THE DESIGN AND ANALYSIS OF QUANTUM CRYPTOGRAPHIC PROTOCOLS

by

Hong Lai

A dissertation submitted in fulfilment of the requirements

for the degree of

DOCTOR OF PHILOSOPHY

Department of Computing
Faculty of Science and Engineering
Macquarie University
Sydney, Australia

Supervisors: Prof. Mehmet A. Orgun and Prof. Josef Pieprzyk

April 2015

STATEMENT OF CANDIDATE

I (HONG LAI) certify that the work in this thesis entitled "THE DESIGN AND ANALYSIS OF QUANTUM CRYPTOGRAPHY PROTOCOLS" has not previously been submitted for a degree nor has it been submitted as part of the requirements for a degree to any other university or institution other than Macquarie University.

I also certify that the thesis is an original piece of research and has been written by me. Any help and assistance that I have received in my research work and the preparation of the thesis itself have been appropriately acknowledged.

In addition, I certify that all information sources and literature used are indicated in the thesis.

Signature ..... Hong Lai

Date ..... 20 July 2015

ABSTRACT

Quantum cryptography including quantum key distribution and quantum secret sharing, a fundamental branch in quantum information processing, is the process whereby two or more parties agree on a key for subsequent cryptographic use. The goal of quantum cryptography is to establish a secure key in an insecure communication environment, leading to the difficulty of the protocols' design and analysis. In this thesis, we focus on the design and analysis of secure and efficient protocols of two or more parties in quantum settings.

Firstly, we focus on high-capacity quantum key distribution protocols over the general and collective-noise quantum channels. With Lucas numbers and Chebyshev maps, flexible lower-dimensional high-capacity quantum key distribution can be achieved. Our proposed protocol can simultaneously satisfy high secure key generation rates and long achievable operating distances. Then, we construct sixteen $2-$extended unitary operations in terms of the four unitary operations based on collective noises to double the capacity of a photon carried.

Then, we use recurrence and fountain codes to present (2,3) threshold discrete variable quantum secret sharing of secure direct communication. Moreover, we generalize the (2,3) protocol to (n, n) threshold quantum secret sharing of secure direct communication. To be exact, fountain codes can be used to distill a shorter but highly secure key information and authenticate the identities of participants and detect eavesdropping. Recurrence can be used to improve key generation rates.

Finally, we construct $n-$extended unitary operations in terms of the four unitary operations to present hybrid quantum key distribution and hybrid quantum

secret sharing protocols based on threshold and adversary structure. The goal of these protocols is to reduce the number of photons and quantum participants used so that they can be realized with the current quantum technology.

STATEMENT OF CANDIDATE

I (HONG LAI) certify that the work in this thesis entitled "THE DESIGN AND ANALYSIS OF QUANTUM CRYPTOGRAPHIC PROTOCOLS" has not previously been submitted for a degree nor has it been submitted as part of the requirements for a degree to any other university or institution other than Macquarie University.

I also certify that the thesis is an original piece of research and has been written by me. Any help and assistance that I have received in my research work and the preparation of the thesis itself have been appropriately acknowledged.

In addition, I certify that all information sources and literature used are indicated in the thesis.

Signature .....

Date .....

ACKNOWLEDGMENTS

Study and research have been two extremely enjoyable experiences for me, giving me a lot of chances to learn many exciting new things and get to know many great people. However, none of these would have been possible without the help and support of many people whom I met on the way of my Ph.D education.

I would like to express my most sincere thanks to my two principle supervisors Prof. Mehmet A. Orgun and Prof. Jinghua Xiao who is my supervisor in BUPT (because I am a cotutelle student from Macquarie University and Beijing University of Posts and Telecommunications (BUPT)). They are both strict supervisors and loving fathers. I will remain forever grateful for their approachability, inspirational suggestions and constructive criticism, teaching me a lot about doing research rigorously and presenting the research results correctly. They always gave me the freedom to try things out, while encouraging me to focus on the significant parts. Jinghua Xiao offered me a chance to study abroad and Mehmet A. Orgun helped me seize the chance. Jinghua Xiao always directed me to plan for future while Mehmet A. Orgun helped me cope with everything enormously during all the processes. Mehmet A. Orgun is a very responsible, patient and helpful supervisor. He took full advantage of everything that he could do to broaden my horizons and enhance my study, such as helping me apply for grants for attending conferences and visits, and introducing his friends whose interests are close to me, and spending a lot of time on revising and improving my papers. I am also grateful to my associate supervisor Prof. Josef Pieprzyk. I am lucky to discuss with him and get him to help me revise my papers, which provide enlightening ideas and give important suggestions for my papers. I enjoy being

their student.

I was privileged to have Dr Liyin Xue for his invaluable guidance and for continued supervision of my Ph.D research. Without him, many parts of this thesis would have been much smaller. I have learned about many interesting things from him, ranging from the beautiful topic of mathematics to communication. Whenever I wanted to discuss with him, he always turned up in time, even if when he was busy. He even met me at the airport when I first arrived at Sydney international airport and hosted me for a week, and hunted for accommodation with me. Meanwhile, thanks go to his wife, Jia Liu for her help, support and understanding. This thesis is dedicated to Mehmet A. Orgun, Liyin Xue, Josef Pieprzyk and Jinghua Xiao, without whom, none of this would have been even possible.

Fortunately, I was able to visit some places during my time as a Ph.D student. I am grateful to Prof. David Meyer (UCSD) and David Rideout (UCSD) for inviting me and giving me such a nice welcome. It was a pleasure to have been there, and to discuss and talk with them. A big "thank you" goes to Dr Chuan Wang and Prof. Fei Gao (BUPT) who have helped me understand quantum cryptography at the stage of rudiment. I have had many helpful discussions with others during this Ph.D, including Prof. Xiao Ma (SYSU), Prof. Ruiyao Duan (UTS) and Prof. Barry Sanders (UCalgary), Dr Haipeng Peng (BUPT), Prof. Lixiang Li (BUPT), Dr Xiaodong Lin (UOIT) and Prof. Shihong Wang (BUPT).

A great "thank you" goes to my junior high school teacher, Yong He, for his continual belief in me. He was never stingy with his smiles when I did well in class and in exams. It was amazing and moving for me to meet him outside my classroom of my university, he wanted to help me hunt for a job when he knew I would graduate. I will forever remember his words on my exercise book "I will

mount a long wind some day and break the heavy waves, and set my cloudy sail straight and bridge the deep, deep sea". His words gave me the strength to face life's difficulties. Without him, being able to insist on studying would have never been possible.

In order to complete my college and master education, I had to make money by working as a tutor to pay for my tuition fees and living expenses in the past seven years. Fortunately, my college Headmaster Yanmei Qin gave me a lot of support, such as introducing students to me, helping me to apply various of scholarships and grants, never punishing me when I was late or even absent for every meeting on weekend when I gave a lesson to my students. My classmates always, particularly Yan Yang often looked for me when my students' parents wanted to inform me something because I did not have a cellphone at that time. Without their support and help, I could not finish my studies successfully during those seven years.

Special thanks to my academic brothers Shudong Li, Youliang Zhong, Jianjie Zhao, Xiong Li and Zhongtian Jia, for their care, support and help in my studies and life. I would also like to thank my roommates Rongxiang Liu, Weimin Wang, Xiaoying Tan for enjoyable talks in the room, making my life more colorful.

Finally, and most importantly, I thank my parents for their support, making my study easy.

The generous financial help from Macquarie University is gratefully acknowledged.

To my teachers

Publications and submissions

This thesis has resulted in the following publications and submissions, my contribution to those publications and submissions is 75%.

Journal papers

1. H. Lai, J. H. Xiao, L. X. Li, Y. X. Yang, Recursive hiding of biometrics-based secret sharing scheme using adversary structure, *Information Processing Letters*, 683-687, 2012(112).

2. H. Lai, J. H. Xiao, L. X. Li, Y. X. Yang, Applying semi-group property of enhanced Chebyshev polynomials to anonymous authentication protocol. *Mathematical Problems in Engineering*, Volume 2012, Article ID 454823, 17 pages, 2012.

3. H. Lai, J. H. Xiao, M. A. Orgun, L. Y. Xue, J. Pieprzyk, Quantum direct secret sharing with efficient eavesdropping-check and authentication based on distributed fountain codes. *Quantum Information Processing*, 895-907, 2014(13).

4. H. Lai, M. A. Orgun, J. H. Xiao, L. Y. Xue, Fault-tolerant high-capacity quantum key distribution over a collective-noise channel, *Quantum Information Processing*, 1523-1535, 2014(13).

5. H. Lai, M. A. Orgun, J. H. Xiao, J. Pieprzyk, L. Y. Xue, Y. X. Yang, Provably secure three-party key agreement protocol using Chebyshev maps in the standard mode, *Nonlinear Dynamics*, 1427-1439, 2014(4).

6. H. Lai, L. Y. Xue , M. A. Orgun, J. H. Xiao, J. Pieprzyk, A hybrid quantum key distribution using extended unitary operations and distributed fountain codes, *Quantum Information Processing*, 697-713, 2015(14).

7. H. Lai, M. A. Orgun, J. H. Xiao, L. Y. Xue, J. Pieprzyk, Dynamic (2,3) threshold quantum secret sharing of secure direct communication, *Communications in*

Theoretical Physics, 459-465, 2015(63).

8. H. Lai, M. A. Orgun, J. Pieprzyk, J. H. Xiao, L. Y. Xue, Z. T. Jia, Controllable quantum private queries using an entangled Fibonacci-sequence spiral source, *Physics Letters A*, doi:10.1016/j.physleta.2015.05.040.

Conference papers

1. H. Lai, M. A. Orgun, L. Y. Xue, J. H. Xiao, J. Pieprzyk, Dual compressible hybrid quantum secret sharing schemes based on extended unitary operations, *Proc. SPIE 9123, Quantum Information and Computation XII*, Baltimore, USA, May, 1-13, 2014.

2. S. D. Li, H. Lai, W. B. Wu, S. W. Jiang, G. X. Hu, Novel space efficient secret sharing for implicit data security, *International Conference on Information Science and Digital Content Technology (ICIDT)*, Jeju Island, Korea (South). 283-286, 2012

Journal Submissions

1. H. Lai, M. A. Orgun, J. Pieprzyk, J. H. Xiao, L. Y. Xue, Lower-dimensional high-capacity quantum key distribution using Chebyshev-map values corresponding Lucas numbers coding, Submitted to *Journal of Physics A: Mathematical and Theoretical*, April 2015.

List of symbols

$\|\varphi\rangle$	An n-qubit pure state representing a quantum coin
L_n	The nth Lucas number
F_n	The nth Fibonacci number
C	The set of complex numbers
N	The set of natural numbers
$Cos(x)$	Cosine function
$\mathcal{L}$	The set of Lucas numbers
log_2	The logarithm with base 2
$\otimes$	The tensor product
$\oplus$	The modulo-2 addition operation

Abbreviations

QKD	Quantum key distribution
QSS	Quantum secret sharing
EPR	Einstein-Podolsky-Rosen
OAM	orbital angular momentum
SPDC	spontaneous parametric down-conversion
XOR	exclusive or
GHZ	Greenberger-Horne-Zeilinger
QSDC	quantum secure direct communication
RPSOs	phase shift operations
IPE	invisible photon eavesdropping
QBER	quantum bit error rate
HQKD	hybrid quantum key distribution
HQSS	hybrid quantum secret sharing

List of Figures

List of Tables

Contents

Chapter 1

Introduction

1.1 Motivation

More and more individuals and organizations are connecting their internal networks and computers to the insecure Internet, ranging from a bill payment and electronic banking to a global network contributing to a great amount of dollars of electronic commerce. Therefore, it is critical to provide security that can ensure the confidentiality and the integrity of data over the insecure channel. To address these issues, many secure cryptographic protocols and approaches have been proposed. Quantum cryptography is one of such critical methods, which allows communicating parties to establish a key over hostile network systems. The key provides a secure channel for subsequent use. Quantum cryptography employs quantum mechanics (rather than the assumed hardness of certain computational problems like the integer-factoring or discrete-logarithm problems in classical cryptography) to promise secure key distribution.

In 1994, Shor [1] showed that integer-factoring or discrete-logarithm problems in classical cryptography can be theoretically solved in polynomial time on a quantum computer. Since then, Shor's algorithm sparked a great deal of interest in the study of quantum

computers in the scientific community. Quantum computers are immensely powerful due to two main properties [2]: 1) they can be in multiple states at once, and 2) they can act on all of their states simultaneously. Though quantum computers may eventually put an end to many of the public key techniques that are widely used today, their potential realization is what spurred the research in quantum cryptography because quantum cryptography does not rely on unproven mathematical assumptions about the intrinsic difficulty of certain operations [3]. Quantum cryptography derives from quantum and cryptography. As we know, quantum is the minimum discrete quantity of any physical entity involved in an interaction (this definition is from wikipedia.org.), and cryptography is a technique for secure communication in the presence of an adversary. That is, by combining the classical cryptographic approach (i.e., one-time pad) with quantum effects [4], quantum cryptography enables these functions to work.

The strong point of quantum cryptography is that its security is guaranteed by laws of physics as it is impossible for an unauthorized party to copy an unknown quantum state. Therefore, many protocols for quantum cryptography including quantum key distribution and quantum secret sharing (which extends from two parties in quantum key distribution to more parties [5]) have been proposed in [3,6–21]. However, four major weaknesses have stood in the way of widespread applications of these protocols [22, 23], i.e., low coding capacity, low qubit efficiency, short achievable operating distances and low secure key generation rates. On the other hand, there are two major problems [24–26]: 1) It is very hard and expensive to deal with a lot of quantum data. And 2) Quantum information is fragile (here, it means that it is easy to be broken physically) in nature. In fact, these are also the main reasons why quantum cryptography has not yet been widely used in our daily life. In this thesis, these issues are studied and analyzed.

In Chapter 3 of this thesis, we first propose a high-capacity and extensible Quantum Key Distribution (QKD) protocol, in which the number of particles that are used to be

entangled is reduced but the dimensions of used entangled particles are increased in the protocol. Then, we construct 2-extended unitary operations to design two fault-tolerant high-capacity quantum key distribution protocols over a collective-noise channel, aiming at improving the capacity of a single photon and reducing the use of particles. We use recurrence and fountain codes to design two efficient quantum secret sharing protocols of secure direct communication in Chapter 4. Finally, we generalize 2-extended unitary operations to n-extended unitary operations. With the use of n-extended unitary operations, classical data can be combined with quantum data to implement hybrid quantum secret sharing and hybrid quantum key distribution protocols as discussed in Chapter 5. In the proposed protocols, the number of photons can be reduced to 1 in theory.

1.2 Related work

In this section, we present the related work for the subfields of quantum cryptography, i.e., quantum key distribution and quantum secret sharing.

1.2.1 Quantum key distribution

Quantum key distribution (QKD) is relatively new in the information security world, in which the laws of quantum mechanics are applied to create new cryptographic primitives. Wiesner [27] is the first researcher to use the properties of quantum mechanics to securely encode information in 1970s. However, in 1984, Bennett and Brassard (the BB84 protocol) [3] developed the first and the most famous prepare-and-measure quantum key distribution (QKD) protocol, in which Alice sends each qubit in one of four states of two complementary bases. In 1991, Ekert [7] proposed another well-known QKD protocol based on entanglement. After these groundbreaking protocols, there have been dozens of QKD protocols, but they are either based on the BB84 protocol or on Ekert 91. BB84

protocol's security is first proved by Mayers [28], and later by Shor and Preskill [29]. But most proofs are based on the assumption of idealized QKD system components, like well-characterized detectors and perfect single photon sources [30]. Therefore, Wang *et al.* [31] and Masanes *et al.* [32] proposed to use decoy particles or states and a device-independent method to address the above-mentioned weaknesses respectively. Moreover, quantum key distribution protocols can be implemented using a variety of different quantum technologies such as lasers, fibre-optics and free space transmission to mention a few. When the BB84 protocol was invented, the distance between two parties was in the range of a meter. In 1993, Muller *et al.* [33] reported that the distance could be increased to 1.1 km using fiber optic channels. In 2013, Inagaki *et al.* [34] demonstrated a solution that enabled the communicating parties to be 300 km apart.

In recent years, there has been a growing interest in the study of high-capacity quantum key distribution protocols that use high-dimensional Hilbert spaces. The study is motivated by the following two advantages: (1) it is expected that a single photon can be used to encode multiple bits of a shared key and (2) it seems that high-dimensional systems can be made robust against certain types of noise [35, 36]. The recent high-capacity quantum key distribution protocols have been reported in [22, 23, 37–39]. In Barreiro and Kwiat's protocol [37], the capacity of each entangled state has been enhanced by incorporating quantum states which are meanwhile entangled in multiple degrees of freedom "hyperentangled". Also, they have applied the hyperentanglement to advanced quantum communication such as remotely entangled state preparation and super-dense coding [6]. Mafu *et al.* [38] have shown that increasing the dimension contributes to increasing the information capacity per photon and key generation rates. But they have also found that the advantage of increasing the dimension is limited by practical implementations. Boyd *et al.*'s protocol [39] suffers from the corruption of the quantum state of the received photons due to atmospheric turbulence, though their proposed QKD protocol can enable

each photon to carry many bits of information by constructing a free-space. In 2013, Simon and Sergienko [23] have used a hyperentangled system to increase the Hilbert space dimension N, in which one entangled degree of freedom is used for key generation, and a different degree of freedom for security check. In Chapter 3, we use the conjugation relation between Lucas numbers and Fibonacci numbers to achieve pure classical key expansion based on Simon et al.'s work [22].

However, the above-mentioned high-capacity QKD protocols are studied in an ideal situation, i.e., a noiseless quantum channel. In actual settings, there always exists noise including thermal fluctuation, vibration, and an imperfection of the fiber in quantum channels during the process of transmitting qubits. All of those qubits will be affected by the same noise, which is caused by the variation of the noise sources that are longer than that of qubits traveling inside a time window. It is called collective noise. That is, if a few qubits are transmitted through the noise channel at the same time or they are close to each other spatially, the transformation of the noise on each of the qubits is identical [40].

Many studies on QKD protocols under collective noisehave been proposed [40–48], mainly focusing on collective-dephasing and collective-rotation noises. For example, in 2004, Boileau *et al.* [41] presented a QKD protocol under collective random unitary noise with the linear combination of two singlet states. In 2008, Li and Li [42] proposed two robust QKD protocols against two kinds of collective noise associated with the two Bell states $|\psi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)$ and $|\phi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B)$ to encode a message. Here $|0\rangle$ and $|1\rangle$ denote two possible states of a photon respectively, i.e., the horizontal polarization state and the vertical polarization state. They are the two eigenstates of the basis Z (that is, the Pauli operator σ_z). Their subscripts A and B represent two photons in an entangled state. In 2009, Li *et al.* [40] studied two robust quantum key distribution protocols under collective-dephasing and collective-rotation noiseusing quantum dense coding. In Chapter 3, we propose to use 2-extended unitary operations

over collective noiseto obtain higher-capacity quantum key distribution protocols [50].

1.2.2 Quantum secret sharing

Quantum secret sharing (QSS) (which is the generalization of QKD [5]), has made great progress since the first QSS protocol has been proposed by Hillery *et al.* [51] in 1999. Hillery *et al.*'s protocol is a natural extension of the classical secret sharing proposed by Shamir [52] and Blakley [53] in 1979 independently. Soon after Karlsson *et al.* [54] proposed another QSS protocol with a two-photon polarization entangled state. Since these two QSS protocols [51, 54] were presented, many authors [24, 55–77] have proposed a variety of QSS protocols in both theory and experiments. For theory, Xiao *et al.* [57] proposed an efficient multiparty QSS protocol. Deng *et al.* [73–75] presented a few protocols for QSS based on polarized single photons or EPR pairs. In 2010, Lin *et al.* [62] proposed a semi-quantum secret sharing protocol using entangled states, where Alice (who can perform any quantum operation) can securely distribute a key to Bob (who is classical). For experiments [76, 77], a QSS protocol based on four-state Grover algorithm was successfully demonstrated using the nuclear magnetic resonance technique.

