Distribution Networks,” arXiv:cs/0506003v1, 2005.
- [45] Rex A. C. Medeiros, Francisco M. de Assis, Bernardo L. Juior, Aercio F. Lima, “Quantum Authentication Scheme Based on Algebraic Coding,” arXiv:quant-ph/0307095v2, 2003.
- [46] D. R. Kuhn, “A Hybrid Authentication Protocol Using Quantum Entanglement and Symmetric Cryptography,” arXiv:quant-ph/0301150v1, 2003.
- [47] Xiaoyu Li, and Dexi Zhang, “Quantum Information Authentication Using Entangled States,” *Proceedings of the International Conference on Digital Telecommunications*, 2006, pp. 64-68.

- [48] Tien-Sheng Lin, I.-M. Tsai, Han-Wai Wang, Sy-Yen Kuo, "Quantum Authentication and Secure Communication Protocols," *Proceedings of the Sixth IEEE Conference on Nanotechnology*, June 2006, vol. 2, pp. 863-866.
- [49] Wang Jian, Zhang Quan, and Tang Chao-Jing, "Multiparty Simultaneous Quantum Identity Authentication Based on Entanglement Swapping," *Chinese Physics Letters*, vol. 23, no. 9, pp. 2360-2363, September 2006.
- [50] Stefan Rass, "A Method of Authentication for Quantum Networks," *International Journal of Information Technology*, vol. 3, no. 3, pp. 160-167, 2006.
- [51] Dexi Zhang, and Xiaoyu Li, "Quantum Authentication Using Orthogonal Product States," *Proceedings of the Third International Conference on Natural Computation*, August 24-27, 2007, vol. 4, pp. 608-612.
- [52] Guihua Zeng, and Guangcan Guo, "Quantum Authentication Protocol," arXiv:quant-ph/0001046v1, 2000.
- [53] Changho Hong, Jiin Kim, Hwayean Lee, and Hyungjin Yang, "Authenticated Multiuser Quantum Direct Communication Using Entanglement Swapping," arXiv:quant-ph/0601194v1, 2006.
- [54] Hwayean Lee, Jongin Lim, and HyungJin Yang, "Quantum Direct Communication with Authentication," arXiv:quant-ph/0512051v1, 2005.
- [55] Zhan-jun Zhang, Yi-min Liu, and Hao Yuan, "Improving Security of Quantum Identity Authentication Based on Ping-Pong Technique for Photons," arXiv:quant-ph/0701045v4, January 2007.
- [56] Howard Barnum, Claude Crepeau, Daniel Gottesman, Adam Smith, and Alain Tapp, "Authentication of Quantum Messages," *Proceedings of the 43rd Annual IEEE Symposium on the Foundations of Computer Science*, 2002, pp. 449-458.
- [57] Xin Lu, Zhi Ma, and Deng-Guo Feng, "A Quantum Authenticated Encryption Scheme," *Proceedings of the 7th International Conference on Signal Processing*, August 31-September 4, 2004, vol. 3, pp. 2306-2309.

- [58] Jonathan Oppenheim, and Michal Horodecki, “How to Reuse a One-Time Pad and Other Notes on Authentication, Encryption and Protection of Quantum Information,” *Physical Review A*, vol. 72, 042309, 2005.
- [59] M. Peev, M. Nolle, O. Maurhardt, T. Lorunser, M. Suda, A. Poppe, R. Ursin, A. Fedrizzi, and A. Zeilinger, “A Novel Protocol-Authentication Algorithm Ruling Out a Man-in-the Middle Attack in Quantum Cryptography,” *International Journal of Quantum Information*, vol. 3, no. 1, pp. 225-232, 2005.
- [60] Akihiro Yamamura, and Hirokazu Ishizuka, “Error Detection and Authentication in Quantum Key Distribution,” *Lecture Notes in Computer Science*, vol. 2119; *Proceedings of the 6th Australasian Conference on Information Security and Privacy*, 2001, pp. 260-273.
- [61] E. Waks, K. Inoue, C. Santori, D. Fattal, J. Vuckovic, G. Solomon, and Y. Yamamoto, “Secure Communication: Quantum Cryptography with a Photon Turnstile,” *Nature*, vol. 420, no. 6917, pp. 762-762, 2002.
- [62] Jennifer Ouellette, “Quantum Key Distribution,” *The Industrial Physicist*, vol. 10, no. 6, pp. 22-25, January 2005.
- [63] Takashi Yamamoto, Sahin Kaya Özdemir, Masato Koashi, and Nobuyuki Imoto, “Faithful Quantum Communication Over Noisy Environment,” *IEEE LEOS NEWSLETTER*, pp. 4, 6-8, 10, December 2006.
- [64] Chip Elliott, David Pearson, and Gregory Troxel, “Quantum Cryptography in Practice,” *Proceedings of the International Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, Karlsruhe, Germany, 2003, pp. 227-238.
- [65] A. Poppe, A. Fedrizzi, R. Ursin, and H. R. Bohm et al., “Practical Quantum Key Distribution with Polarization Entangled Photons,” *Optics Express*, vol. 12, no. 16, pp. 3865-3871, 2004.
- [66] Stamatios V. Kartalopoulos, “Quantum Cryptography for Secure Optical Networks,” *Proceedings of the IEEE International Conference on Communications*, Glasgow, Scotland, June 24-28, 2007, pp. 1311-1316.