In 2005, Zhang [78] generalized the work in [79] into the QSS regime, and proposed a new concept, i.e, QSS of secure direct communication. Thereafter, many researchers followed Zhang's work and proposed many new protocols. Moreover, QSS with continuous variables is shown to be feasible by Tyc and Sanders [80], who developed continuous variable threshold QSS and showed explicitly how to achieve the (2,3) threshold QSS special case. In 2002, Lance *et al.* [81] extended their protocol by utilizing an electro-optic feedforward technique and gave two further protocols. In Chapter 4, we also propose two quantum direct secret sharing protocols based on their work [82].

1.3 The Contributions and organisation of the thesis

1.3.1 Main contributions of the thesis

In this dissertation, we design and analyze several quantum cryptographic protocols to address the problems of the existing studies. To be exact, the major contributions of this dissertation are outlined as follows:

In Chapter 3, we first analyze Simon *et al.*'s protocol, and we observe that Lucas numbers (defined by $L_0 = 2$, $L_1 = 1$, $L_{n+2} = L_{n+1} + L_n$) have a close relationship to the first kind of Chebyshev polynomials (T_n), i.e., $2i^{-n}T_n(\frac{i}{2}) = L_n$ [83]. This relationship motivates us to propose an approach to lower-dimensional high-capacity quantum key distribution with pure classical key expansion. The proposed distribution of keys replacing Fibonacci numbers with Lucas numbers in analogy with the Simon *et al.* protocol [22] is valid because the dimensionality is the same as that in the previously proposed Fibonacci protocol. But in our approach, the actual coding uses Chebyshev-map values (which means that the variable $x, x \in \mathcal{C}$, is confirmed in Chebyshev polynomials) and k-Chebyshev-map values (which refer to the correlation of variable x), making consecutive and flexible key expansion possible. Due to the key expansion property, only a few Lucas numbers are required for a secure generation of long keys. Besides, proper Lucas numbers can be chosen to meet both longer distances and lower error rates at the same time. Therefore, our protocol can achieve lower-dimensional high-capacity quantum transmission.

The work on high-capacity quantum key distribution protocol using Chebyshev-map values corresponding to Lucas numbers coding appeared in the following paper:

H. Lai, M. A. Orgun, J. Pieprzyk, J. H. Xiao, L. Y. Xue, Lower-dimensional high-capacity quantum key distribution using Chebyshev-map values corresponding Lucas numbers coding, Submitted to *Journal of Physics A:*

Mathematical and Theoretical, April 2015.

In Chapter 3, we then analyze many QKD protocols over collective noises [40–48] and identify that either four- or six- photon entanglements [40, 41, 43, 44, 46] are used or the times of Bell-measurements [46] needed are much more than those of [42, 45]. Currently, the preparation of multi-photon entangled states and Bell-measurements are not easy to realize [49], which will increase the difficulty of the implementation of QKD protocols with the current technology. Though it is easier to implement some of the protocols in [42, 45] over collective noisein practice, the qubit efficiency is much lower compared to those in [40, 41, 43, 44, 46] (see Table 3.3). To obtain the advantages of the protocols in [40, 41, 43, 44, 46] (higher qubit efficiency) and those in [42, 45] (easier to implement), we propose a new approach to quantum key distribution based on the use of extended unitary operations from collective noisetogether with quantum dense coding [50].

The work on fault-tolerant high-capacity quantum key distribution over a collective-noise channel appeared in the following publication:

H. Lai, M. A. Orgun, J. H. Xiao, L. Y. Xue, Fault-tolerant high-capacity quantum key distribution over a collective-noise channel, *Quantum Information Processing)*, 1523-1535, 2014(13).

In Chapter 4, we show that a (2,3) (meaning that any two participants of all three participants can share a secret) discrete variable threshold quantum secret sharing protocol of secure direct communication can also be achieved based on recurrence using the same devices as in BB84. Besides, we use the idea of distributed fountain codes to let participants know the positions of the inserted nonorthogonal state particles and the control codes for the implementation of no-cloning principle for eavesdropping-check and authentication. The proposed protocol is inherently immune to Trojan horse attacks. Moreover,

every particle can on average carry up to 1.5-bit messages rather than at most 1 bit because the shares of smaller secret pieces are all accumulated into the shares of the largest secret piece, and Bobs can detect eavesdropping by themselves without sending classical messages to Alice due to the generated control codes, thereby enhancing the efficiency of quantum secret sharing.

The work on recursive (2,3) threshold quantum direct secret sharing appeared in the following publication:

> H. Lai, M. A. Orgun, J. H. Xiao, L. Y. Xue, J. Pieprzyk, Dynamic (2,3) threshold quantum secret sharing of secure direct communication, *Communications in Theoretical Physics*, 459-465, 2015(63).

In Chapter 4, we also propose a simple and effective way to achieve secure quantum direct secret sharing. The proposed protocol uses the properties of fountain codes to allow a realization of the physical conditions necessary for the implementation of no-cloning principle for eavesdropping-check and authentication. In our protocol, to achieve a variety of security purposes, nonorthogonal state particles are inserted in the transmitted sequence carrying the secret shares to disorder it. However, the positions of the inserted nonorthogonal state particles are not announced directly, but are obtained by sending the degrees and positions of a sequence that is pre-shared between Alice and Bobs. Moreover, Bobs can confirm that whether there exists an eavesdropper without sending classical messages to Alice. Most importantly, without knowing the positions of the inserted nonorthogonal state particles and the sequence constituted by the first particles from every EPR pair, the proposed protocol is shown to be secure.

The work on quantum direct secret sharing based on distributed fountain codes appeared in the following publication:

> H. Lai, J. H. Xiao, M. A. Orgun, L. Y. Xue, J. Pieprzyk, Quantum direct

secret sharing with efficient eavesdropping-check and authentication based on distributed fountain codes. *Quantum Information Processing*, 895-907, 2014(13).

In Chapter 5, we first introduce extended unitary operations by the tensor product of $n, n \geq 2$, basic unitary operations, and then use those extended operations and distributed fountain codes to design a hybrid QKD protocol. Meanwhile, we propose hybrid quantum secret sharing protocols based on a threshold and adversary structure. On the one hand, the extended unitary operations can eventually boil down to the four basic unitary operations when they are used to transform EPR pairs; on the other hand, the ultimate operations (i.e., the n-extended unitary operations (see Chapter 5)) can link the transition operation with control bits, making hybrid QKD and QSS protocols possible. Moreover, the number of digits of the key messages that can be carried by per photon is limited by practical considerations rather than by any matter of principle.

The work on hybrid QKD and QSS using extended unitary operations appeared in the following publications:

H. Lai, M. A. Orgun, L. Y. Xue, J. H. Xiao, J. Pieprzyk, Dual compressible hybrid quantum secret sharing protocols based on extended unitary operations, *Proc. SPIE 9123, Quantum Information and Computation XII*, Baltimore, USA, May, 1-13,2014.

H. Lai, L. Y. Xue , M. A. Orgun, J. H. Xiao, J. Pieprzyk, A hybrid quantum key distribution using extended unitary operations and distributed fountain codes, *Quantum Information Processing*, 697-713, 2015(14).

1.3.2 Organisation of the thesis

The structure of the thesis is as follows (see Figure 1.1).

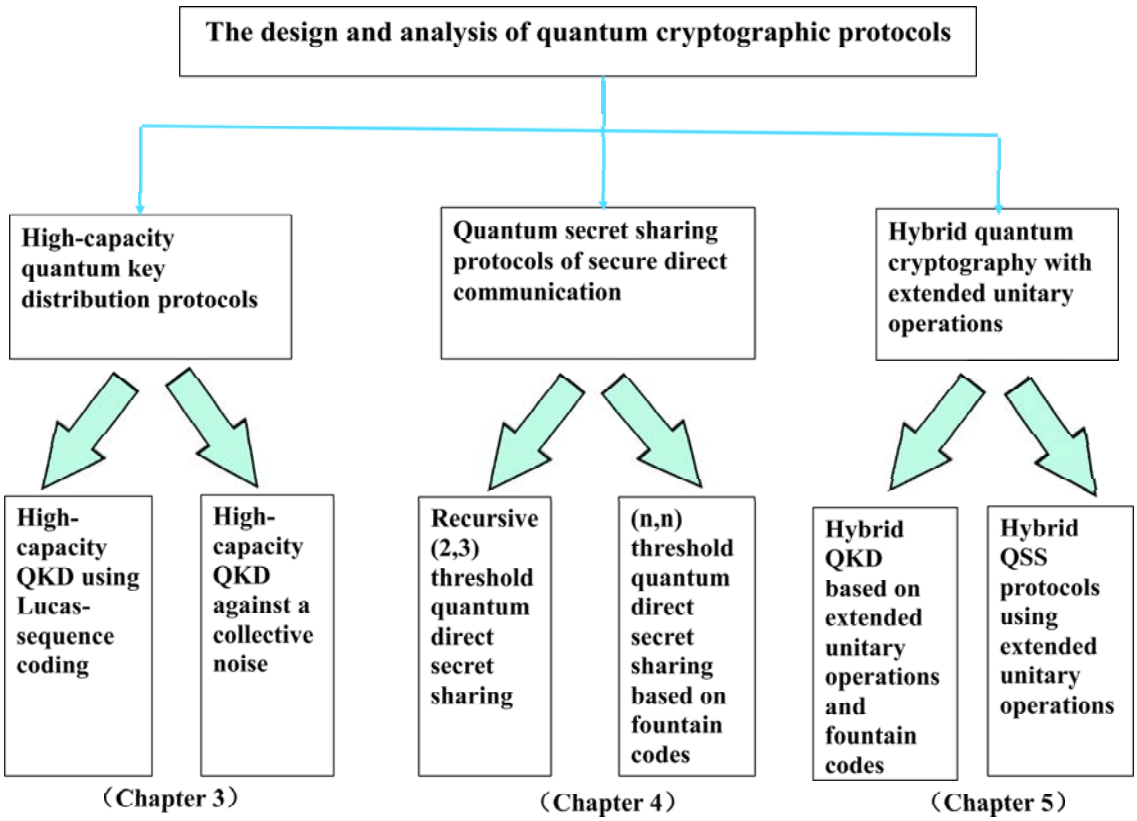

Figure 1.1: The sketch of the organisation of the thesis.

Chapter 3 presents three high-capacity quantum key distribution protocols using Lucas-sequence coding and 2-extended unitary operations over collective noise respectively.

Chapter 4 first describes a (2,3) threshold quantum secret sharing protocol for secure direct communication by utilizing fountain codes and a recursive secret encoding method. Then it generalizes it to (n, n) threshold quantum secret sharing.

Chapter 5 presents a hybrid quantum key distribution protocol and two hybrid quantum secret sharing protocols by extending the basic unitary operations to n-extended unitary operations, which combines the advantages of quantum cryptography with classical cryptography.

Chapter 6 outlines the major conclusions of the thesis and discusses future research directions.

Chapter 2

Preliminaries

In this section, we provide the preliminary background used in the thesis in a general way.

2.1 Cryptographic background

2.1.1 Fountain codes

Fountain codes (also known as rateless erasure codes) have the property that a potentially limitless sequence of encoding symbols can be generated on-line from a given set of k source symbols, as few or as many as needed. The process of generating an encoding symbol (see Figure 2.1) is conceptually very easy to describe [84, 85]:

1. choose the degree d $(1 \leq d \leq \mu)$ of the encoding symbol at random,
2. select at random exactly d distinct bits from the source symbols,
3. compute the value of the encoding symbol by XOR-ing d source symbols.

Definition 1. (Decoder recovery rule) [84, 85]: If there is at least one encoding symbol that has exactly one degree then the source symbol can be recovered immediately

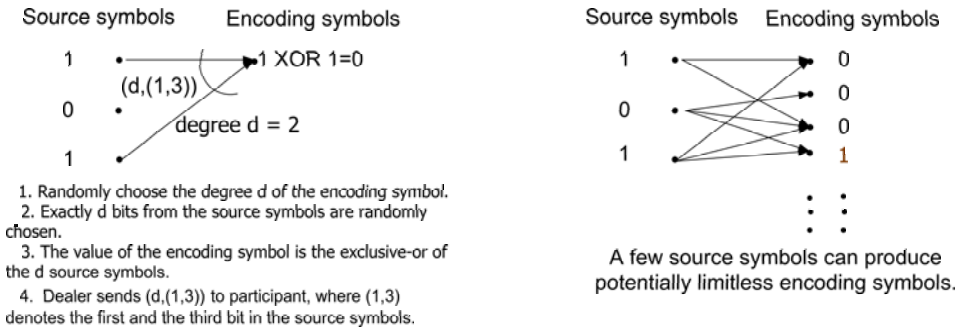

Figure 2.1: Generation of encoding symbols

since it is a copy of the encoding symbol. The value of the recovered source symbol is exclusive-ored into any remaining encoding symbols that also have that source symbol as a neighbor, the recovered source symbol is removed as a neighbor from each of these encoding symbols and the degree of each such encoding symbol is decreased by one to reflect this removal (see Figure 2.2).

Note that the "decoder recovery rule" does not need to be used in our protocols in Chapters 3-5. We stipulate that the communicating parties first share a sequence as source symbols before key distribution takes place. We simply use the idea of producing fountain codes to prepare control codes and obtain the positions of inserted nonorthogonal state particles based on the source symbols, which are established by using the way in BB84.

2.1.2 Hash functions

In our thesis, we use a suitable strongly collision-free hash function [86] in Chapter 5 for quantum secret sharing based on adversary structure , which takes as input a binary string of an arbitrary length, and produces as output a binary string of a fixed length. It has the following 4 properties.

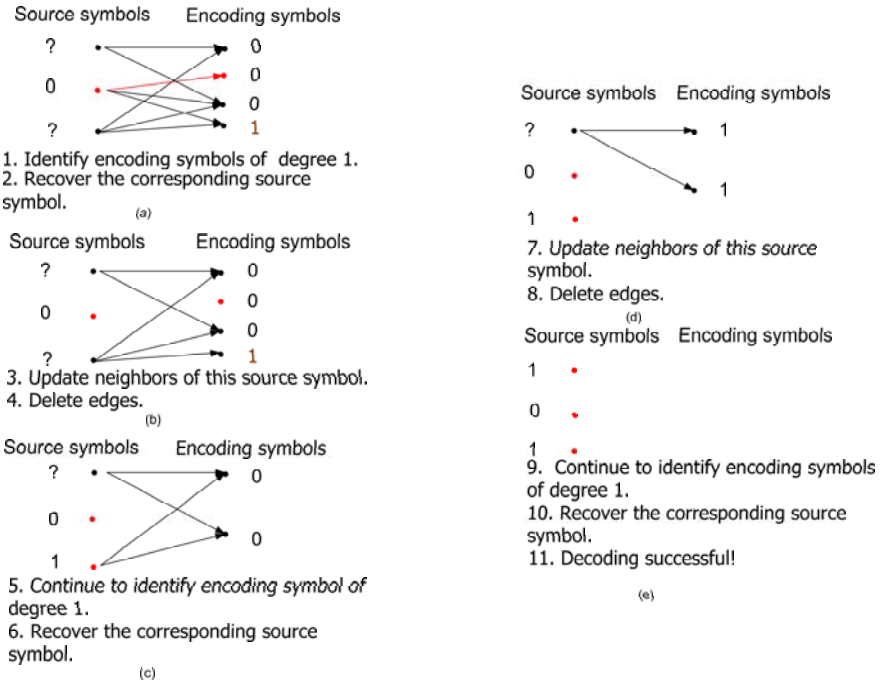

Figure 2.2: An introduction of the decoding process.

(1) It is easy to compute the hash value for any given message.

(2) It is infeasible to generate a message that has a given hash.

(3) It is infeasible to modify a message without changing the hash.

(4) It is infeasible to find two different messages with the same hash.

If, given a message x, it is computationally infeasible to find a message y not equal to x such that $H(x) = H(y)$ then H is said to be a weakly collision-free hash function.

A strongly collision-free hash function H is one for which it is computationally infeasible to find any two messages x and y such that $H(x) = H(y)$.

2.2 Mathematical background

2.2.1 Chebyshev maps

Definition 2 [87]. The first kind of Chebyshev maps of degree n ($n \in \mathbb{N}$) are defined

as

$$T_n(x) \quad = \quad cos(n \times arccos(x)), \{x | x \in \mathcal{C}\} \tag{2.1}$$

The recurrent formulas are defined as:

$$T_n(x) \quad = \quad 2xT_{n-1}(x) - T_{n-2}(x) \tag{2.2}$$

where $n \geq 2, T_0(x) = 1$, and $T_1(x) = x$.

For degree $n = 2, 3, 4, 5$, we can obtain the expressions as below from equation (2.2):

$$\begin{aligned} T_2(x) &= 2x^2 - 1 \\ T_3(x) &= 4x^3 - 3x \\ T_4(x) &= 8x^4 - 8x^2 + 1 \\ T_5(x) &= 16x^5 - 20x^3 + 5x \end{aligned} \tag{2.3}$$

Definition 3 [88]. The k-Chebyshev maps ($k \in \mathbb{N}^*$) are defined as

$$x_{m+1} = cos(k \times arccos(x_m)), \{x | x \in \mathcal{C}\} \tag{2.4}$$

Note that the k-Chebyshev maps refer to a function or a map.

According to Definitions 2 and 3, we have:

$$\begin{aligned} T_n(x_{m+1}) &= cos(n \times arccos(cos(k \times arccos(x_m)))) \\ &= cos(nk \times arccos(x_m)) \end{aligned} \tag{2.5}$$

2.2.2 Fibonacci numbers

First, we provide the basic background about the Fibonacci numbers [89].

Definition 4 [89]. The Fibonacci numbers or Fibonacci sequence are defined by the recurrence relation

$$F_n = \begin{cases} 1 & n = 0 \\ 1 & n = 1 \\ F_{n-1} + F_{n-2} & n \geq 2 \end{cases} \tag{2.6}$$

2.2.3 Lucas numbers

The Lucas numbers or Lucas series are an integer sequence named after the mathematician Francois Eduardo Anatole Lucas (1842-1891). He studied both Lucas numbers and Fibonacci numbers; the former is the closely related the later.

Similarly to the Fibonacci numbers, each Lucas number is defined to be the sum of the two immediate predecessors, that is, it is an integer sequence with Fibonacci recurrent relation. However, the first two Lucas numbers are $L_0 = 2$, $L_1 = 1$ instead of 1 and 1. Consequently, the properties of Lucas numbers are therefore somewhat different from those of the Fibonacci numbers.

First, we recall the definition of Lucas numbers, and then state some well-known facts on the Fibonacci and Lucas numbers [90].

Definition 5 [90]. (Lucas numbers). The Lucas numbers can be defined as follows:

$$L_n = \begin{cases} 2 & n = 0 \\ 1 & n = 1 \\ L_{n-1} + L_{n-2} & n \geq 2 \end{cases} \tag{2.7}$$

In particular, $L_2 = 3$, $L_3 = 4$, $L_4 = 7$, $L_5 = 11$, $L_6 = 18$, $L_7 = 29$, $L_8 = 47$, $L_9 = 76$.

The conjugation relation [90] between Lucas numbers and Fibonacci numbers is

$$L_{n+2} = F_{n+1} + F_{n-1} \tag{2.8}$$

Fibonacci numbers and Lucas numbers are special in the vast array of integer sequences [89]. In Chapter 4, we use the relation and difference between these two series to achieve efficient quantum key distribution for key expansion with Chebyshev-map values corresponding to Lucas numbers.

Moreover, Lucas numbers are related to the first kind of Chebyshev maps by the equation given below [83]

$$2i^{-n}T_n(\frac{i}{2}) = L_n, \tag{2.9}$$

where i is an imaginary number.

2.3 Quantum cryptographic background

To better understand the content in our thesis, we now present the following quantum cryptographic background.

Given a two-level quantum system, each bit can be represented by using a basis consisting of two eigenstates $|0\rangle$ and $|1\rangle$. Moreover, any state can be denoted as a linear combination of $|0\rangle$ and $|1\rangle$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2.10}$$

where $\alpha, \beta \in \mathcal{C}$ and $\alpha^2 + \beta^2 = 1$.

The bit in a quantum system is called a quantum bit or qubit. Multiple qubits can form a quantum system together. For example, the space of a two-qubit system is the tensor product of their spaces, and the joint state of two qubits is spanned by the basis

$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. In principle, the space of an n-qubit system can be modeled as a 2^n dimensional complex vector space [8].

2.3.1 Two important principles

When designing quantum cryptosystems, the following two laws of quantum mechanics must be taken into consideration.

Heisenberg uncertainty principle

Different from classical physics, quantum mechanics guarantee that the act of measurement is integral. Therefore, it is impossible to encode information into quantum properties of a photon without being detected. This statement is known as the Heisenberg uncertainty principle [8].

This principle plays a critical role in preventing the attempts of eavesdroppers in a cryptosystem based on quantum cryptography. For any two observable properties linked together like mass and momentum, we have that

$$\langle\langle \triangle\ A\rangle^2\rangle\langle\langle \triangle\ B\rangle^2\rangle \geq \frac{1}{4}||\langle[A, B]\rangle||^2 \tag{2.11}$$

where $\triangle\ A = A - \langle A\rangle$, $\triangle\ B = B - \langle B\rangle$, and $[A, B] = AB - BA$, where A and B are a pair of operators.

Given the principle, two interrelated properties must be measured individually but the measurement affects the other. This is because it is impossible to partition a photon into two halves and to measure its state without affecting its value. Consequently, if anyone tries to detect the state of photons being sent to the receiver, the receiver can detect an error [8].

No cloning theorem

Wootters and Zurek [8] proved that it is impossible for an adversary to have a perfect copy of Alice's message in the quantum world.

The ideal machine would produce:

$$\varphi \otimes |b\rangle \otimes |0\rangle \longrightarrow \varphi \otimes \varphi \otimes |f_\varphi\rangle \tag{2.12}$$

where $|f_\varphi\rangle$ denotes the final state of Eve's machine which might depend on φ. Accordingly, using obvious notations,

$$|\uparrow, b, 0\rangle \longrightarrow |\uparrow, \uparrow, f_\uparrow\rangle \tag{2.13}$$

$$|\downarrow, b, 0\rangle \longrightarrow |\downarrow, \downarrow, f_\downarrow\rangle \tag{2.14}$$

By linearity of quantum dynamics it follows that

$$\begin{aligned} |\rightarrow, b, 0\rangle &= \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle) \otimes |b, 0\rangle \\ &\rightarrow \frac{1}{\sqrt{2}}(|\uparrow, \uparrow, f_\uparrow\rangle + |\downarrow, \downarrow, f_\downarrow\rangle) \end{aligned} \tag{2.15}$$

But the latter state differs from the ideal copy $|\rightarrow, \rightarrow, f_\rightarrow\rangle$, whatever the states $|f_\varphi\rangle$ are.

Because the perfect quantum copy machines cannot exist, Eve cannot obtain a perfect quantum copy. Making a perfect copy can be done in classical cryptography and that is why classical cryptography cannot detect eavesdropping. However, the quantum no cloning theorem prevents Eve from perfect eavesdropping, making quantum cryptography potentially secure.

2.3.2 Quantum entanglement

In short, quantum entanglement, one of the central principles of quantum physics, means that multiple particles are linked together. As long as one particle's quantum state is measured, the other particles can be determined. Moreover, the states of individual particles cannot be used to describe the entangled particles, but all entangled particles from the entangled state can share information, no matter how far apart the particles may be at the time.

EPR (Einstein-Podolsky-Rosen) pairs [6]

In quantum information science, the Bell states are a concept and represent the simplest examples of entanglement. An EPR pair is in one of the four Bell states shown as follows:

$$\begin{aligned} |\psi^+\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B), |\psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B), \\ |\Phi^+\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B), |\Phi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B). \end{aligned} \tag{2.16}$$

2.3.3 Unitary operations

A unitary operator is a rotation of a Hilbert space about the origin. Four unitary operations [91] U_0, U_1, U_2, U_3 are listed as follows.

$$U_0 = I_2 \otimes I_2 = \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{2.17}$$

$$U_1 = I_2 \otimes \sigma_x = \begin{pmatrix} \sigma_x & 0 \\ 0 & \sigma_x \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{2.18}$$

$$U_2 = I_2 \otimes -i\sigma_y = \begin{pmatrix} -i\sigma_y & 0 \\ 0 & -i\sigma_y \end{pmatrix} = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{2.19}$$

$$U_3 = I_2 \otimes \sigma_z = \begin{pmatrix} \sigma_z & 0 \\ 0 & \sigma_z \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \tag{2.20}$$

where σ_x, σ_y and σ_z are the Pauli matrices.

Dense coding

In 1992, C. H. Bennett and S. J. Wiesner presented the special feature of Einstein-Podolsky-Rosen (EPR) pairs, i.e., dense coding [6]. Without loss of generality, suppose that Alice and Bob share an EPR pair $|\psi^-\rangle_{AB}$, that is, Alice holds particle A and Bob has B. Alice can encode two bits of messages into the state by performing one of the four basic local unitary operations on particle A, under which this state changes as:

$$U_0^A|\psi^-\rangle = |\psi^-\rangle, U_1^A|\psi^-\rangle = |\psi^+\rangle, U_2^A|\psi^-\rangle = |\phi^-\rangle, U_3^A|\psi^-\rangle = |\phi^+\rangle. \tag{2.21}$$

where the superscript A denotes the photon on which unitary operations are performed. Then Alice transmits the encoded particle A to Bob via a quantum channel. Bob can distinguish which unitary operation is performed by Alice using Bell measurement on

particles A and B. Bob is able to obtain two-bit messages from Alice when U_0, U_1, U_2, U_3 represent 00, 01, 10, 11 separately. For instance, Bob knows Alice's message is 11 if his measurement result is $|\phi^+\rangle$. Likewise, any one of the four EPR pairs can be used as the original state in the communication.

Chapter 3

High-capacity quantum key distribution protocols

In this chapter, with Chebyshev-map values corresponding to Lucas numbers coding, we achieve a lower-dimensional high-capacity protocol for quantum key distribution which can greatly enhance the number of digits of the key that can be carried per photon. Moreover, our protocol can be implemented without the limit of OAM bandwidths and exchanging classical messages for key generation. Also, we present two high-capacity quantum key distribution protocols over collective noise using 2-extended unitary operations.

3.1 Introduction

In recent years, there has been a growing interest for researchers to study high-capacity quantum key distribution protocols by developing high-dimensional Hilbert spaces due to two main advantages. First, multiple bits of a shared key can be encoded on a single photon. Second, high-dimensional systems can be more robust against certain types of noise [35, 36]. Consequently, the use of many degrees of freedom of photons has been

investigated, including position momentum [92], time [93], energy time [94–96] and orbital angular momentum (OAM) [97–100]. Among these methods, according to Simon *et al.* [22], OAM with spontaneous parametric down-conversion (SPDC) is the most promising in producing entangled OAM states. This is because SPDC is able to provide photon pairs that are not only entangled in states of a single degree of freedom, but also are actually hyper-entangled in both polarization and OAM at the same time.

Yu *et al.* [101] propose to use planar plasmonic interfaces to produce optical beams carrying single OAM states. It is also shown that, in nanoplasmonic Vogel spiral arrays, distinctive scattering resonances can support photonic band gaps with band edge modes carrying multiple OAM values distributed among Fibonacci numbers [22]. Moreover, Vogel spiral arrays can generate multiple OAM states encoding a well-defined numerical sequence in their far-field radiation patterns [102]. Also, it is reported in [103] and [104] that a down-conversion bandwidth of over 40 is possible and an entanglement between photons with OAM of the order of 600 can be achieved. Based on these, Simon *et al.* [22] suggest a different form of high-capacity and high-efficiency quantum cryptography. They apply specially engineered OAM-entangled states of light and Fibonacci numbers to achieve it. However, the high capacity of the Simon *et al.* protocol [22] is still limited by implementation difficulties and the coding is not so flexible. This is because increasing the information capacity depends on OAM with greater bandwidths and the method used for encoding. As a result, due to the limitation of bandwidths in practice, it is unlikely to meet both the longer distance and lower error rates simultaneously. In other words, if smaller Fibonacci values for pump values are used, then photons can travel longer distances but at the expense of higher error rates. If, however, larger Fibonacci values for pump values are used, then error rates can be made low but photons can travel short distances.

To address the above mentioned problems, in this chapter, we first propose an approach

which could be considered as lower-dimensional high-capacity quantum key distribution using Chebyshev-map values corresponding Lucas numbers coding. Simon *et al.* [22] comment that their experiment setup will also work when Fibonacci numbers are replaced by Lucas numbers. That is to say, we can replace the Fibonacci values onto entangled orbital angular momentum states in Simon *et al.*'s protocol with Lucas numbers. This alone would not be sufficient to overcome the limitation of the Simon *et al.* protocol. We observe that Lucas numbers have a close relationship to the first kind of Chebyshev maps (T_n), i.e., $2i^{-n}T_n(\frac{i}{2}) = L_n$ [83]. This relationship motivates us to propose an approach to lower-dimensional high-capacity quantum key distribution using Chebyshev-map values corresponding to Lucas numbers coding, to address the above two weaknesses. The proposed distribution of keys replacing Fibonacci numbers with Lucas numbers in analogy with the Simon *et al.* protocol [22] is valid because the dimensionality is the same as that in the previously proposed Fibonacci protocol. But in our approach, the actual coding uses Chebyshev-map values (which means that the variable $x, x \in \mathcal{C}$, is confirmed in Chebyshev maps) and k-Chebyshev-map values (which refer to the correlation of variable x), making consecutive and flexible key expansion possible. Due to the key expansion protocol, only a few Lucas numbers are required for a secure generation of long keys. Besides, proper Lucas numbers can be chosen to meet both longer distances and lower error rates at the same time. Therefore, our protocol can achieve lower-dimensional high-capacity quantum transmission.

On the other hand, many studies on QKD protocols focusing on collective-dephasing and collective-rotation noise have been proposed [40–48]. In [40,41,43,44,46], either four- and six-photon entanglements are used or the times of Bell-measurements needed [46] are much more than those of [42,45]. However, the preparation of multi-photon entangled states and Bell-measurement are not easy to realize [49], which will increase the difficulty of the implementation of QKD protocols with the current techniques. In [42,45], though it

is easier to implement the protocols over collective noise in practice, the qubit efficiency is much lower compared those in [40,41,43,44,46] (see Table 3.2). To obtain the advantages both the protocols in [42, 45] (higher qubit efficiency) and those in [40, 41, 43, 44, 46] (easier to implement), we propose a new approach to quantum key distribution based on the use of extended unitary operations from collective noise together with quantum dense coding. The motivation for this approach is that, the original proposals for QKD against a collective noise, encoded information into the logical qubit of an individual photon or an entangled state. Consequently, only one or two bits of information can be compressed into each logical qubit.

In our last two protocols, the method that we use is to first extend the four unitary operations based on collective noise to sixteen 2−extended unitary operations, and then encode each logical qubit with one of the sixteen extended unitary operations. Bob can deduce the unitary operations performed by Alice using the initial states, the measurement outcomes and a collation table pre-shared by Alice and Bob. Though the pre-shared collation table is used, the capacity of every Bell-state is enhanced. This is worthwhile because a quantum bit is more expensive to prepare than a classical bit. Actually, there is no limit to how many bits of information can be compressed into a logical qubit, as the unitary operations from collective noise together with quantum dense coding can be extended to the infinite-dimension case. Our current aim is to compress four bits of information into every logical qubit. One motivation for doing this is that the rate of data transmission is therefore increased. Another more subtle motivation for using a large number of extended unitary operations is that the security of the protocol can be increased in this manner.

3.2 High-capacity QKD using Lucas-sequence coding

3.2.1 Entangled Lucas-sequence spiral source

When the Fibonacci sequences are replaced by Lucas sequences, Simon *et al.* said that their protocol also works. Moreover, Lucas sequences (L_n) are related to the Chebyshev maps (T_n) by the equations $2i^{-n}T_n(\frac{i}{2}) = L_n$ [83]. Hence, we can consider an entangled Lucas-sequence spiral source, which uses the same mechanism of an entangled Fibonacci spiral source as in [22]. That is, a different entangled light source which may be used to physically implement the OAM-based realization of QKD protocol. According to a scaling factor a_0 and a divergence angle α by $r_n = \sqrt{n}a_0$ and $\theta_n = n\alpha$, a Vogel spiral being an array of N particles with polar positions (r_n, θ_n) is represented by a density function [102]:

$$\rho(r,\theta) = \sum_{n=1}^{N} \delta(r - \sqrt{n}a_0)\delta(\theta - n\alpha) \tag{3.1}$$

For arbitrary α and a_0 [102], the Fraunhofer far field Vogel spirals can be computed analytically, within scalar diffraction theory. The far field [102] with a diffracted input beam in cylindrical coordinates is as follows:

$$E_\infty(v_r, v_\theta) = E_0 \sum_{n=1}^{N} e^{j2\pi\sqrt{n}a_0 v_r cos(v_\theta - n\alpha)} \tag{3.2}$$

where (v_r, v_θ) are the Fourier conjugate variable of (r, θ). Fourier-Hankel analysis of the calculated far-field radiation is performed to decompose it into radial and azimuthal components, providing the OAM values [102].

Due to the conjugate relation between Lucas and Fibonacci numbers ($L_{n+2} = F_{n+1} + F_{n-1}$), the experiment setup in Simon *et al.*'s protocol also works when Fibonacci numbers are replaced by Lucas numbers. Hence, we consider an entangled Lucas number spiral

source (see Figure 3.1), which can use the same mechanism of an entangled Fibonacci spiral source as in [22]. Figure 3.1 demonstrates that a schematic of our improved high-capacity QKD based on Simon's protocol using Lucas sequences, in which the relationship between Chebyshev-map values and Lucas numbers of the spiral source enable a different way of achieving high-capacity QKD. The method can achieve consecutive and flexible key expansion using Chebyshev maps. To be exact, though the source produces entangled photons whose orbital angular momenta (OAM) values are Lucas numbers, we encode key messages with the Chebyshev-map values corresponding to Lucas numbers. The coding rules are described as follows.

3.2.2 Coding rules of proposed protocol

Before giving details of our protocol, we need to initialise the protocol parameters.

1. Choose N consecutive *proper* Lucas numbers set $\mathcal{L}=\{L_{n_0}, L_{n_0+1}, \ldots, L_{n_0+N-1}\}$, where "proper" means that the numbers should allow encodings with a desired tradeoff between transmission distances and error rates. This step is a modification of Simon *et al.*'s protocol [22]. The Lucas numbers are next converted into Chebyshev-map values. The values are used to encode $\log_2 N$-bit key information. Note that as Lucas numbers are related to the first kind of Chebyshev maps by Equation (2.14), so we have $x_{m+1} = \frac{i}{2} = cos(k \times arccos(x_m))$.

2. Generate at random the values k and m using the pre-shared source files between Alice and Bob and the fountain codes (see Figure 2.1). The values $x_m, \cdots, x_1$ are determined using the k-Chebyshev map from Equation (2.4).

3. Compute $T_r(x_m), \cdots, T_r(x_1), r = n_0, \ldots, n_0 + N - 1$. Note that $\log_2^m$-bit key information can be encoded using each of m Chebyshev-map values, following $T_r(x_{m+1})$

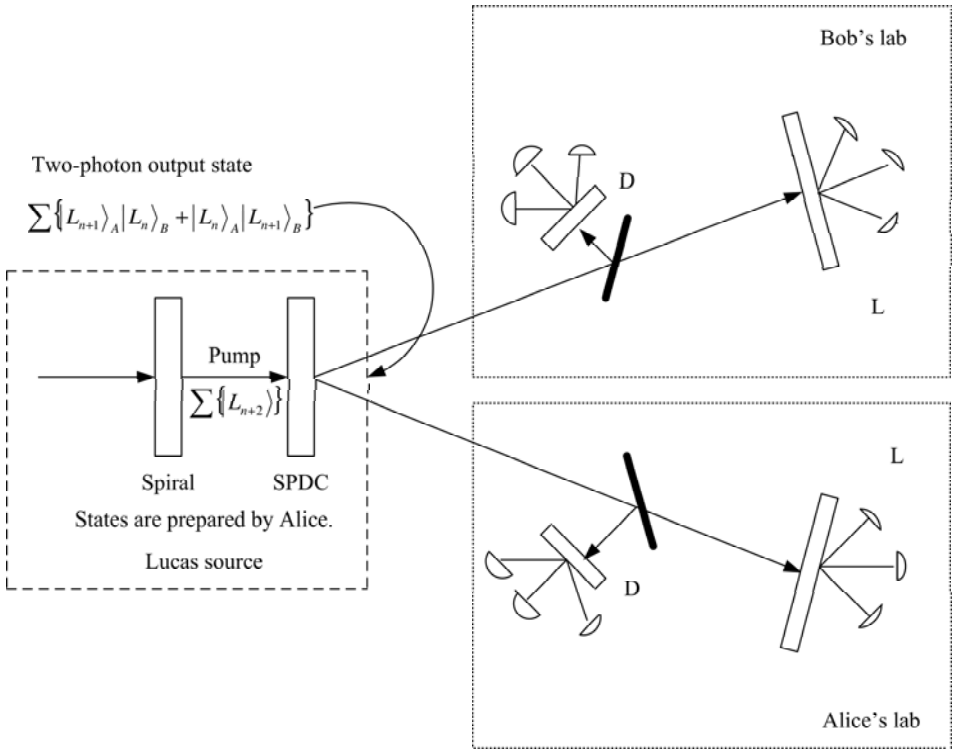

Figure 3.1: Experimental setup for lower-dimensional high-capacity QKD with Lucas-valued OAM (adapted from [22]). A laser interacts with a Vogel spiral array, producing intense superpositions of states with Lucas OAM, $l = L_n$, that then pump the nonlinear crystal, producing signal-idler pairs through SPDC. The OAM sorters that are labeled L are used for allowing photons to arrive at the arrays of single-photon detectors when they are Lucas valued as well, and the devices labeled D are used for allowing "diagonal" superposition of the form $\frac{1}{\sqrt{2}}(|L_n\rangle + |L_{n+2}\rangle)$, and filtering any non-Lucas valued entangled photons.

that corresponds to L_r. The value m is determined by the quality of the quantum channel. That is, the lower the error rate is, the larger the m is.

Therefore, if OAM values in the set of $\{L_{n_0}, L_{n_0+1}, \ldots, L_{n_0+N-1}\}$ are used, then each photon can be used to carry $\log_2 N$ to $(\log_2 N + m \log_2 m)$ bits of classical information.

To illustrate the initialisation process, consider an example for $N = 4, m = 8$,

1. Alice chooses $\{L_6, L_7, L_8, L_9\}$, and calculates $\{T_6(\frac{i}{2}), T_7(\frac{i}{2}), T_8(\frac{i}{2}), T_9(\frac{i}{2})\}$. Every

value from $\{T_6(\frac{i}{2}), T_7(\frac{i}{2}), T_8(\frac{i}{2}), T_9(\frac{i}{2})\}$ can be used to encode two bits of classical information. The encoding can look as follows.

$$\begin{aligned} T_6(x_{m+1}) &= T_6\left(\frac{i}{2}\right) \Rightarrow 00, \\ T_7(x_{m+1}) &= T_7\left(\frac{i}{2}\right) \Rightarrow 01, \\ T_8(x_{m+1}) &= T_8\left(\frac{i}{2}\right) \Rightarrow 10, \\ T_9(x_{m+1}) &= T_9\left(\frac{i}{2}\right) \Rightarrow 11. \end{aligned} \tag{3.3}$$

2. According to Equation (2.9) and assuming that $x_{m+1} = x_9 = \frac{i}{2}$ in Equation (2.4), Alice computes $x_8, x_7, \cdots, x_1$ and obtains $T_6(x_8), \cdots, T_6(x_1), \cdots, T_9(x_8), \cdots, T_9(x_1)$.