- [67] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, "Practical Quantum Key Distribution over 60 Hours at an Optical Fiber Distance of 20km Using Weak and Vacuum Decoy Pulses for Enhanced Security," *Optics Express*, vol. 15, no. 13, pp. 8465-8471, 2007.
- [68] E. Diamanti, H. Takesue, C. Langrock, M. M. Fejer, and Y. Yamamoto, "100 km Secure Differential Phase Shift Quantum Key Distribution with Low Jitter Up-Conversion Detectors," *Optics Express*, vol. 14, no. 26, pp.13073-13082, 2006.
- [69] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum Key Distribution over 67km with a Plug & Play System," *New Journal of Physics*, vol. 41, no. 4, pp. 411-418, 2002.
- [70] C. Gobby, Z. L. Yuan, and A. J. Shields, "Quantum Key Distribution over 122km of Standard Telecom Fiber," *Applied Physics Letters*, vol. 84, pp. 3762-3764, 2004.
- [71] P. D. Townsend, "Quantum Cryptography in Optical Fiber Networks," *Proceedings of the International Conference on Integrated Optics and Optical Fiber Communication*, 1999, vol. 4, pp. 141-143.
- [72] M. S. Goodman, P. Toliver, and R. J. Runser et al., "Quantum Cryptography for Optical Networks: A Systems Perspective," *Proceedings of the 16th Annual Meeting of the IEEE Lasers and Electro-Optics Society*, October 27-28, 2003, vol. 2, pp. 1040-1041.
- [73] Chip Elliott, "Quantum Cryptography," *IEEE Security and Privacy*, vol. 2, no. 4, pp. 57-61, July 2004
- [74] Donald S. Bethune, Martha Navarro, and William P. Risk, "Enhanced Autocompensating Quantum Cryptography System," *Applied Optics*, vol. 41, no. 9, pp. 1640-1648, 2002.
- [75] G. Massimo Palma, "Quantum Cryptography," in *Handbook of Information Security, Volume II, Information Warfare, Social, Legal, and International Issues and Security Foundations*, John Wiley and Sons Inc., New Jersey, 2006, pp. 606-616.
- [76] D. Bruss, G. Erdelyi, T. Meyer, T. Riege, and J. Rothe, "Quantum Cryptography: A Survey," *ACM Computing Surveys*, vol. 39, no. 2, pp. 1-27, 2007.

- [77] G. Benenti, G. Casati, and G. Strini, *Principles of Quantum Computation and Information, Vol. I: Basic Concepts*, World Scientific Publishing, New Jersey, 2004.
- [78] Stamatios Kartalopoulos, “Is Optical Quantum Cryptography the ‘Holy Grail’ of Secure Communication?” *SPIE Newsroom*, 2005.
(<http://spie.org/x8860.xml?highlight=x2412>)
- [79] Samuel Lomonaco, “A Talk on Quantum Cryptography, or How Alice Outwits Eve,” *Proceedings of the Symposia in Applied Mathematics*, vol. 58, Washington, DC, January 2002, pp. 237-264.
- [80] Stamatios V. Kartalopoulos, “A Primer on Cryptography in Communications,” *IEEE Communications Magazine*, vol. 44, no. 4, pp. 146-151, April 2006.
- [81] W. Heisenberg, “Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik,” *Zeitschrift für Physik*, vol. 43, pp. 172-198, 1927.
- [82] W. K. Wootters, and W. H. Zurek, “A Single Quantum Cannot be Cloned,” *Nature*, vol. 299, pp. 802-803, 1982.
- [83] D. Dieks, “Communication by EPR Devices,” *Physics Letters A*, vol. 92, no. 6, pp. 271-272, 1982.
- [84] Caslav Brukner, Marek Zukowski, and Anton Zeilinger, “The Essence of Entanglement,” arXiv:quant-ph/0106119v1, 2001.
- [85] Thomas Jennewein, Christoph Simon, Gregor Weihs, Harald Weinfurter, and Anton Zeilinger, “Quantum Cryptography with Entangled Photons,” *Physical Review Letters*, vol. 84, no. 20, pp. 4729-4732, 2000.
- [86] William Perkins, “Trusted Certificates in Quantum Cryptography,” arXiv:cs/0603046v1, March 2006.
- [87] Partha Basuchowdhuri, “Classical Authentication Aided Three-Stage Quantum Protocol,” arXiv:cs/0605083v1, May 2006.
- [88] Priya Sivakumar, “Implementing the Three-Stage Quantum Cryptography Protocol,” arXiv:cs/0603067v1, March 2006.