3. Alice takes the values $T_{i'}(x_8), \cdots, T_{i'}(x_1)$; $i' = 6, 7, 8, 9$, and uses them to encode the key. The encoding is as follows:

$$\begin{aligned} &T_{i'}(x_{j_1}) \Rightarrow 000, \quad T_{i'}(x_{j_2}) \Rightarrow 001, \\ &T_{i'}(x_{j_3}) \Rightarrow 010, \quad T_{i'}(x_{j_4}) \Rightarrow 011, \\ &T_{i'}(x_{j_5}) \Rightarrow 100, \quad T_{i'}(x_{j_6}) \Rightarrow 101, \\ &T_{i'}(x_{j_7}) \Rightarrow 110, \quad T_{i'}(x_{j_8}) \Rightarrow 111, \end{aligned} \tag{3.4}$$

where the indices $j_1, j_2, \ldots, j_8$ running through all possible permutations of eight elements. For instance, for the permutation of three elements, the indices run through the set $\{(1,2,3), (1,3,2), (2,1,3), (2,3,1), (3,1,2), (3,2,1)\}$. However, the permutation of $j_1, j_2, \ldots, j_8$ that will be used should be determined by the value $(i' \times k) mod\ 8!$ in the exact protocol.

Note that according to $x_{m+1} = cos(k \times arccos(x_m)) = \frac{i}{2}$, we can obtain $x_8 = arccos(k^{-1} \times arccos(\frac{i}{2}))$. We do not need to compute the values $T_{i'}(x_j)$ for $i' = 6, 7, 8, 9$ and $j = 1, \ldots, 8$ after obtaining x_m; $m = 1, \ldots, 8$.

As illustrated in the above example, we can just use four Lucas numbers for OAM values, but each Lucas number can then represent a twenty-six-digit binary string, increasing the encoding capacity from two-digit binary strings to twenty-six-digit binary strings. This is because of the use of another twenty-four-digit binary string from the key expansion in Equation (3.4) with k-Chebyshev maps.

3.2.3 Proposed protocol

The protocol is similar to Simon *et al.*'s protocol and therefore the setup is the same as the one from Figure 3.1. Alice and Bob use their L and D OAM sorters that allow L-type and D-type measurements, respectively. The L sorters allow measurements of photons, when their states are encoded using Lucas numbers. The D sorters, on the other hand, measure photon states using "diagonal" superposition of the form $\frac{1}{\sqrt{2}}(|L_n\rangle + |L_{n+2}\rangle)$, and filtering any non-Lucas numbers.

In Figure 3.1, the light coming from the entangled spiral source is in a superposition of states with OAM equal to Lucas numbers. All the states that leave the spiral and enter the down-conversion crystal must be of the form $\sum_{n=n_0}^{n_0+N-1} |L_{n+2}\rangle, n_0 \geq 1, n_0 \in \mathbb{N}$. Down-conversion breaks each $|L_{n+2}\rangle$ into two smaller OAM values, $|L_{n+1}\rangle$ and $|L_n\rangle$. Similar to [22], during the process of transmission and detection, the OAM sorters can be used to block all outgoing states that are non-Lucas numbers, i.e., not in $|L_{n+2}\rangle$, protecting against possible problems such as turbulence-induced OAM changes.

The OAM conservation law in collinear SPDC implies that $L_{n_i} + L_{n_s} = L_{n+2}$ (a pump photon is incident on a nonlinear crystal and decays into two photons with less energy from SPDC, usually called "signal" and "idler"), where L_{n_i},L_{n_s},L_{n+2} are the Lucas numbers of signal beam, idler beam and pump beam respectively. Together with Lucas recurrence relation and the restriction to outgoing values in $\mathcal{L}$, collinear SPDC forces L_{n_i} and L_{n_s} to be the two Lucas numbers immediately preceding L_{n+2}, where L_{n_i} is the signal value and

L_{n_s} is the idler value. But signal (or idler) value can be in signal (or idler) beam. Hence, the result is the following OAM-entangled outgoing state

$$\sum_n \{|L_{n+1}\rangle|L_n\rangle + |L_n\rangle|L_{n+1}\rangle\}_{AB}. \tag{3.5}$$

Note that if pump values L_{n+2} between 18 and 76 are used, then only values of L_{n_i} and L_{n_s} between 11 and 47 should appear.

Before presenting the protocol, we list the assumptions made.

3.2.4 Four Cases for Alice's and Bob's Detectors

The beam splitter in Alice's (Bob's) laboratory sends the entangled photon to either L or D sorter at random. So, there are four possible cases:

- The beam splitters in both Alice's and Bob's laboratories send the entangled photon to the L sorters.
- The beam splitter in Alice's laboratory sends the entangled photon to the L sorters, and the beam splitter in Bob's laboratory sends the entangled photon to the D sorters.
- The beam splitter in Alice's laboratory sends the entangled photon to the D sorters, and the beam splitter in Bob's laboratory sends the entangled photon to the L sorters.
- The beam splitters in both Alice's and Bob's laboratories send the entangled photon to the D sorters.

For the first three cases, Alice and Bob can establish a key with the following steps.

Step 1 Alice and Bob share a small sequence S of length l (whose length grows sublinearly in the number of channel uses [105]), such as

$\{\underbrace{0, 01, 0, 1001, 10, 10, 1011, 01, 00, \cdots, 1010}_{l\ bits}\}$. Note that the division to S is flexible. When it changes, Alice/Bob informs Bob/Alice by sending the positions of the bits in S via an authenticated classical channel.

Step 2 Assume an entangled state with OAM in $\mathcal{L}$ (take $l = L_{n+2} = L_9$ as an example). The setup in Figure 3.1 is arranged so that the two OAM values Alice and Bob obtain must be the two Lucas numbers preceding that of the pump ($L_{n+1} = L_8$ and $L_n = L_7$ in our example). However, which goes to Alice and which goes to Bob is undetermined (see Figure 3.2). Hence, the exchange of classical messages is needed to remove the uncertainty between Alice and Bob via an authenticated classical channel.

Step 3 After both of them receive a photon from SPDC, Alice (Bob) records the sorter that the photon goes to and the definite OAM value detected. Finally, Alice (Bob) publicly announces them with the degrees and positions of S to Bob (Alice).

With the pre-shared source files between Alice and Bob and the degrees and positions of the source files sent by each other, Alice and Bob can use the obtained encoding packets, to know the each other's sorters and the type of the entangled states and the values k and m for key generation and eavesdropping detection with the following agreements.

(1) 0, then either the beam splitter in Alice's (Bob's) laboratory sends the entangled photon to the D sorter or Alice's (Bob's) detected Lucas values are even.

(2) 1, then either the beam splitter in Alice's (Bob's) laboratory sends the entangled photon to the L sorter or Alice's (Bob's) detected Lucas values are odd.

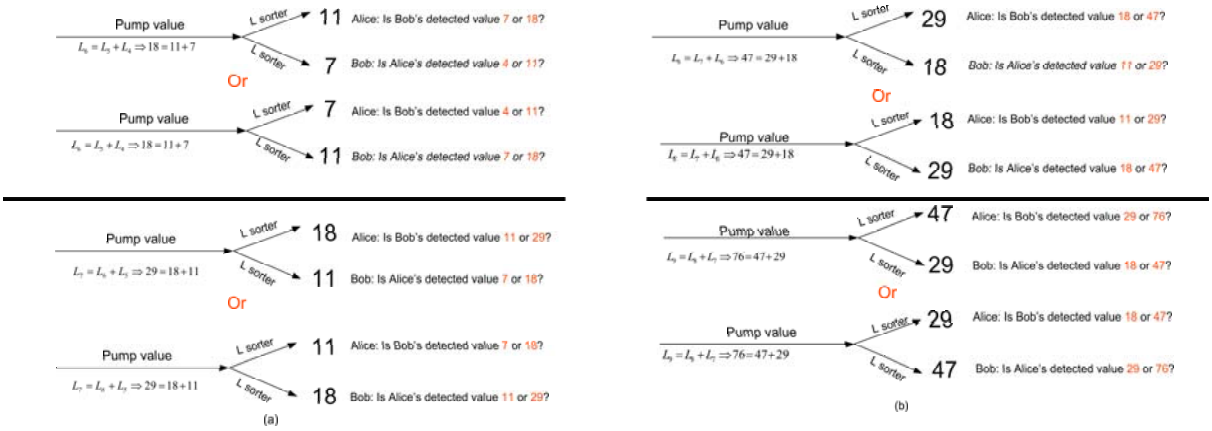

Figure 3.2: Possible outcomes for the example of the pump value $l = 7, 11, 18, 29$.

(3) 10, then the beam splitter in Alice's (Bob's) laboratory sends the entangled photon to the L sorter, and the detected Lucas value is the smaller of the two odd Lucas numbers that Alice (Bob) speculates.

(4) 11, then the beam splitter in Alice's (Bob's) laboratory sends the entangled photon to the L sorter, and the detected Lucas value is the larger of the two odd Lucas numbers that Alice (Bob) speculates.

However, the Eve cannot know exact sorters or Alice's (Bob's) detected Lucas values without the pre-shared sequence S. The security of our protocol is based on the following fact: when one of the parties detects a particular Lucas number, it is not certain what number the other party would detect (see Figure 3.2). For example, if Alice measures value $L_{n+1} = L_8$, then the value Bob measures can be either $L_{n+2} = L_9$ or $L_n = L_7$.

Step 4 After receiving the degrees and positions of the pre-shared sequence S, Alice and Bob can remove the uncertainty in terms of (1)-(4) in Step 3. Therefore, Alice and Bob can obtain the pump value L_9 by recovering each other values and adding them to their received and measured values.

According to the coding rules, Alice and Bob can further obtain $T_9(\frac{i}{2})$ and two-bit key information from $T_9(\frac{i}{2})$, and $x_8, \cdots, x_1$ using equations $2i^{-n}T_m(\frac{i}{2}) = L_m$ and $\frac{i}{2} = x_9 = cos(k \times arccos(x_8))$, respectively. Meanwhile, Alice sends the degrees and positions of the set of source files S for getting the values k and m to Bob via an authenticated classical channel. Finally, both of them can compute $T_9(x_{j_1}), T_9(x_{j_2}), T_9(x_{j_3}), \cdots, T_9(x_{j_m})$ using $(9 \times k) mod\, m!$ with their obtained i' and k and m, and the binary numbers for $T_9(x_{j_1}), T_9(x_{j_2}), T_9(x_{j_3}), \cdots, T_9(x_{j_m})$ can be similarly obtained in terms of Equations (9) and (10).

Step 5 Once the sorting has been done and the corresponding digital OAM values have been converted into binary numbers, the analysis of error rates, error correction, and privacy amplification are similar to those involved in other proposed QKD protocols [8].

Case 4. When both Alice and Bob choose the D sorters, they will both receive superposition states, they randomly choose the degrees and positions for generating encoding packet 0, and send it to let each other know those information via an authenticated classical channel. As a result, the pump value is still a superposition state, and Alice and Bob cannot uniquely determine the pump value. In this case, they will discard the instance.

3.2.5 Eavesdropping

Suppose that an adversary Eve is eavesdropping on the quantum channel between Alice and Bob. Clearly, she does not know, which type of detection measurement (D or L) is going to be chosen by Alice or Bob. So, Eve has no choice but to guess. If she chooses the D sorter when Alice chooses the L sorter or she chooses the L sorter when Alice chooses the D sorter, then the Alice measurement is going to be erroneous with the probability $\frac{1}{2}$. The Eve activity is going to be detected by Alice and Bob when they

compare their protocol transcripts.

More precisely, assume that Eve makes

1. a D-type measurement on a photon, which is actually in the eigenstate $|L_{n+2}\rangle$. Then she will detect one of the two superpositions $|L_{n+2}\rangle + |L_n\rangle$ or $|L_{n+2}\rangle + |L_{n+4}\rangle$, with probability $\frac{1}{2}$, respectively. She can send a copy of it to Alice. If Alice receives one of these superpositions and makes an L-type measurement, she will read out one of the values L_n, L_{n+2}, or L_{n+4}, with respective probabilities of $\frac{1}{4}$, $\frac{1}{2}$, $\frac{1}{4}$. However, she should obtain $|L_{n+2}\rangle$ with probability 1 if there is no eavesdropper.

2. an L-type measurement on a photon, which is actually in the superposition state $|L_{n+2}\rangle + |L_n\rangle$. She will detect one of the two eigenstates L_n, L_{n+2}, with probability $\frac{1}{2}$, respectively. Eve may send a copy of it to Alice. If Alice receives one of these eigenstates and makes a D-type measurement, she will obtain one of the superpositions $|L_{n+2}\rangle + |L_n\rangle$ or $|L_{n+2}\rangle + |L_{n+4}\rangle$ or $|L_n\rangle + |L_{n-2}\rangle$, with respective probabilities of $\frac{1}{4}$, $\frac{1}{2}$, $\frac{1}{4}$. However, she should only obtain $|L_{n+2}\rangle + |L_n\rangle$ with probability 1 if there is no eavesdropper.

In both cases, when Alice compares her results with Bob's, Alice and Bob will find that their outcomes are inconsistent a fraction f of the time, where

$$\begin{aligned} f &= (fraction\ of\ times\ Eve\ interferes) \\ &\quad \times (fraction\ of\ times\ Eve\ guesses\ wrong\ basis) \\ &\quad \times (fraction\ of\ times\ wrong\ basis\ leads\ to\ error) \\ &= \eta \times \frac{1}{2} \times \frac{1}{2} \\ &= \frac{\eta}{4} \end{aligned} \tag{3.6}$$

which is exactly the same as that for the Simon *et al.* protocol.

3.2.6 Exchange of classical messages

As discussed in 3.2.4, the protocol needs to exchange the classical information to let Alice and Bob know each other's chosen sorters and their detected values, and the values k and m for key generation. Meanwhile, this must be done in such a way that the Eve cannot do much better than to randomly guess the encoding packets even if she obtains the exchanged classical information. Fortunately, we can use the idea of combining the locking of classical information [106] and fountain codes [84] with privacy amplification [107] to achieve it.

On one hand, Guha *et al.* [108] state that the cryptographic applications of classical information locking in quantum key distribution are applicable if the distribution of the message is completely random from the perspective of the adversary. In our protocol, the degrees and positions are used for letting Alice and Bob know the each other's chosen sorters, and the type of the entangled states and the values k and m in our protocol are chosen completely randomly. On the other hand, our method actually is also privacy amplification [107]. Hence, a pre-shared sequence with a small number of bits is sufficient for encrypting a long message in quantum cryptography. This is because the method of privacy amplification [107] can be used where in case Eve may have some information about the key, a shorter key is extracted so that Eve has little information about the new key. These imply that the method that we use to obtain the information for knowing the chosen sorters and detected OAM value by Alice and Bob and k and m is secure.

This is because with the way to prepare exchanged classical messages, Alice just randomly chooses the degrees and positions of the source files and sends them to Bob via an authenticated classical channel without transmitting the encoding packets (see Figure 2.1). That is, without the shared source files, Eve cannot obtain any useful information about the values k_αs and m_αs, where $k_\alpha, m_\alpha \geq 2$, $\alpha = 1, 2, \cdots, n$. Moreover, for every entangled photon, the corresponding k_α and m_α (i.e., the degrees and positions of the

source files) are always updated. To obtain the information on k_αs and m_αs, Eve can guess the shared source files with maximum probability $\frac{1}{2^{200}}$, which is negligible. Eve can also guess $k_1, k_2, \cdots, k_n$ and $m_1, m_2, \cdots, m_n$. The chance to obtain all the values k_αs and m_αs is $\frac{1}{k_1 \times m_1 \times \cdots \times k_n \times m_n}$. The chance is also negligible, even if n is small, say 50, because $k_\alpha,\ m_\alpha \geq 2,\ \alpha = 1, 2, \cdots, n$. Likewise, for the each other's chosen sorters, and the type of the entangled states, the Eve can guess them with probabilities of $\frac{1}{2}$, $\frac{1}{4}$ respectively without the shared source files.

Most importantly, the m_αs which are also obtained with the degrees and positions of the source files can be chosen flexibly in terms of the quality of the quantum channel. To be exact, if the use of l values can lead to extremely low error rates, the values m_αs can be large, otherwise, they should be small.

We remark that our protocol is a modification of the Simon *et al.* protocol with Fibonacci numbers replaced with Lucas numbers, aiming at extending the performance of the protocol, i.e., achieving the consecutive and flexible key expansion using the close relationship between Chebyshev-map values and Lucas numbers.

3.2.7 Features of our proposed protocol

Though we just replace the Fibonacci numbers in the Simon *et al.* protocol with Lucas numbers, the following six features can be obtained because of the relationship among Chebyshev maps, k-Chebyshev maps and Lucas numbers observed.

1. **Key expansion property.** The most significant improvement of our modified protocol based on Simon *et al.*'s protocol lies in the key expansion. In Simon *et al.*'s protocol, the information capacity can be doubled by using positive and negative Fibonacci OAM values. By contrast, since Chebyshev-map values that correspond to Lucas numbers are used, it is followed by the key expansion using k-Chebyshev maps. That is, not only can our proposed protocol double with positive and negative

Lucas OAM values or even multiply the information capacity per photon, but also much fewer OAM values are needed. This is because the information capacity of a photon in our protocol can be increased from $\log_2 N$ to $(\log_2 N + m \log_2 m)$. In other words, our protocol has the key expansion property, which plays a key role in reducing the number of particles that are used for preparing entangled particles. As a result, the key expansion property allows to achieve secure generation of long keys from much fewer photons.

2. **Lower-dimensional high-capacity property.** Due to the key expansion property, our protocol can achieve lower-dimensional high-capacity with larger value m and fewer Lucas values used.

3. **The flexible key expansion.** Due to the coding rules used in our proposed protocol, the value m can be chosen flexibly, making the flexible key expansion possible.

4. **Selective property.** Due to the key expansion property, some consecutive and proper Lucas values can be chosen to encode entangled states in our proposed protocol. This achieves both the longer distances and lower error rates simultaneously.

5. **Less turbulence and measurement errors.** In our protocol, the type of OAM entangled two-photon source in Simon *et al.*'s protocol also works, so, the analysis on the effects from turbulence and measurement errors in Simon *et al.*'s protocol also holds, i.e., though the use of high-l values can contribute to extremely low error rates, the transmitted distances is short, while lower values of l can travel longer distances but error rates are higher. However, due to the above "selective property", it is possible to choose proper Lucas values to lessen turbulence and measurement errors (that is, to travel longer distances with smaller error rates) under the same conditions.

6. **No limit of spiral and OAM bandwidths.** In our proposed protocol, the key expansion property allows to achieve secure generation of long keys from much fewer photons just by choosing a larger positive integer m, avoiding the addition of more detectors and beam splitters and images superimposed on a hologram in Simon *et al.*'s protocol [22]. Hence, there is no limit of spiral and OAM bandwidths for enhancing the information capacity in our protocol, which in turn makes our protocol more practical.

3.3 High-capacity QKD against a collective noise

In this section, we consider two QKD protocols with the advantages referred to in [40–48] (that is implementable and efficient), mainly using the 2-extended unitary operations based on a collective-dephasing noise to improve Li *et al.*'s protocol [45] with the aim of increasing the qubit efficiency while at the same time reducing the number of Bell measurements. We first review Li et al's protocol and then propose our improved protocol.

3.3.1 Unitary operations based on a collective-dephasing noise

Next, we introduce some basic definitions for the extended unitary operations based on collective-dephasing noise. These definitions are from [45].

Definition 1. An entangled state based on a collective-dephasing noise [45].

$$|\Phi^{\pm}\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0_L\rangle_B \pm |1\rangle_A|1_L\rangle_B), |\Psi^{\pm}\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1_L\rangle_B \pm |1\rangle_A|0_L\rangle_B). \quad (3.7)$$

Note that the subscript L means the logical qubit, consisting of a few physical qubits, which are subjected to the same noise. Since these physical qubits have a certain relationship between them, the constructed logical qubits are free from the effect of noise as well.

Definition 2. A collective-dephasing noise [45]. A collective-dephasing noise can be described as

$$U_{dp}|0\rangle = |0\rangle, U_{dp}|1\rangle = e^{i\phi}|0\rangle. \tag{3.8}$$

where ϕ is the noise parameter which varies with time.

A logical qubit made of two physical qubits with antiparallel parity will have the same phase factor $e^{i\phi}$, and it is therefore free from collective-dephasing noise [45]. The two physical qubits are given as follows:

$$|0_L\rangle = |01\rangle, |1_L\rangle = |10\rangle. \tag{3.9}$$

Definition 3. Four entangled logical states for a collective-dephasing noise [45].

$$\begin{aligned} |\Phi_{dp}^{\pm}\rangle_{AB_1B_2} &= \frac{1}{\sqrt{2}}(|0\rangle_A|01\rangle_{B_1B_2} \pm |1\rangle_A|10\rangle_{B_1B_2}), \\ |\Psi_{dp}^{\pm}\rangle_{AB_1B_2} &= \frac{1}{\sqrt{2}}(|0\rangle_A|10\rangle_{B_1B_2} \pm |1\rangle_A|01\rangle_{B_1B_2}). \end{aligned} \tag{3.10}$$

where the logical qubit B consists of two physical qubits B_1 and B_2. They are such GHZ states used in [45] and our protocol.

Definition 4. Four unitary operations for a collective-dephasing noise [45].

$$\begin{aligned} &\Omega_{00} = \Omega_I = I_1 \otimes I_2, \Omega_{01} = \Omega_z = U_{z1} \otimes I_2, \\ &\Omega_{10} = \Omega_x = U_{x1} \otimes U_{x2}, \Omega_{11} = \Omega_y = U_{y1} \otimes U_{x2}. \end{aligned} \tag{3.11}$$

where the subscript 1 denotes that the photon B_1 is encoded using the unitary operation. So does the meaning of subscript 2.

Moreover, when the four unitary operations over a collective-dephasing noise are used

to transform one of the states $\{|\Phi_{dp}^{\pm}\rangle, |\Psi_{dp}^{\pm}\rangle\}$, the following results can be obtained [45].

$$\begin{aligned}
&\Omega_{00}|\Phi_{dp}^{+}\rangle = |\Phi_{dp}^{+}\rangle, \Omega_{01}|\Phi_{dp}^{+}\rangle = |\Phi_{dp}^{-}\rangle, \Omega_{10}|\Phi_{dp}^{+}\rangle = |\Psi_{dp}^{+}\rangle, \Omega_{11}|\Phi_{dp}^{+}\rangle = |\Psi_{dp}^{-}\rangle.\\
&\Omega_{00}|\Phi_{dp}^{-}\rangle = |\Phi_{dp}^{-}\rangle, \Omega_{01}|\Phi_{dp}^{-}\rangle = |\Phi_{dp}^{+}\rangle, \Omega_{10}|\Phi_{dp}^{-}\rangle = |\Psi_{dp}^{-}\rangle, \Omega_{11}|\Phi_{dp}^{-}\rangle = |\Psi_{dp}^{+}\rangle.\\
&\Omega_{00}|\Psi_{dp}^{+}\rangle = |\Psi_{dp}^{+}\rangle, \Omega_{01}|\Psi_{dp}^{+}\rangle = |\Psi_{dp}^{-}\rangle, \Omega_{10}|\Psi_{dp}^{+}\rangle = |\Phi_{dp}^{+}\rangle\Omega_{11}|\Psi_{dp}^{+}\rangle = |\Phi_{dp}^{-}\rangle.\\
&\Omega_{00}|\Psi_{dp}^{-}\rangle = |\Psi_{dp}^{-}\rangle, \Omega_{01}|\Psi_{dp}^{-}\rangle = |\Psi_{dp}^{+}\rangle, \Omega_{10}|\Psi_{dp}^{-}\rangle = |\Phi_{dp}^{-}\rangle, \Omega_{11}|\Psi_{dp}^{-}\rangle = |\Phi_{dp}^{+}\rangle.
\end{aligned} \tag{3.12}$$

3.3.2 2−extended unitary operations based on a collective-dephasing noise

We construct 2−extended unitary operations in a general way where each operation is the result of the tensor product of two unitary operations, defined as follows:

$$\begin{aligned}
&\Omega_{0000} = \Omega_{00} \otimes \Omega_{00}, \Omega_{0001} = \Omega_{00} \otimes \Omega_{01}, \Omega_{0010} = \Omega_{00} \otimes \Omega_{10}, \Omega_{0011} = \Omega_{00} \otimes \Omega_{11},\\
&\Omega_{0100} = \Omega_{01} \otimes \Omega_{00}, \Omega_{0101} = \Omega_{01} \otimes \Omega_{01}, \Omega_{0110} = \Omega_{01} \otimes \Omega_{10}, \Omega_{0111} = \Omega_{01} \otimes \Omega_{11},\\
&\Omega_{1000} = \Omega_{10} \otimes \Omega_{00}, \Omega_{1001} = \Omega_{10} \otimes \Omega_{01}, \Omega_{1010} = \Omega_{10} \otimes \Omega_{10}, \Omega_{1011} = \Omega_{10} \otimes \Omega_{11},\\
&\Omega_{1100} = \Omega_{11} \otimes \Omega_{00}, \Omega_{1101} = \Omega_{11} \otimes \Omega_{01}, \Omega_{1110} = \Omega_{11} \otimes \Omega_{10}, \Omega_{1111} = \Omega_{11} \otimes \Omega_{11}.
\end{aligned} \tag{3.13}$$

The 2−extended unitary operations can be used to transform one of the states $\{|\Phi_{dp}^{\pm}\rangle, |\Psi_{dp}^{\pm}\rangle\}$ into any $\{|\Phi_{dp}^{\pm}\rangle, |\Psi_{dp}^{\pm}\rangle\}$ as follows:

$$\begin{aligned}
&\Omega_{0000}|\Phi_{dp}^{+}\rangle = \Omega_{0101}|\Phi_{dp}^{+}\rangle = \Omega_{1010}|\Phi_{dp}^{+}\rangle = \Omega_{1111}|\Phi_{dp}^{+}\rangle = \Omega_{00}|\Phi_{dp}^{+}\rangle = |\Phi_{dp}^{+}\rangle\\
&\Omega_{0001}|\Phi_{dp}^{+}\rangle = \Omega_{0100}|\Phi_{dp}^{+}\rangle = \Omega_{1011}|\Phi_{dp}^{+}\rangle = \Omega_{1110}|\Phi_{dp}^{+}\rangle = \Omega_{01}|\Phi_{dp}^{-}\rangle = |\Phi_{dp}^{-}\rangle,\\
&\Omega_{0010}|\Phi_{dp}^{+}\rangle = \Omega_{0111}|\Phi_{dp}^{+}\rangle = \Omega_{1000}|\Phi_{dp}^{+}\rangle = \Omega_{1101}|\Phi_{dp}^{+}\rangle = \Omega_{10}|\Phi_{dp}^{+}\rangle = |\Psi_{dp}^{+}\rangle,\\
&\Omega_{0011}|\Phi_{dp}^{+}\rangle = \Omega_{0110}|\Phi_{dp}^{+}\rangle = \Omega_{1001}|\Phi_{dp}^{+}\rangle = \Omega_{1100}|\Phi_{dp}^{+}\rangle = \Omega_{11}|\Phi_{dp}^{+}\rangle = |\Psi_{dp}^{-}\rangle.
\end{aligned} \tag{3.14}$$

And they are abbreviated as follows:

$$\begin{aligned}
\Omega_{0000} = \Omega_{0101} = \Omega_{1010} = \Omega_{1111} = \Omega_{00},\\
\Omega_{0001} = \Omega_{0100} = \Omega_{1011} = \Omega_{1110} = \Omega_{01},\\
\Omega_{0010} = \Omega_{0111} = \Omega_{1000} = \Omega_{1101} = \Omega_{10},\\
\Omega_{0011} = \Omega_{0110} = \Omega_{1001} = \Omega_{1100} = \Omega_{11}.
\end{aligned} \tag{3.15}$$

Definition 5. Transition operations and ultimate operations based on a collective-dephasing noise. If $\Omega_{b_{i_1}b_{i_2}b_{i_3}b_{i_4}}(w) = \Omega_{b_{j_1}b_{j_2}}(w), w \in \{|\Phi_{dp}^{\pm}\rangle, |\Psi_{dp}^{\pm}\rangle\}$, where $b_{i_1}b_{i_2}b_{i_3}b_{i_4}$ and $b_{j_1}b_{j_2}$ represent any two sequences of 4− and 2−bit values respectively, then $\Omega_{b_{j_1}b_{j_2}}$ is called the transition operation of $\Omega_{b_{i_1}b_{i_2}b_{i_3}b_{i_4}}$. Meanwhile, $\Omega_{b_{i_1}b_{i_2}b_{i_3}b_{i_4}}$ is called the ultimate operation of $\Omega_{b_{j_1}b_{j_2}}$.

For example, according to Definition 5, for 2−extended unitary operations, Ω_{00} is the transition operation of ultimate operation Ω_{0000}, and Ω_{0000} is the ultimate operation of transition operation Ω_{00}.

Definition 6. Control bits based on a collective-dephasing noise. For given 2−extended unitary operations, when all the four 2−extended unitary operations are used to transform an identical state which is in $\{|\Phi_{dp}^{\pm}\rangle, |\Psi_{dp}^{\pm}\rangle\}$, there are four 2−extended unitary operations having the same outcomes. The four 2−extended unitary operations are listed with matching sequence numbers that are denoted by the bit values. The bit values are called the control bits.

Then Table 3.1 can be obtained in terms of (3.15) and Definitions 5 and 6.

Definition 7. Corresponding classical bits based on a collective-dephasing noise. The bit values obtained by applying XOR to the bit values from the subscript of the transition operation and the control bits are called the corresponding classical bits.

Table 3.1: Collation table based on a collective-dephasing noise for $n = 2$.

	Control bits			
BΩO	00	01	10	11
Ω_{00}	Ω_{0000}	Ω_{0101}	Ω_{1010}	Ω_{1111}
Ω_{01}	Ω_{0001}	Ω_{0100}	Ω_{1011}	Ω_{1110}
Ω_{10}	Ω_{0010}	Ω_{0111}	Ω_{1000}	Ω_{1101}
Ω_{11}	Ω_{0011}	Ω_{0110}	Ω_{1001}	Ω_{1100}

BΩO denotes basic unitary operation based on a collective-dephasing noise.

3.3.3 2−extended unitary operations based on a collective-rotation noise

Definition 8. A collective-rotation noise [45].

$$U_r|0\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle, U_r|1\rangle = -\sin\theta|0\rangle + \cos\theta|1\rangle. \tag{3.16}$$

where the parameter θ is determined by the noise and time together. As above, with such collective-rotation noise, $|\phi^+\rangle$ and $|\psi^-\rangle$ are free from the effect of noise. Logical qubits can be chosen as

$$|0_L\rangle = |\phi^+\rangle, |1_L\rangle = |\psi^-\rangle. \tag{3.17}$$

Definition 9. An entangled state based on a collective-rotation noise [45].

$$\begin{aligned} |\Phi_r^{\pm}\rangle_{AB_1B_2} &= \frac{1}{\sqrt{2}}(|0\rangle_A|\phi^+\rangle_{B_1B_2} \pm |1\rangle_A|\psi^-\rangle_{B_1B_2}), \\ |\Psi_r^{\pm}\rangle_{AB_1B_2} &= \frac{1}{\sqrt{2}}(|0\rangle_A|\psi^-\rangle_{B_1B_2} \pm |1\rangle_A|\phi^+\rangle_{B_1B_2}). \end{aligned} \tag{3.18}$$

Definition 10. Four unitary operations for a collective-rotation noise [45].

The four unitary operations $\{\Theta_{00}, \Theta_{01}, \Theta_{10}, \Theta_{11}\}$ over a collective-rotation noise can be written as

$$\begin{aligned} &\Theta_{00} = \Theta_I = I_1 \otimes I_2, \Theta_{01} = \Theta_z = U_{z1} \otimes I_{z2}, \\ &\Theta_{10} = \Theta_x = U_{z1} \otimes U_{x2}, \Theta_{11} = \Theta_y = I_1 \otimes U_{y2}. \end{aligned} \tag{3.19}$$

The four unitary operations can be used to transform one of the states $\{|\Phi_r^{\pm}\rangle, |\Psi_r^{\pm}\rangle\}$ into any $\{|\Phi_r^{\pm}\rangle, |\Psi_r^{\pm}\rangle\}$ as follows [45]:

$$\begin{aligned} &\Theta_{00}|\Phi_r^+\rangle = |\Phi_r^+\rangle, \Theta_{01}|\Phi_r^+\rangle = |\Phi_r^-\rangle, \Theta_{10}|\Phi_r^+\rangle = |\Psi_r^+\rangle, \Theta_{11}|\Phi_r^+\rangle = |\Psi_r^-\rangle. \\ &\Theta_{00}|\Phi_r^-\rangle = |\Phi_r^-\rangle, \Theta_{01}|\Phi_r^-\rangle = |\Phi_r^+\rangle, \Theta_{10}|\Phi_r^-\rangle = |\Psi_r^-\rangle, \Theta_{11}|\Phi_r^-\rangle = |\Psi_r^+\rangle. \\ &\Theta_{00}|\Psi_r^+\rangle = |\Phi_r^+\rangle, \Theta_{01}|\Psi_r^+\rangle = |\Phi_r^-\rangle, \Theta_{10}|\Psi_r^+\rangle = |\Phi_r^+\rangle, \Theta_{11}|\Psi_r^+\rangle = |\Phi_r^-\rangle. \\ &\Theta_{00}|\Psi_r^-\rangle = |\Psi_r^-\rangle, \Theta_{01}|\Psi_r^-\rangle = |\Psi_r^+\rangle, \Theta_{10}|\Psi_r^-\rangle = |\Phi_r^-\rangle, \Theta_{11}|\Psi_r^-\rangle = |\Phi_r^+\rangle. \end{aligned} \tag{3.20}$$

The 2−extended unitary operations based on a collective-rotation noise can be constructed in the same way as in (3.13) and the similar outcomes can be obtained.

3.3.4 Review of Li *et al.*'s protocol

In this subsection, we give a brief review of Li *et al.*'s protocol, together with the main steps as follows:

Step 3.3.4.1. Alice first prepares a sufficient number of entangled states based on a collective-dephasing noise, which are in $|\Phi_{dp}^+\rangle_{AB_1B_2} = \frac{1}{\sqrt{2}}(|0\rangle_A|01\rangle_{B_1B_2} + |1\rangle_A|10\rangle_{B_1B_2})$. Then she divides these entangled states into two photon sequences, S_A and S_B, where S_A is made up of all the logical qubits A and S_B all the logical qubits B with physical qubits B_1 and B_2.

Step 3.3.4.2. Then Alice keeps the sequence S_A and transmits the sequence S_B to Bob.

Step 3.3.4.3. After Bob receives the sequence S_B, he first analyzes the error rate by choosing some of the logical qubits S_B randomly. And the remaining logical qubits constitute the message sequence S_{BM} for key generation. Bob measures each logical qubit in the sample by using either the base $\sigma_z^B \equiv \sigma_z^{B_1} \otimes \sigma_z^{B_2}$ or the base $\sigma_x^B \equiv \sigma_x^{B_1} \otimes \sigma_x^{B_2}$. Moreover, Bob informs Alice about the chosen samples from the logical qubits. Through performing the two bases, the entangled states prepared by Alice can be transformed as

$$\begin{aligned} |\Phi_{dp}^{+}\rangle_{AB_1B_2} &= \frac{1}{\sqrt{2}}(|0\rangle_A|01\rangle_{B_1B_2} \pm |1\rangle_A|10\rangle_{B_1B_2}) \\ &= \frac{1}{\sqrt{2}}[|+\rangle_A(|++\rangle - |--\rangle)_{B_1B_2} + |-\rangle_A(|-+\rangle - |+-\rangle)_{B_1B_2}] \end{aligned} \tag{3.21}$$

If the outcomes obtained by Alice and Bob satisfy the equations when the same bases are chosen for their logical qubits, then there are no eavesdroppers, and they continue to the next step. Otherwise, they abort this operation.

Step 3.3.4.4. After confirming that the quantum channel is secure, Bob encodes each logical qubit from S_{BM} with any of the following unitary operations $\{\Omega_{00}, \Omega_{01}, \Omega_{10}, \Omega_{11}\}$. The subscripts of Ω denote the codes $\{00, 01, 10, 11\}$. The states operated by Bob are also free from the effect of noise when they are transmitted to Alice through a quantum channel with the collective-dephasing noise. After performing the unitary operations, Bob sends the encoded sequence S'_{BM} to Alice over a collective-dephasing noise channel.

Step 3.3.4.5. Alice chooses each entangled state based on a collective-dephasing noise from the two-photon sequences S'_{BM} and S_{AM} (S_{AM} consists of the logical qubits corresponding to the logical qubits in S_{BM}). For the two photons AB_1, Alice performs a Bell-state measurement on them. For the photon B_2 with $X = \sigma_x$ basis, Alice performs a single-photon measurement on it. By doing so, the states $|\Phi_{dp}^{\pm}\rangle_{AB_1B_2}$ and $|\Psi_{dp}^{\pm}\rangle_{AB_1B_2}$ can be discriminated, which are denoted as follows:

$$\begin{aligned} |\Phi_{dp}^{\pm}\rangle_{AB_1B_2} &= \frac{1}{\sqrt{2}}(|\phi^{\pm}\rangle_{AB_1} \otimes |+\rangle_{B_2} - |\phi^{\mp}\rangle_{AB_1} \otimes |-\rangle_{B_2}), \\ |\Psi_{dp}^{\pm}\rangle_{AB_1B_2} &= \frac{1}{\sqrt{2}}(|\psi^{\pm}\rangle_{AB_1} \otimes |+\rangle_{B_2} - |\psi^{\mp}\rangle_{AB_1} \otimes |-\rangle_{B_2}). \end{aligned} \tag{3.22}$$

Where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ are two eigenvectors of Pauli operator σ_x. It can be easily seen that, from (3.10), Alice can distinguish the four three-photon GHZ states and determine the operations performed by Bob on the logical qubits B with these two measurement outcomes.

Step 3.3.4.6. Alice can check the security of the transmission from Bob by error rate analysis by choosing a subset from the measured outcomes on the three-qubit states operated on by Bob and asking Bob to tell her his operation on the chosen subset. If the error rate is within a preset value, she tells Bob that their quantum communication is secure; otherwise, they abort the operation and repeat the QKD from the beginning.

Step 3.3.4.7. If the quantum channel is secure, Alice is able to obtain the key with the classical error correction codes and message authentication codes [8].

3.3.5 High-capacity QKD against a collective-dephasing noise

The steps in our improved protocol are similar to those in Li et al.'s protocol [45] but with several critical differences. Our improved quantum key distribution protocol against a collective-dephasing noise is based on 2−extended unitary operations which can be seen in Figure 3.3. Another critical difference between our improved protocol and that of Li *et al.* [45], is that Bob prepares the entangled states and initiates the protocol rather than Alice. For the sake of the completeness of the thesis, we describe the steps for our improved protocol as follows:

Step 3.3.5.1. Bob prepares n entangled states over a collective-dephasing noise, which are in $|\Phi_{dp}^{+}\rangle_{AB_1B_2} = \frac{1}{\sqrt{2}}(|0\rangle_A|01\rangle_{B_1B_2} + |1\rangle_A|10\rangle_{B_1B_2})$. All of the 1st particles of n entangled states are to form an ordered photon sequence S_A and all of the 2nd and 3rd particles of n entangled states are to form an ordered photon sequence S_B.

Step 3.3.5.2. Then Bob keeps the sequence S_A and transmits the sequence S_B to Alice.