- [89] James Harold Thomas, “Variations on Kak’s Three Stage Quantum Cryptography Protocol,” arXiv:0706.2888v1, June 2007.
- [90] Partha Basuchowdhuri, “Comparing BB84 and Authentication-Aided Kak’s Three-Stage Quantum Protocol,” arXiv:cs/0703092v1, March 2007.
- [91] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, and H. Weier et al., “Free-Space Distribution of Entanglement and Single Photons over 144 km,” *Nature Physics*, vol. 3, pp. 481-486, 2007.
- [92] P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. E. Lita, A. J. Miller, and J. E. Nordholt, “Long-Distance Quantum Key Distribution in Optical Fiber,” *New Journal of Physics*, vol. 8, pp. 193, 2006.
- [93] id Quantique.(<http://www.idquantique.com>)
- [94] MagiQ Technologies. (<http://www.magiqtech.com>)
- [95] SmartQuantum. (<http://www.smartquantum.com>)
- [96] QuintessenceLabs Pty Ltd. (<http://www.quintessencelabs.com>)
- [97] Stamatios V. Kartalopoulos, *DWDM Networks, Devices, and Technology*, IEEE Press/Wiley, New Jersey, 2003.
- [98] Xiao-jun Wen, and Yun Liu, “Authentic Digital Signature Based on Quantum Correlation,” arXiv:quant-ph/0509129, 2005.
(<http://arxiv.org/pdf/quant-ph/0509129.pdf>)
- [99] Xin Lu, and Dengguo Feng, “Quantum Digital Signature Based on Quantum One-Way Functions,” *Proceedings of the 7th International Conference on Advanced Communication Technology*, 2005, vol. 1, pp. 514-517.

Appendix

List of Publications

Book Chapter

- [1] **Di Jin**, Stamatios V. Kartalopoulos, and Pramode K. Verma, “Wireless Ad Hoc and Sensor Network Security,” Chapter in: *Security and Privacy in Mobile and Wireless Networking*, Stefanos Gritzalis, Tom Karygiannis, and Charalabos Skianis (Eds), ISBN: 978-1905886-906, Troubador Publishing Ltd, Leicester, UK, 2009.

Journal Papers

- [1] **Di Jin**, Pramode K. Verma, and Stamatios V. Kartalopoulos, “Fast Convergent Key Distribution Algorithms Using a Dual Quantum Channel,” to be published by the *Wiley Journal of Security and Communication Networks*, 2008.
- [2] Stamatios V. Kartalopoulos, and **Di Jin**, “Vulnerabilities and Security Strategy for the Next Generation Bandwidth Elastic PON,” *WSEAS Transactions on Communications*, vol. 6, no. 10, pp. 815-823, 2007.
- [3] **Di Jin**, Stamatios V. Kartalopoulos, and Pramode K. Verma, “Analysis of Security Vulnerabilities and Countermeasures of Ethernet Passive Optical Network (EPON),” *Journal of China Communications*, vol. 4, no. 3, pp. 17-29, 2007.
- [4] **Jin Di**, Zhang Kaiju, and Shao Cheng, “Production Object-Oriented Integrated Optimizing Control Strategy in Hot Rolling Process,” *Journal of Iron and Steel Research*, vol. 18, no. 11, pp. 31-34, 2006.
- [5] **Jin Di**, and Shao Cheng, “Application of Simulation Analysis for 6-DOF Hydraulic Parallel Robot of Auto-Disturbance-Rejection-Controller,” *Journal of Dalian University of Technology*, vol. 43, no. 5, pp. 691-696, 2003.
- [6] Sun Haiying, Shao Cheng, and **Jin Di**, “Study on Oil Storage Scheduling Scheme of Refinery,” *Journal of Qiqihar University*, vol. 19, no. 4, pp. 39-43, 2003.

Conference Papers

- [1] **Di Jin**, Pramode Verma, and Stamatios Kartalopoulos, “Key Distribution Using Dual Quantum Channels,” *Proceedings of the Fourth International Conference on Information Assurance and Security*, Naples, Italy, September 8-10, 2008, pp. 327-332.
- [2] Stamatios V. Kartalopoulos, and **Di Jin**, “Vulnerability Assessment and Security of Scalable and Bandwidth Elastic Next Generation PONs,” *Proceedings of the 11th WSEAS International Conference on Communications*, Agios Nikolaos, Crete Island, Greece, July 26-28, 2007, vol. 3, pp. 33-39.
- [3] Zhang Kaiju, **Jin Di (Corresponding Author)**, and Shao Cheng, “Fuzzy Neural Network’s Application in Furnace Temperature Compensation Based on Rolling Information Feedback,” *Proceedings of the 16th IFAC World Congress*, Prague, Czech Republic, July 4-8, 2005, vol. 16, pp. 259-263.

Patent Application

- [1] **Di Jin**, Pramode K. Verma, and Stamatios V. Kartalopoulos, “Methods for Highly Efficient and Tamper-Resistant Quantum Key Distribution Protocols,” being filed as a provisional patent, 2008.