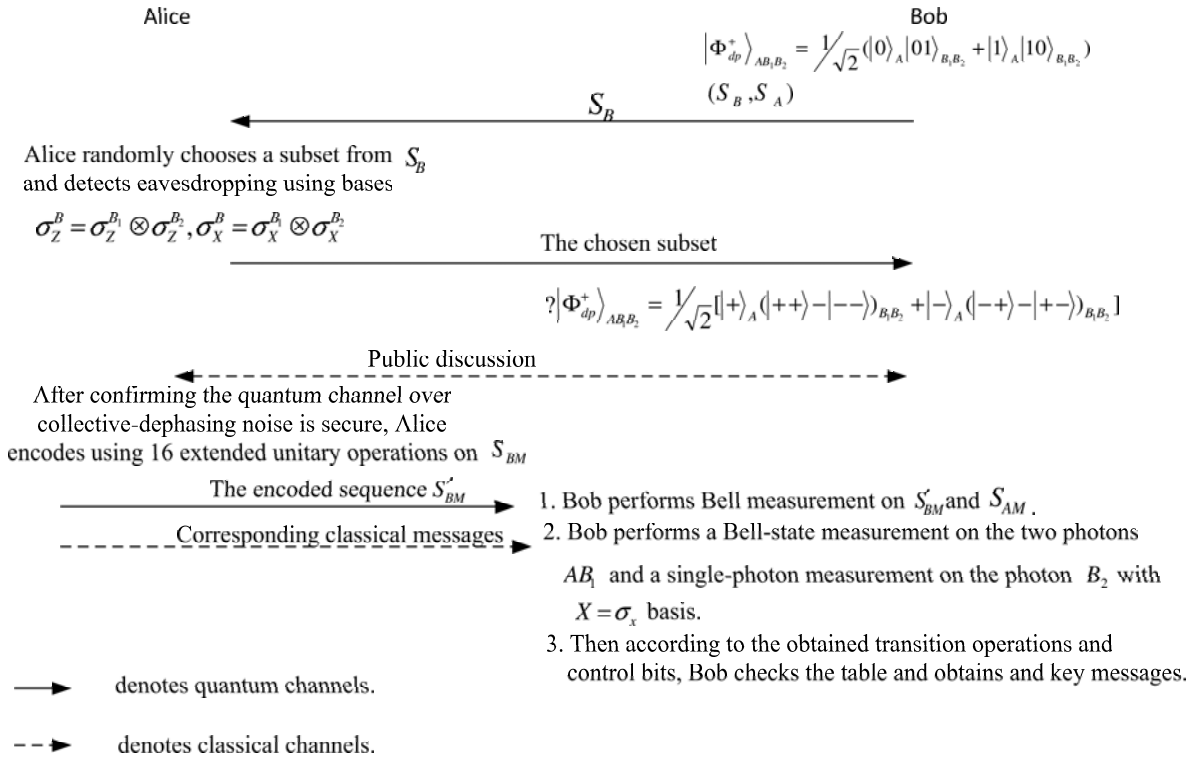

Figure 3.3: The process of the proposed protocol I.

Step 3.3.5.3. When Alice receives the sequence S_B, she chooses a subset S'_B of photons from S_B at random, which are used for analyzing the error rate, and $S_{BM} = S_B/S'_B$ for message sequence for producing the key. The rest of the step is similar to that in Step 3.3.4.3. Note that here, Alice should be replaced by Bob, and vice versa.

Step 3.3.5.4. After confirming that there are no eavesdroppers, Alice encodes each logical qubit from the message sequence S_{BM}, with one of the sixteen unitary operations $\{\Omega_{0000}, \Omega_{0001}, \Omega_{0010}, \Omega_{0011}, \cdots, \Omega_{1100}, \Omega_{1101}, \Omega_{1110}, \Omega_{1111}\}$. The subscripts of Ω denote the codes $\{0000, 0001, 0010, 0011, \cdots, 1100, 1101, 1110, 1111\}$. The obtained states after applying the sixteen unitary operations are still free from the effect of noise. After the extended unitary operations are performed on S_{BM}, Alice transmits the encoded sequence S'_{BM} and the corresponding classical bits to Bob over a quantum channel against collective-dephasing noise and a classical channel respectively.

Step 3.3.5.5. Bob chooses each entangled state for collective-dephasing noise from the two-photon sequences S'_{BM} and S_{AM} (S_{AM} consists of the logical qubits which correspond to the logical qubits in S_{BM}). The rest of the step is similar to that in Step 3.3.4.5. Note that here, Alice should be replaced by Bob, and vice versa.

For example, if Bob obtains the transition operation Ω_{11}, which represents 11, he can figure out the control bits 10 by applying 11 XOR 01 that are the corresponding classical bits. Finally, Bob deduces the ultimate operation Ω_{1001} (that is, the key message 1001) using the control bits 10 and Ω_{11} in terms of Table 3.1.

Step 3.3.5.6. Bob can check the security of the second transmission (from Alice to Bob) in the similar way as in Step 3.3.4.3. He can choose any subset of the outcomes of Alice's measurements on three-qubit states for analyzing the error rate. He can detect eavesdropping of the second transmission by himself as long as Alice informs him about her corresponding operation on the particle in his chosen subset. If the error rate is within a preset value, he tells Alice that their quantum communication is secure. Otherwise, they will abort this operation and start from the beginning.

Step 3.3.5.7. This step is similar to Step 3.3.4.7. But Alice should be replaced by Bob.

3.3.6 High-capacity QKD against a collective-rotation noise

Similar to Li *et al.*'s protocol with a collective-rotation noise, a high-capacity quantum key distribution against a collective-rotation noise can be obtained with the similar changes on the protocol presented in Section 3.3.5. There are main two differences, which are as follows:

1. The four states $\{|\Phi^{\pm}_{dp}\rangle_{AB_1B_2}, |\Psi^{\pm}_{dp}\rangle_{AB_1B_2}\}$ are replaced with $\{|\Phi^{\pm}_{r}\rangle_{AB_1B_2}, |\Psi^{\pm}_{r}\rangle_{AB_1B_2}\}$.

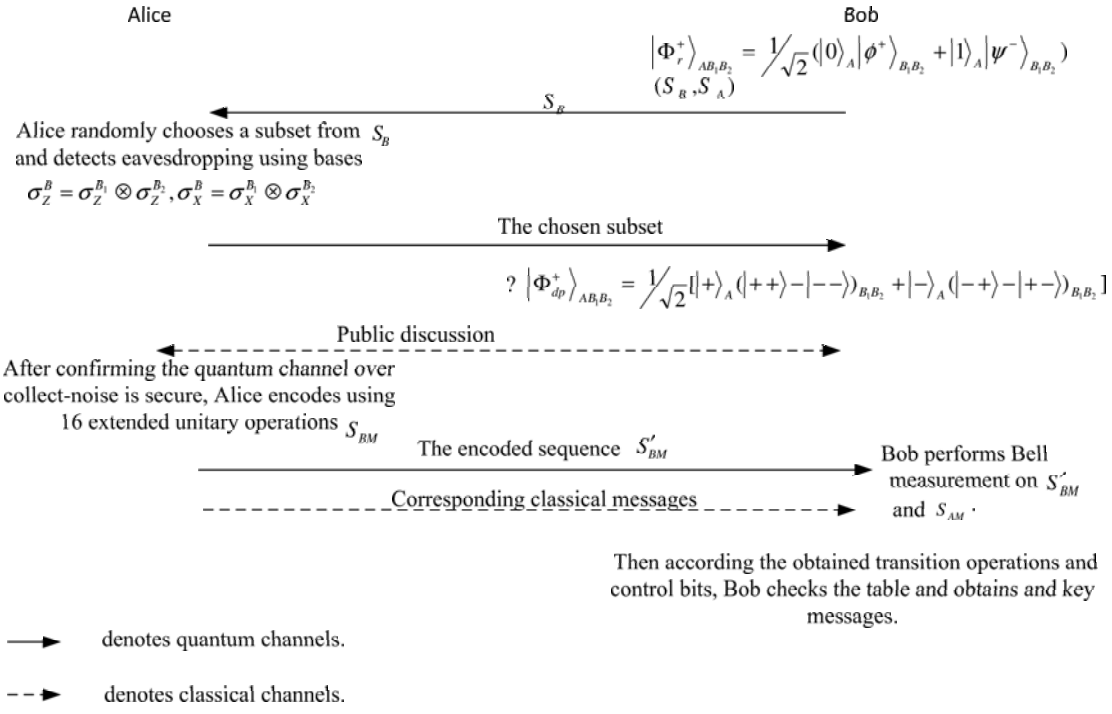

Figure 3.4: The process of the proposed protocol II.

2. Unlike Steps 3.3.5.5 and 3.3.5.6, before Alice takes a Bell-state measurement on B_1 and A and a single-photon measurement on the photon B_2, a Hadamard operation is first performed on B_1 as follows.

$$|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{3.23}$$

Moreover, the four GHZ states based on a collective-rotation noise can be transformed into (3.11) after performing the Hadamard operation.

$$\begin{aligned} |\Phi_r^{\pm}\rangle_{AB_1B_2} &= \frac{1}{\sqrt{2}}(|\phi^+\rangle_{AB_1} \otimes |+\rangle_{B_2} \pm |\psi^-\rangle_{AB_1} \otimes |-\rangle_{B_2}), \\ |\Psi_r^{\pm}\rangle_{AB_1B_2} &= \frac{1}{\sqrt{2}}(|\psi^-\rangle_{AB_1} \otimes |+\rangle_{B_2} \pm |\phi^+\rangle_{AB_1} \otimes |-\rangle_{B_2}). \end{aligned} \tag{3.24}$$

The setup of our improved high-capacity quantum key distribution against a collective-rotation noise is given in Figure 3.4.

3.3.7 Security and performance analysis

Security analysis

We mainly use the 2-extended unitary operations based on collective noise to improve the protocols of Li *et al.* [45], aiming at increasing the qubit efficiency and reducing the times of Bell measurement to half. The key techniques used in our proposed protocol are the same as those in [18]. The security of the protocols proposed by Li *et al.* [45] therefore carries over to our proposed protocols. The detailed security analysis is given in [45].

Performance analysis

In this section, we compare the performance of our proposed protocols with those of other proposed protocols. Table 3.2 compares traditional fault tolerant QKDs and our proposed protocol, using several important features such as the type of entanglement used, the direction of quantum communication, the qubit efficiency and the number of Bell measurements. The first column in the table refers to the considered fault-tolerant QKD protocols [40–46].

On the one hand, in the protocols in [40, 41, 43, 44, 46], four- and six-photon entanglements are used. Up to now, it is not easy to prepare multi-photon entangled states [49], since it will increase the difficulty of the implementation of such a QKD protocol with the current techniques. However, in our protocols, GHZ states are used, which are easier to implement. Moreover, in Yan and Hwang's protocol [46], $2C$ times of Bell measurements are needed, C times in Li and Li's protocol, $\frac{C}{2}$ times in Li *et al.*'s protocol [45], and only $\frac{C}{4}$ in our proposed protocol. It is worth noting that Bell measurements always present a

technical difficulty [45]. Hence, fewer the number of Bell measurements needed, the more feasible the protocol is.

On the other hand, as it can be easily seen from Table 3.2, four- and six-photon entanglements are not used in [42, 45], but the qubit efficiency of their protocols is very low, at 6.25% and 8.33% respectively. The detailed analysis follows a similar analysis presented in [46].

The qubit efficiency (QE) of a quantum protocol is given by the formula $\eta = \frac{c}{q}$ where c denotes the number of shared classical bits and q the number of generated qubits. In the performance analysis of many protocols, an assumption is made that during the public discussion stage, half of the transmitted qubits are used for checking for eavesdropping , and that half of the transmitted qubits are used for checking for Trojan horse attacks like in [46]. In Boileau *et al.*'s, Li *et al.*'s and Sun *et al.*'s protocols [41–43], each 4-particle state prepared by Alice can just carry one-bit key message. Also, one round of public discussion is needed. Hence, the QE of their protocols is $\frac{n}{4n} \times \frac{1}{2} = \frac{1}{8} = 12.5\%$. Similarly, in Xiu *et al.*'s protocol [42], each 6-particle state can just carry one-bit key message as well and one round of public discussion between Alice and Bob is needed. Hence, the QE of Xiu *et al.*'s protocol is $\frac{2n}{6n} \times \frac{1}{2} = \frac{1}{6} = 16.67\%$. In Li and Li's protocol [42] and Li *et al.*'s protocol [45], Alice generates n Bell states and n GHZ states respectively, and each of them can carry one- and two-bit key messages in Li and Li's QKD. There are two rounds of public discussions, and half of the transmitted qubits are used for checking for Trojan horse attacks. Therefore, the QE of Li and Li's and Li *et al.*'s protocols are $\frac{n}{2n} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} = \frac{1}{16} = 6.25\%$ and $\frac{2n}{3n} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} = \frac{1}{12} = 8.33\%$.

Though the QE of Yan and Hwang's protocol [46] is highest, at $\frac{2n}{6n+4n} = \frac{1}{5} = 20\%$, the times of Bell measurements needed is the most, at $2C$.

In our proposed QKD protocols based on extended unitary operations over a collective-dephasing noise channel, Alice has to generate n GHZ states, and each GHZ state can

Table 3.2: Performance comparison of QKD based on collective noise.

Protocols	4-p state	6-p state	B state	GHZ state	QC	QE	TBM	CB
Li *et al.*'s [40]	Yes	No	No	No	one-way	12.5%	0	0
Boileau *et al.*'s [41]	No	Yes	No	No	one-way	12.5%	0	0
Sun *et al.*'s [43]	No	Yes	No	No	one-way	12.5%	0	0
Xiu *et al.*'s [44]	No	Yes	No	No	one-way	16.67%	0	0
Li and Li's [42]	No	No	Yes	No	two-step	6.25%	C	C
Li *et al.*'s [45]	No	No	No	Yes	two-step	8.33%	$\frac{C}{2}$	0
Yan and Hwang's [46]	No	No	No	Yes	one-way	20%	$2C$	0
Our protocol [50]	No	No	No	Yes	two-step	16.67%	$\frac{C}{4}$	$\frac{C}{4}$

4-p state: 4-particle state; 6-p state: 6-particle state; B state: Bell state; QC: Quantum communication; QE: qubit efficiency; TBM: The times of Bell measurements; CB: Classical bits; C: The total number of classical bits needed.

carry four-bit key message. There are two rounds of public discussions between Alice and Bob, and half of the transmitted qubits are used to check for Trojan horse attacks. Therefore, the QE of our protocol is $\frac{4n}{3n} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} = \frac{1}{6} = 16.67\%$. Hence, based on the QE and the available techniques, our protocol is more feasible.

3.4 Summary

By the use of extended unitary operations from collective noise together with quantum dense coding, it is possible to encode many bits of information onto an entangled state. Based on this idea, we have proposed two fault-tolerant high-capacity QKD protocols over a collective-noise channel. The proposed protocols are not only easier to implement, but also have a higher qubit efficiency. Moreover, we have proposed a lower-dimensional high-capacity QKD protocol with the consecutive and flexible key expansion using Chebyshev

maps, which is a significant additional step added to the previous Fibonacci protocol while taking advantage of Lucas numbers being in close relation to Chebyshev maps. We use the properties of Chebyshev maps corresponding to Lucas numbers to avoid the physical limitation for high-capacity QKD. Moreover, on one hand, our protocol is easy to implement by just using the experimental setup in Simon *et al.*'s protocol. On the other hand, it optimizes Simon *et al.*'s protocol by addressing the limitation of spiral and OAM bandwidths. Moreover, our coding rules are not complicated, and the used Lucas values can be chosen to encode signal entangled states in our proposed protocol. This achieves both longer distances and lower error rates simultaneously.

Chapter 4

Quantum secret sharing protocols of secure direct communication

In this chapter, we consider quantum secret sharing, particularly, quantum secret sharing of secure direct communication. We first prove that the simplest nontrivial case, namely, a (2,3) discrete variable threshold quantum secret sharing protocol of secure direct communication can also be achieved using the same devices as in BB84. Then, generalized (n, n) quantum direct secret sharing based on distributed fountain codes is presented.

4.1 Introduction

Recently, a new concept, namely, quantum secure direct communication (QSDC) was proposed by Beige *et al.* [79]. QSDC aims at transmitting secret messages directly instead of first establishing a key to encrypt them. Moreover, *Boström* and Felbinger [18] and Deng *et al.* [109] have already shown that QSDC can be used in some particular settings. Since their seminal work [18,109], a growing number of researchers have been interested in QSDC, and relative improvements and analysis of QSDC [110–114] have been proposed.

In 2005, Zhang [78] generalized the work in [18, 110] into the quantum secret sharing

regime, and proposed a new concept, i.e, quantum secret sharing of secure direct communication. Thereafter, Wang *et al.* [115] generalized Zhang's idea to the high-dimensional case via quantum super-dense coding. Unlike these protocols [110, 115] using entanglement, Han *et al.* [116] proposed a multiparty quantum secret sharing of secure direct communication using single photons. They applied the random phase shift operations (RPSOs) to achieve the sharing controls, aiming at enhancing the security. Nonetheless, owing to the effect of the RPSOs, their proposed protocol requires a quantum memory to store the resulting states so that the participants are able to recover the shared secret. To address this issue, Du *et al.* [117] presented a quantum secret sharing of secure direct communication using one-time pad without the use of quantum memory.

Moreover, Li *et al.* [118] generalized Zhang's protocol and proposed a (t, n) threshold QSS-SDC protocol, in which any t or more participants can recover a secret. However, in Li *et al.*'s protocol, t must be determined in advance rather than arbitrary t, and Cleve *et al.* [17] pointed out it is hard to implement (t, n) threshold quantum state sharing, even the simplest (2,3) threshold quantum state sharing protocol. This is because it depends on having three qutrits available and the capability of universal transformations on these qutrits while qubits and higher order qudits are hard to create and manipulate. However, Tyc and Sanders [80] have shown it is feasible to achieve the (2,3) threshold quantum state sharing with continuous variables. In 2002, Lance *et al.* [81] extended their protocol by utilizing an electro-optic feedforward technique and gave two further protocols. For their first protocol, a pair of optically entangled beams and two phase sensitive amplifiers are used for the reconstruction of the secret state, while a pair of optically entangled beams and an additional electro-optic feedforward loop are used in the second protocol.

In this chapter, with the help of distributed fountain codes, we propose a discrete variable (2,3) threshold quantum secret sharing protocol for secure direct communication and then a generalized (n, n) quantum direct secret sharing protocol [119] with the same

security as those proposed in [3]. The fountain codes can be generated on-line, the number of the used source symbols can be quite small, the way of encoding with the source symbols is very simple, and encoding symbols are generated as few or as many as needed. Due to the randomness and flexibility of control codes, our protocols can be implemented in a simpler and more effective way. In (2,3) threshold quantum secret sharing protocol every particle can on average carry up to 1.5-bit messages and the participants can detect eavesdropping by themselves without exchanging classical information. In the generalized (n, n) quantum direct secret sharing protocol, the idea of producing fountain codes has been applied to produce control codes and the positions of the inserted nonorthogonal state particles, aiming at achieving eavesdropping-detection, authenticating Alice's and participants' identities and resisting a variety of attacks effectively even over lossy or noisy quantum channels.

4.2 Recursive (2,3) threshold quantum direct secret sharing

Our new protocol is based on the following three assumptions.

(1) The adversary Eve can intercept the quantum communication and perform block processing of quantum data on the quantum channel. She can listen to all the messages but cannot modify them on the classical channel.

(2) Alice intends to share a secret $s = \{s^{[1]}, s^{[2]}, \ldots, s^{[l]}\}$ among 3 participants Bob_1, Bob_2, Bob_3, where $s^{[n]} \in \{0, 1\}, n = 1, 2, \ldots, l$, where $s^{[n]}$ denotes the n^{th} bit in s. Moreover, at least two of the Bobs can recover s.

(3) Alice uses 3 values, say, $p_1 = 0$, $p_2 = 1$ and $p_3 = 2$ to encode each bit of the classical secret. Alice and Bob_1, Bob_2, Bob_3 agree that p_1, p_2, p_3 encodes bit 0 if $p_1 = p_2 = p_3$, and p_1, p_2, p_3 encodes bit 1 if $p_1 \neq p_2 \neq p_3$. Hence, 000, 111, or 222 can be used to encode

bit 0, while 021, 012, 102, 120, 210, or 201 can be used to encode bit 1. Note that the module 3 sum of the three values is 0, that is, $(p_1+p_2+p_3)\ mod\ 3 = 0$. Meanwhile, three different particle states $|0\rangle$, $|1\rangle$, $|2\rangle$ are used to represent the corresponding encoding of bits.

4.2.1 Preparation and precomputation

We assume that the length of the shared secret meets the requirement $l = \sum_{i=1}^{k} 3^{i-1}, k \in \mathbb{N}$ and $k \geq 1$. However, if l does not meet the requirement, the following encoding and decoding processes are still effective by dividing the secret into smaller chunks, each of which meets the requirement. For instance, if the length of secret s is $l = 18$, it can be divided into three smaller chunks of 1 bit, 4 bits and 13 bits with the length of $l_1 = 1$, $l_2 = \sum_{i=1}^{2} 3^{i-1}$ and $l_3 = \sum_{i=1}^{3} 3^{i-1}$ respectively. In this case, Alice and the Bobs share the secret by applying the recursive method to each of the chunks separately.

In the following, the symbol s represents the secret (or a chunk of it determined as above) which satisfies the length requirement. Before producing the quantum secret shares $p_{s_{k,1}}$, $p_{s_{k,2}}$ and $p_{s_{k,3}}$, Alice prepares $s_{k,1}$, $s_{k,2}$ and $s_{k,3}$ by the recursive way defined as follows. First of all, each secret share s_j (for $j = 1, 2, 3$) is the result of the concatenation of smaller pieces of $s_{1,1}, \ldots, s_{k,1}$ built using recurrence

$$s_j = \Big|\Big|_{i=1}^{k} s_{i,j} \quad (\text{for } j = 1, 2, 3)$$

By the requirement given in assumption (3) above, the modulo 3 sum of the corresponding values in the three shares equals zero:

$$(\sum_{i=1}^{3} s_i^{[n]}) \mod 3 = 0 \ (\text{for } n = 1, \ldots, l)$$

where $s_i^{[n]}$ denotes the n^{th} value in share s_i.

The encoding process

Base case. For $i = 1$, the first secret piece (the first secret bit) is encoded into three smaller pieces of $s_{1,1}$, $s_{1,2}$, $s_{1,3}$ by assumption (3).

Recursive case. For $i > 1$, assume that pieces $s_{i-1,1}$, $s_{i-1,2}$, $s_{i-1,3}$ are encoded already. Then pieces $s_{i,1}$, $s_{i,2}$, $s_{i,3}$ are encoded as follows:

$$s_{i,1} = \mathbf{s_{i-1,1}} \parallel 3^{i-2}values \parallel 3^{i-2}values$$

$$s_{i,2} = 3^{i-2}values \parallel \mathbf{s_{i-1,2}} \parallel 3^{i-2}values$$

$$s_{i,3} = 3^{i-2}values \parallel 3^{i-2}values \parallel \mathbf{s_{i-1,3}}$$

Here the corresponding values in the three smaller pieces of $s_{i,1}, s_{i,2}, s_{i,3}$ encode one piece of the secret as per assumption (3) above.

More intuitively, for each corresponding bit of the secret message, one encoding symbol is already determined by the previous $(i-1)^{th}$ step. If the bit has value 0, Alice copies the same encoding symbol (0,1 or 2) to the other two. If the bit has value 1, Alice decides on the other two encoding symbols randomly out of two possible combinations based on the already determined encoding symbol where the sum of the encoding symbols will be 3.

The decoding process

Assume that Bob_1's, Bob_2's and Bob_3's shares that are converted from quantum secret shares $p_{s_{k,1}}$, $p_{s_{k,2}}$ and $p_{s_{k,3}}$ are $s_{k,1}$, $s_{k,2}$ and $s_{k,3}$, then any two participants, say Bob_2 and Bob_3, can recover the secret using $s_{k,2}$ and $s_{k,3}$ as follows:

For $n = 1, \ldots, 3^{k-1}$,

$$s_{k,1}^{[n]} = x \in \{0, 1, 2\}$$

where $s_{k,2}^{[n]} + s_{k,3}^{[n]} + x \ mod\ 3 = 0$.

Now, Bob_2 and Bob_3 also have $s_{k,1}$. So Bob_2 and Bob_3 can just line up $s_{k,1}$, $s_{k,2}$ and $s_{k,3}$ and read out each bit of the secret determined by the three corresponding encoding symbols in $s_{k,1}$, $s_{k,2}$ and $s_{k,3}$. They can recover the secret message by applying the recursive method in the reverse direction as follows:

For $2 \leq i \leq k$

$$s_{i-1,1} = s_{i,1}^{[1 \to 3^{i-2}]}$$
$$s_{i-1,2} = s_{i,2}^{[(3^{i-2}+1) \to 2 \times 3^{i-2}]}$$
$$s_{i-1,3} = s_{i,3}^{[(2 \times 3^{i-2}+1) \to 3 \times 3^{i-2}]}$$

where the notation $s^{[m \to n]}$ represents a substring of s from the m^{th} to the n^{th} bits. At each step, they line up $s_{i-1,1}$, $s_{i-1,2}$ and $s_{i-1,3}$, and read out the corresponding bits of the secret.

4.2.2 The proposed (2,3) threshold quantum secret sharing protocol

Sharing secret messages

We now demonstrate our protocol by giving an exact example of encoding and sharing a secret s, say 10101101011010110110101101100111001011 01, following the recursive way. The length of the message is $l = \sum_{i=1}^{4} 3^{i-1} = 3^0 + 3^1 + 3^2 + 3^3$.

(1) For $i = 1$, we encode the first bit of the secret (boxed below) by the base case as follows:

$$s = \boxed{1}\,0101101011010110110101101100111001011 01$$

$$s_{1,1} = 0$$

$$s_{1,2} = 2$$

$$s_{1,3} = 1$$

Note that to encode "0", we arbitrarily choose one of the six combination of "0", "2", "1".

(2) For $i = 2$, we encode the next three bits of the secret (boxed below) by the recursive case as follows:

$$s \ = 1\,\boxed{\mathbf{010}}\,1101011010110110101101100111001011 01$$

$$s_{2,1} = \mathbf{0}11$$

$$s_{2,2} = 0\mathbf{2}1$$

$$s_{2,3} = 00\mathbf{1}$$

(3) For $i = 3$, we encode the next nine bits of the secret (boxed below) by the recursive case as follows:

$$s \ = 1\ 010\ \boxed{\mathbf{110101101}}\ 011011010110110011100101101$$

$$s_{3,1} = \mathbf{011}122102$$

$$s_{3,2} = 121\mathbf{021}200$$

$$s_{3,3} = 201220\mathbf{001}$$

(4) For $i = 4$, we encode the last 27 bits of the secret (boxed below) by the recursive case as follows:

$$s \ = 1\ 010\ 110101101\ \boxed{\mathbf{011011010110110011100101101}}$$

$$s_{4,1} = \mathbf{01112210}2011101221001121202$$

$$s_{4,2} = 020101122\mathbf{12102120}0101022100$$

$$s_{4,3} = 00211011220121121\mathbf{201220001}$$

Then Alice allocates the quantum secret shares to Bob_1, Bob_2, Bob_3 in terms of $s_{4,1}$, $s_{4,2}$ and $s_{4,3}$, which is as follows:

(5) Alice converts the largest of the classical shares, that is, $s_{4,1}$, $s_{4,2}$ and $s_{4,3}$ into corresponding particle states $p_{s_{k,1}} = \{|0\rangle, |1\rangle, \ldots, |0\rangle, |2\rangle\}$; $p_{s_{k,2}} = \{|0\rangle, |2\rangle, \ldots, |0\rangle, |0\rangle\}$ and $p_{s_{k,3}} = \{|0\rangle, |0\rangle, \ldots, |0\rangle, |1\rangle\}$.

(6) For Bob_1, Alice then produces sufficiently many nonorthogonal state particles with base B_1 and value V_1 in terms of the control codes (which are generated by the established sequence S_1 like in BB84) in terms of Figure 2.1 as decoy particles. In B_1, 0 represents base $\oplus$ and 1 represents base $\otimes$. In base $\oplus$, 0 denotes state $|\rightarrow\rangle$, 1 denotes state $|\uparrow\rangle$; In base $\otimes$, 0 denotes state $|\nearrow\rangle$, 1 denotes state $|\searrow\rangle$. For example, if $B_1 = 01100101, V_1 = 10110100$, then the states of these nonorthogonal state particles are $|\uparrow\rangle$ $|\nearrow\rangle$ $|\searrow\rangle$ $|\uparrow\rangle$ $|\rightarrow\rangle$ $|\searrow\rangle$ $|\rightarrow\rangle$ $|\nearrow\rangle$. Moreover, Alice and Bob_1 agree that in the control codes, "0" denotes that the measurement base"$\oplus$" should be used and "1" denotes that the measurement base "$\otimes$" should be used.

(7) Then Alice first produces a new particle sequence $p'_{s_{k,1}}$ by inserting her prepared nonorthogonal state particles into $p_{s_{k,1}} = \{|0\rangle, |1\rangle, \ldots, |0\rangle, |2\rangle\}$ and recodes each insertion position. Then Alice sends the new sequence $p'_{s_{k,1}}$ to Bob_1 via a quantum channel. Meanwhile, degrees and positions are used to generate the control codes for detecting eavesdropping and to obtain the positions of nonorthogonal state particles to Bob_1 through a classical channel.

(8) After receiving $p'_{s_{k,1}}$ from Alice, Bob_1 first obtains the positions of the nonorthogonal state particles using the degrees and positions of the source symbols sent by Alice.

Then Bob_1 produces the control codes in terms of the degrees and the positions of the source symbols. Bob_1 is able to detect eavesdropping according to the nonorthogonal state particles and the control codes without sending classical messages to Alice. If the error rate of the nonorthogonal state particles exceeds the threshold they agree in advance, they abort this protocol. Otherwise, Alice and Bob_1 can conclude that there is no eavesdropping in this communication and Alice is a trusted dealer, then Bob_1 continues to the next step.

(9) Bob_1 filters the nonorthogonal state particles and obtains his quantum secret share $|0\rangle$, $|1\rangle$, ..., $|0\rangle$, $|2\rangle$.

(10) Alice transmits $p_{s_{k,2}}, p_{s_{k,3}}$ to Bob_2 and Bob_3 respectively in the same way that is used in (5) and (7).

Message recovery

Any two of the three participants can recover the secret, say Bob_2 and Bob_3. They convert their quantum secret shares $p_{s_{k,2}} = \{|0\rangle, |2\rangle, \ldots, |0\rangle, |0\rangle\}$ and $p_{s_{k,3}} = \{|0\rangle, |0\rangle, \ldots, |0\rangle, |1\rangle\}$ into corresponding encoding symbols $s_{4,2} = 02010112212102120010102 2100$, $s_{4,3} = 002110112 201211212201220001$. Then, according to the encoding rule, Bob_2 and Bob_3 can obtain the share of Bob_1, which is $p_{s_{k,1}} = \{|0\rangle, |1\rangle, \ldots, |0\rangle, |2\rangle\}$ with its corresponding encoding symbols $s_{4,1} = 011122102011101221001121202$.

Having obtained all of $s_{4,1}, s_{4,2}, s_{4,3}$, Bob_2 and Bob_3 can then recover the secret message by applying the recursive method in the reverse direction in a step-wise fashion.

(1) Bob_2 and Bob_3 line up the three pieces and obtain the bits $14 \rightarrow 40$ in s (denoted by $s^{[14\rightarrow 40]}$).

$$s_{4,1} = \mathbf{01112210}2011101221001121202$$

$$s_{4,2} = 020101122\mathbf{12102120}0101022100$$

$$s_{4,3} = 00211011220121121\mathbf{201220001}$$

$$s^{[14\rightarrow 40]} = \boxed{011011010110110011100101101}$$

(2) Then Bob_2 and Bob_3 extract $s_{3,1}, s_{3,2}, s_{3,3}$ and line them up to obtain the bits 5→13 in s (denoted by $s^{[5\rightarrow 13]}$).

$$s_{3,1} = \mathbf{011}122102$$

$$s_{3,2} = 121\mathbf{021}200$$

$$s_{3,3} = 201220\mathbf{001}$$

$$s^{[5\rightarrow 13]} = \boxed{110101101}$$

(3) Then Bob_2 and Bob_3 extract $s_{2,1}, s_{2,2}, s_{2,3}$ and line them up to obtain the bits 2→4 in s (denoted by $s^{[2\rightarrow 4]}$).

$$s_{2,1} = \mathbf{0}11$$

$$s_{2,2} = 0\mathbf{2}1$$

$$s_{2,3} = 00\mathbf{1}$$

$$s^{[2\rightarrow 4]} = \boxed{010}$$

(4) Finally, Bob_2 and Bob_3 extract $s_{1,1}, s_{1,2}, s_{1,3}$ and line them up to obtain the first bit in s (denoted by $s^{[1]}$).

$$s_{1,1} = 0$$

$$s_{1,2} = 2$$

$$s_{1,3} = 1$$

$$s^{[1]} = \boxed{1}$$

Hence, Bob_2 and Bob_3 recover the secret $s = 101011010110101101101011011001100101101$.

Although we have presented our protocol by way of an example, a general presentation of the (2,3) threshold quantum secret sharing scheme of secure direct communication can be easily achieved in the same way.

4.2.3 The efficiency and security analysis

In this section, we analyze the efficiency and security of our proposed protocol from the following aspects.

Efficiency

We show that by the use of the recursive method, the efficiency of secret sharing in our proposed protocol has been greatly improved. The specific analysis is made as follows.

The qutrit efficiency is:

$$\eta_E = \frac{q_s}{q_t}$$

where q_s denotes the Alice's shared secret bits, and q_t is the total number of the photons of the secret share of every participant in the protocol. For a secret with the length of $l = \sum_{i=1}^{k} 3^{i-1}, i \geq 1$, as l goes to ∞, the qutrit efficiency is

$$\eta_E = \lim_{k\to\infty} \frac{1+3+3^2+\ldots+3^{k-1}}{3^{k-1}} = \lim_{k\to\infty} \frac{3^k-1}{2\cdot 3^{k-1}} = \frac{3}{2}$$

That is to say, every particle can on average carry up to 1.5-bit messages rather than at most 1 bit message in existing relevant quantum secret sharing protocols.

It is worth noting that, as is mentioned in 4.2.1, if the length of a secret does not meet the formation $l = \sum_{i=1}^{k} 3^{i-1}$, it can be divided into smaller chunks such that these smaller chunks satisfy the formation before applying the recursive method. For the same example in 4.2.1, for a secret of 18 bits, we first cut the secret into three chunks, $s^{[1]}$ of 1 bit, $s^{[2\to 5]}$ of 4 bits and $s^{[6\to 18]}$ of 13 bits, and then encode them as above. The qutrit efficiency is $\frac{18}{1+3+9} = \frac{18}{13}$.

Hence, we can obtain the following theorem.

Theorem 1. For a secret with any length $l = \sum_{i=1}^{k} x_i \sum_{j=1}^{i} 3^{j-1}$, where $\sum_{i=1}^{k} 3^{i-1} \leq l < \sum_{i=1}^{k+1} 3^{i-1}$ in our proposed recursive (2,3) threshold quantum secret sharing, the qutrit efficiency is $1 \leq \eta_E < \frac{3}{2}$.

Proof. We first consider the following two particular cases.

(1) When $x_i = 1, 2, 3$, according to the definition of η_E, $\eta_E = 1$ for each case.

(2) When $x_i = 0, i = 1, 2, \ldots, k-1, x_k = 1$, the recursive method works, then the maximum η_E can be obtained, that is, $\eta_E = \lim_{k\to\infty} \frac{1+3+3^2+\ldots+3^{k-1}}{3^{k-1}} = \lim_{k\to\infty} \frac{3^k-1}{2\cdot 3^{k-1}} = \frac{3}{2}$.

(3) Then we prove the general case.

$$
\begin{aligned}
\eta_E &= \frac{\sum_{i=1}^{k} x_i \sum_{j=1}^{i} 3^{j-1}}{\sum_{j=1}^{k} 3^{j-1}} \\
&= \frac{x_1 + (1+3)x_2 + \ldots + (1+3+\ldots+3^{k-1})x_k}{x_1 + 3x_2 + \ldots + 3^{k-1}x_k} \\
&= \frac{x_1 + \ldots + 3^{k-1}x_k + [x_2 + \ldots + (1+3+\ldots+3^{k-2})x_k]}{x_1 + \ldots + 3^{k-1}x_k} \\
&= 1 + \frac{x_2 + \ldots + (1+3+\ldots+3^{k-2})x_k}{x_1 + 3x_2 + \ldots + 3^{k-1}x_k} \\
&= 1 + \frac{x_2 + \ldots + (1+3+\ldots+3^{k-2})x_k}{x_2 + \ldots + (1+\ldots+3^{k-2})x_k + (x_1 + \ldots + \frac{3^{k-1}+1}{2}x_k)} \\
&= 1 + \frac{1}{1 + \frac{x_1+\ldots+\frac{3^{k-1}+1}{2}x_k}{x_2+\ldots+(1+3+\ldots+3^{k-2})x_k}} \\
&= 1 + \frac{1}{1 + \frac{x_2+\ldots+(1+3+\ldots+3^{k-2})x_k+x_1+\ldots+x_k}{x_2+\ldots+(1+3+\ldots+3^{k-2})x_k}} \\
&= 1 + \frac{1}{1+1 + \frac{x_1+\ldots+x_k}{x_2+\ldots+(1+3+\ldots+3^{k-2})x_k}} \\
&= 1 + \frac{1}{1+1 + \frac{x_2+\ldots+3^{k-1}x_k+x_1+\sum_{i=2}^{k}\frac{3-3^{i-1}}{2}x_i}{x_2+\ldots+3^{k-1}x_k}} \\
&= 1 + \frac{1}{1+1+1 + \frac{x_1+\sum_{i=2}^{k}\frac{3-3^{i-1}}{2}x_i}{x_2+\ldots+3^{k-1}x_k}}
\end{aligned}
\tag{4.1}
$$

When $i = 2$, let $M = \frac{x_1+\sum_{i=2}^{k}\frac{3-3^{i-1}}{2}x_i}{x_2+\ldots+3^{k-1}x_k}$, then $M_{max} = \frac{x_1}{x_2}$. Hence, $(\eta_E)_{min} = 1 + \frac{1}{3+\frac{x_1}{x_2}} = \frac{4x_2+x_1}{3x_2+x_1}$.

According to the above-mentioned cases (1), (2) and (3) in this proof, we can obtain $1 \leq \eta_E < \frac{3}{2}$.

Meanwhile, we make a table (see Tab. 4.1) to compare the qubit or qutrit efficiency in the recent well-known protocols, including Bennett and Brassard [3], Bennett [6] and Ekert [7].

Also, due to the shared sequences between Alice and Bobs, Bobs can detect eavesdropping by themselves without sending classical messages to Alice. Instead, Bobs only need to ascertain whether the error rate of the detection particles, i.e., nonorthogonal

Table 4.1: The comparison of qubit or qutrit efficiency.

Protocols	b_s	q_s	b_e	R
our protocol [82]	≈ 1.5	1	0	≈ 1.5
Bennett and Brassard's protocol [3]	1	1	2	$\frac{1}{3}$
Bennett's protocol [6]	1	2	0	0.5
Ekert's protocol [7]	2	2	2	0.5

state particles, is larger than the preset value or not. As a result, the process of secret sharing is more efficient.

Moreover, our proposed protocol can be easily generalized to $(2, n)$ threshold quantum secret sharing of secure direct communication. When more participants are involved, more particles can be saved.

Dynamics

Due to the way of encoding each bit of the message in assumption (3), there are three different choices (000, 111, or 222) to encode bit 0 and six different approaches (021, 012, 102, 120, 210, or 201) to encode bit 1. When a participant leaves and a new participant joins, we just change the encoding, for example, before that we use 000 to decode bit 0, after that we use 222 to do so; similarly, before that we use 012 to encode bit 1, but after that we use 210. Though the secret stays unchanged, the secret shares change. The secret share of the participant who has left is useless.

Security analysis

We now discuss the security of our proposed protocol. The security of the protocol is based on quantum no-cloning theorem and the disordered photons by inserting nonorthogonal state particles. Quantum no-cloning theorem guarantees that an eavesdropper, Eve,

is not able to make certain of the initial states of the transmitted particles prepared by Alice, as in the BB84 protocol [3]. The difference between the BB84 protocol (here, we take BB84 because our protocol is derived from it) and our protocol is that the communicating parties choose the measurement base randomly for keeping Eve from eavesdropping in the former, while nonorthogonal state particles are inserted to prevent Eve from obtaining the Alice's secret sharing in the latter. Assume that Eve intercepts the photons from Alice to $Bob_i, (i = 1, 2, 3)$ and resends her prepared photons to $Bob_i, (i = 1, 2, 3)$. However, she cannot extract Alice's secret message without disturbing the process of secret sharing. This is because, on the one hand, she does not know the positions of inserted nonorthogonal state particles, which are identified by the degrees and the positions of the shared sequence between Alice and $Bob_i, (i = 1, 2, 3)$. On the other hand, she does not know which measurement base should be used, as the measurement base is also identified by the control codes that are produced by the degrees and the positions of the shared sequence. Moreover, the positions of inserted nonorthogonal state particles and the control codes are generated in the way of preparing fountain codes, which can be generated on-line and have the features of flexibility and randomness. In this case, Eve can just obtain a series of useless data.

Besides, in our (2,3) threshold quantum secret sharing protocol, any two or more participants can reconstruct the secret, but any single participant cannot derive the secret message from his share alone with a non-negligible probability. Because each individual share is always a random quantum state sequence consisting of $|0\rangle$, $|1\rangle$ and $|2\rangle$ and the probability of a successful guess of the other two codes from a single known code is $\frac{1}{3}$. This is in fact less than the probability of a successful guess of one bit of the secret message.

Most importantly, the most common attack, that is, the Trojan horse attack is useless in our protocol. The Trojan horse attack strategy is normally involved in the invisible photon eavesdropping (IPE) attack. Whether Eve is $Bob_i (i = 1, 2, 3)$ or an outside eaves-

dropper, she may consider such attack strategies firstly when she attempts to recover the secret. Now, we analyze the IPE attack in detail. Eve prepares a sequence of invisible photons with a special wavelength in advance, which is close to the legitimate one. In this case, she can add invisible photons to the photons that are sent to the other two participants before Alice. However, as the photons in our proposed protocol are transmitted once, Trojan horse attacks are avoided automatically. Therefore, Eve cannot obtain any useful messages using invisible photons, that is, our protocol is free from Trojan horse attacks.

4.3 (n, n) threshold quantum direct secret sharing based on fountain codes

In this section, we describe our proposed (n, n) threshold quantum direct secret sharing protocol [119]. In the protocol, Alice and every Bob first establish a sequence that is considered as the source symbols in advance like in BB84, which is unknown to Eve. These source symbols are used to prepare the control codes and obtain the positions of the inserted nonorthogonal state particles in terms of Figure 2.1. Next, nonorthogonal state particles are produced to detect eavesdropping according to the prepared control codes. Finally, Bobs and Alice send the particle sequences and encoded particle sequences after inserting nonorthogonal state particles into them to each other.

4.3.1 The proposed protocol

We first list the following three assumptions:

1) The same as (1) of 4.2.1.

2) Alice intends to share a secret $s_A = \{s_A^1, s_A^2, \ldots, s_A^l\}$ among n participants $Bob_1, Bob_2, \ldots, Bob_n$, where $s_A^k \in \{0, 1\}, k = 1, 2, \ldots, l$. She will first split s_A into n secret shares

$s_{B_1}, s_{B_2}, \ldots, s_{B_n}$ where $s_{B_i} = \{s_{B_{i1}}, s_{B_{i2}}, \ldots, s_{B_{il}}\}(i = 1, 2, \ldots, n)$, which will later be delivered to $Bob_1, Bob_2, \ldots, Bob_n$ respectively. Only if all Bobs collaborate with their shadows, can Alice's secret s_A be recovered.

3) Alice and $Bob_i(i = 1, 2, \ldots, n)$ agree on that each of the unitary operations denote a two-bit classical message, i.e., U_0, U_1, U_2, U_3 correspond to 00, 01, 10 and 11, respectively. Alice and $Bob_i(i = 1, 2, \ldots, n)$ establish $S_i(i = 1, \ldots, n)$ using the same way in BB84. Then $S_i(i = 1, \ldots, n)$ is used as source symbols in producing fountain codes which are used for control codes in the following protocol.

The process of our protocol is as follows:

Step 1. $Bob_i(i = 1, 2, \ldots, n)$ prepares $\frac{l}{2}$ EPR pairs and each EPR pair is supposed to be $|\Phi^+\rangle_{h_{i_1}t_{i_1}} = \frac{1}{\sqrt{2}}(|0\rangle_{h_{i_1}}|0\rangle_{t_{i_1}} + |1\rangle_{h_{i_1}}|1\rangle_{t_{i_1}})$. All of the 1st particles of each $|\Phi^+\rangle_{h_{i_1}t_{i_1}}(i_1 = 1, 2, \ldots, \frac{l}{2})$ are to form an ordered photon sequence $H_i(i = 1, 2, \ldots, n)$ and all of the 2nd particles of each $|\Phi^+\rangle_{h_{i_1}t_{i_1}}$ are to form an ordered photon sequence $T_i(i = 1, 2, \ldots, n)$. The latter is for encoding secret shares.

Step 2. $Bob_i(i = 1, 2, \ldots, n)$ produces sufficiently many nonorthogonal state particles for detecting eavesdropping using the same way in (6) of 4.2.2.

Step 3. $Bob_i(i = 1, 2, \ldots, n)$ randomly inserts his prepared nonorthogonal state particles into the ordered photon sequence $T_i(i = 1, 2, \ldots, n)$ and records each position (only $Bob_i(i = 1, 2, \ldots, n)$ knows the positions of these nonorthogonal state particles and he keeps them secret until the communication is completed). We denote the sequence that is composed of nonorthogonal state particles and $T_i(i = 1, 2, \ldots, n)$ with $T_i'(i = 1, 2, \ldots, n)$. Then $Bob_i(i = 1, 2, \ldots, n)$ sends photon sequence $T_i'(i = 1, 2, \ldots, n)$ via a quantum channel. Meanwhile $Bob_i(i = 1, 2, \ldots, n)$ clearly tells Alice which degrees and positions are used to the generate control codes for detecting eavesdropping and which are used to obtain the positions of nonorthogonal state particles (of course Alice needs to convert the binary bit values into decimal numbers when the positions of the

nonorthogonal state particles are involved) via a classical channel.

Step 4. After receiving T_i' from $Bob_i(i = 1, 2, \ldots, n)$, Alice first finds the positions of the nonorthogonal state particles using degrees and positions of the source symbols from $Bob_i(i = 1, 2, \ldots, n)$. Then Alice produces the control codes in terms of the degrees and the positions of the source symbols from $Bob_i(i = 1, 2, \ldots, n)$. Alice is able to detect eavesdropping according to the nonorthogonal state particles and her generated control codes. If there is no eavesdropping, the outcomes should be completely unanimous. After that, if the error rate exceeds the threshold they preset, they abort this protocol. Otherwise, Alice and $Bob_i(i = 1, 2, \ldots, n)$ can conclude that there is no eavesdropping in this communication and Alice continues to the next step.

Step 5. Alice first encodes the shadow (that is, the share) sequence $\{s_{B_{i1}}, s_{B_{i2}}, \ldots, s_{B_{il}}\}(i = 1, 2, \ldots, n)$ onto $T_i(i = 1, 2, \ldots, n)$ which is contained in T_i' using one of the four unitary operations (U_0, U_1, U_2, U_3). Consequently, the state $|\Phi^+\rangle$ of each particle is transformed into one of $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\psi^+\rangle$, $|\psi^-\rangle$, respectively. These operations correspond to 00, 01, 10, and 11. The encoded sequence is denoted by $T_i''(i = 1, 2 \ldots, n)$. Then Alice produces sufficiently many nonorthogonal state particles for detecting eavesdropping with base B_i' and value V_i' in the same way as that are used in (6) of 4.2.2. Likewise, Alice and $Bob_i(i = 1, 2, \ldots, n)$ agree that in the control codes, "0" denotes that measurement base"$\oplus$" should be used and "1" denotes that measurement base "$\otimes$" should be used.

Step 6. Alice randomly inserts her prepared nonorthogonal state particles into the ordered photon sequence $T_i''(i = 1, 2, \ldots, n)$ and records each position (only Alice knows the positions of these nonorthogonal state particles and she keeps them secret until the communication is completed). We denote the sequence that is composed of the nonorthogonal state particles and $T_i''(i = 1, 2, \ldots, n)$ with $T_i'''(i = 1, 2, \ldots, n)$. Then Alice sends the photon sequence $T_i'''(i = 1, 2, \ldots, n)$ via a quantum channel to $Bob_i(i = 1, 2, \ldots, n)$. Meanwhile Alice clearly tells $Bob_i(i = 1, 2, \ldots, n)$ which degrees and positions are used

to generate control codes for detecting eavesdropping and which are used to obtain the positions of the nonorthogonal state particles (of course Alice needs to convert the binary bit values into decimal numbers when the positions of the nonorthogonal state particles are involved) to $Bob_i(i = 1, 2, \ldots, n)$ via a classical channel.

Step 7. When receiving $T_i'''(i = 1, 2, \ldots, n)$, $Bob_i(i = 1, 2, \ldots, n)$ first finds the positions of the nonorthogonal state particles using degrees and positions of the source symbols from Alice. Then $Bob_i(i = 1, 2, \ldots, n)$ produces control codes in term of the degrees and the positions of the source symbols from Alice. $Bob_i(i = 1, 2, \ldots, n)$ is able to detect eavesdropping according to the nonorthogonal state particles and his generated control codes. If there is no eavesdropping, the outcomes should be completely unanimous. After that, if the error rate is smaller than a preset threshold, Alice and $Bob_i(i = 1, 2, \ldots, n)$ can conclude that there is no eavesdropping in this communication, and $Bob_i(i = 1, 2, \ldots, n)$ continues to next step. Otherwise, the process is aborted.

Step 8. Finally, $Bob_1, Bob_2, \ldots, Bob_n$ obtain $T_i''(i = 1, 2, \ldots, n)$ which is contained in the T_i''' and measure all the particles in $\{(H_1, T_1''), (H_2, T_2''), \ldots, (H_n, T_n'')\}$ in their hands respectively and the corresponding measurement outcomes are $\{s_{B_1}, s_{B_2}, \ldots, s_{B_n}\}$. Hence, when $Bob_1, Bob_2, \ldots, Bob_n$ collaborate with each other, they can recover the secret $s_A = s_{B_1} \oplus s_{B_2} \oplus \ldots \oplus s_{B_n}$.

4.3.2 Security analysis

In this section, we analyze the security of our proposed protocol against inside and outside attacks and under noisy and lossy quantum channels.

Insider attacks

For computer systems, insider attacks are the primary hazard. Insiders are probably to have legitimate access to the system with specific goals and objectives. Normally,

insiders can plant Trojan horse attacks with the file system.

Trojan horse attacks. For such attacks, suppose that Eve is any participant, say Bob_1, who wants to estimate the states of the photons the minute Alice extracts the secret message. In this case, she can add invisible photons to the photons that are sent to the other $n-1$ participants before Alice. However, in our proposed protocol, on the one hand, $Bob_2, \ldots, Bob_n$ and Alice insert nonorthogonal state particles into $T_i (i = 2, \ldots, n)$ and $T_i'' (i = 2, \ldots, n)$ in terms of the control codes (which are generated by $S_i (i = 2, \ldots, n)$). On the other hand, the generated control codes and the positions of inserted nonorthogonal state particles are obtained according to the sent degrees and positions of the source symbols in the pre-shared sequence between $Bob_i (i = 2, \ldots, n)$ and Alice. Consequently, without knowing the pre-shared sequence between $Bob_i (i = 2, \ldots, n)$ and Alice, Eve cannot tell whether the particles are from EPR pairs or from nonorthogonal state particles, i.e., Eve cannot obtain any useful information using invisible photons, and our protocol is free from Trojan horse attacks.

Outside attacks

Suppose that Eve is an outside eavesdropper who intends to steal Alice's secret message. In this situation, Eve can try to estimate the states of the photons immediately before or after Alice's operation to extract the secret message. She adds invisible photons to the photons from Alice to $Bob_i (i = 1, 2, \ldots, n)$ before Alice. Similar to the Trojan horse attacks' analysis, Eve cannot obtain Alice's secret message either.

Eavesdropping attacks. We detect eavesdropping by the way (no-cloning principle) that is used in the BB84 protocol [3], that is, any measurement will certainly disturb the quantum state except when the quantum state is the measuring device's eigenstate. The nonorthogonal state particles, in our protocol, are used to check whether there exist eavesdroppers in terms of their produced control codes. Therefore, its security is equal to

that in the BB84 protocol.

Intercept-measure-resend attacks. In this attack, Eve wants to estimate the states of the photons immediately before or after Alice's operation to extract the secret message. Hence, Eve first intercepts the photons from Alice to $Bob_i(i = 1, 2, \ldots, n)$. Then she measures these photons before Bob. Finally, she re-sends the intercepted photons to $Bob_i(i = 1, 2, \ldots, n)$. In this way, Eve cannot extract Alice's secret message with this attack without knowing the control codes and the positions of the inserted nonorthogonal state particles, but will disturb the process of secret sharing. Therefore, in detecting eavesdropping and authentication phase, this attack will be discovered using their produced control codes easily.

Cheating attacks. Alice and $Bob_i(i = 1, 2, \ldots, n)$ can authenticate each other by detecting the error rate on the quantum channel using the control codes generated from the shared source symbols $S_i(i = 1, 2, \ldots, n)$. In ideal conditions, their measured outcomes should be unanimous. Moreover, only the degrees and the positions of the source symbols are transmitted between Alice and $Bob_i(i = 1, 2, \ldots, n)$, so Eve cannot obtain $S_i(i = 1, 2, \ldots, n)$. Therefore, it is not possible for Eve to impersonate Alice/$Bob_i(i = 1, 2, \ldots, n)$ and distribute false information to $Bob_i(i = 1, 2, \ldots, n)$/Alice.

Dense coding attacks. Dense coding attacks are effective in sending an ordered photon sequence [120]. However, in our proposed protocol, the ordered photon sequence is disordered by the inserted nonorthogonal state particles, and Eve cannot obtain the positions of the inserted nonorthogonal state particles because Alice/$Bob_i(i = 1, 2, \ldots, n)$ just transmit the degrees and positions of the source symbols(that is their pre-shared sequences) without these source symbols. Therefore, our proposed protocol can resist dense coding attacks.

Noisy and lossy quantum channels

In most of the existing quantum secret sharing protocols, the quantum channels are supposed to be ideal (i.e., noiseless and lossless). However, even if quantum channel is a noisy or a lossy, our proposed protocol is still robust. Here, we assume that Eve is able to establish an ideal channel with every Bob. The case of noisy and the lossy quantum channels are discussed separately as follows.

Case 1. Noisy quantum channels. Eve may attempt to hide her attack behavior in the noise of the quantum channel. Obviously, it is impossible to detect an attack if the quantum bit error rate (QBER) τ of noise (which according to [68] is approximately within $2 \sim 8.9\%$ depending on the channel situation such as distance, etc.) is higher than the preset eavesdropper check threshold ϵ. However, in step 4 of our protocol, we can set the threshold ϵ in our protocol to be $0.1 \sim 0.2$ since the eavesdropping detection rate of each decoy photon (nonorthogonal state particles) is $\frac{1}{4}$ (25%). It is obviously higher than τ, so Eve will not be able to hide her attack behavior in the noise of the quantum channel.

Case 2. Lossy quantum channels. In practical settings, quantum channels are lossy. When the transmission occurs over a lossy quantum channel, some of the photons might be lost. Fortunately, our protocol employs the idea of generating fountain codes which can solve the lossy quantum channel issue. That is to say, the participants are able to inform the sender about which particles have been received and which particles lost during the transmission process using the classical channel (the reason is the same as that in Case 1). The participants just use the received photons to perform the public discussion. This is because the lost photons and their corresponding particles will be eventually discarded. Moreover, from those lost photons, Eve cannot extract any useful information about the shared key. Hence, our protocol is still secure under this case.

4.3.3 Features of our protocol

Compared with the existing quantum direct secret sharing protocols, our protocol has the following features.

1. In our protocol, the nonorthogonal state particles are used to detect eavesdropping in terms of the control codes generated from the shared sequence $S_i(i = 1, 2, \ldots, n)$ between Alice and $Bob_i, i = 1, 2, \ldots, n$, and the efficiency of detecting eavesdropping is 100% under the ideal conditions compared with 50% in [3]. Moreover, due to the use of the control codes. Alice and Bobs can detect eavesdropping by themselves instead of sending classical messages to Alice. Hence, our proposed protocol is more efficient than [78, 109–112].

2. Our protocol makes use of the property of quantum physics to realize authentication. Instead of using classical methods and transmitting classical information, we use nonorthogonal state particles and entanglement. Entangled states are applied to transmitted secret shares, nonorthogonal state particles are employed to ensure the security of the communication, and identity authentication is based on the control codes generated from the shared source symbols $S_i(i = 1, 2, \ldots, n)$.

3. Because the control codes and the positions of inserted nonorthogonal state particles are generated on-line through the exclusive-or of $i_1(i_1 = 1, 2, \ldots, p)$ bits from the shared sequence $S_i(i = 1, 2, \ldots, n)$ between Alice and $Bob_i, i = 1, 2, \ldots, n$, the size of $S_i(i = 1, 2, \ldots, n)$ can be small and used limitlessly. Moreover, as shown above, our protocol is able to resist a variety of attacks effectively.

4.4 Summary

In this chapter, we first have developed a (2,3) threshold quantum secret sharing protocol for secure direct communication by utilizing fountain codes and a recursive secret encoding method, in which we reduce the amount of quantum data involved and enhance the efficiency of secret sharing. Because of the use of a recursive method and the use of fountain codes, every particle can on average carry up to 1.5-bit messages and the participants can detect eavesdropping by themselves without sending classical messages to Alice. Moreover, the proposed protocol can be easily implemented using the same devices as in BB84. Then the idea of producing fountain codes has been applied in the proposed (n, n) quantum direct secret sharing protocol to produce control codes and the positions of the inserted nonorthogonal state particles, aiming at achieving eavesdropping-detection, authenticating Alice's and participants' identities and resisting a variety of attacks effectively even over lossy or noisy quantum channels. Moreover, the EPR pairs are prepared by Bobs rather than Alice, and consequently, the sequence $H_i(i = 1, 2, \ldots, n)$ in our protocol is not transmitted over the quantum channel, greatly reducing the risk of secret leakage.

Chapter 5

Hybrid quantum cryptography with extended unitary operations

Taking the advantages of both classical (easy and cheap to implement) and quantum (able to resist the appearance of quantum computers) protocols into account, in this chapter, we propose one hybrid quantum key distribution protocol and two hybrid quantum secret sharing protocols by the virtue of constructing extended unitary operations.

5.1 Introduction

Nascimento *et al.* [24] proposed the first hybrid quantum secret sharing protocol. That is, let $|\psi\rangle$ be a quantum state consisting of n particles and K (a random sequence of classical bits of length $2n$), then assign to each particle of $|\psi\rangle$ two classical bits of K that determine which transformation is performed on the respective particle. For instance, 00 corresponds to applying the identity mapping I, 01 to the Pauli X operator, 10 to the Pauli Z operator and 11 to the Pauli Y operator. After this encryption, the resulting state $|\widehat{\psi}\rangle$ is a complete mixture and no information can be gained from it. Only if one has the classical key K, can the original state $|\psi\rangle$ be obtained from $|\widehat{\psi}\rangle$. Later on, Singh *et al.* [69]

extended and improved Nascimeto *et al.*'s protocol, and further proposed some approaches for sharing a quantum secret in a hybrid way, that is, certain participants have only classical shares and the remaining participants have (possibly multiple) quantum shares. In 2011, Fortescue *et al.* [70] proposed a construction for perfect quantum secret sharing protocols based on imperfect "ramp" secret sharing combined with classical encryption, in which the individual participants' shares are split into quantum and classical components, allowing the former to be of lower dimension than the secret itself, and hence reducing the communication cost of quantum secret sharing. However, the total amount of quantum data allocated is not necessarily decreased in these three hybrid quantum secret sharing protocols [24, 69, 70].

As we know, an important issue existing in hybrid quantum secret sharing protocols is the amount of data that is allocated to the participants. The smaller the amount of allocated data, the better the performance of a protocol. Furthermore, as quantum data is very difficult and costly to cope with, it is desirable to use as little quantum data as possible. To address the issue, we first extend the four basic local unitary operations to $2^{2n}, n \geq 2$, n-extended unitary operations that are still composed of the four basic local unitary operations (from 2.17 to 2.20). Extended unitary operations are then used in the design of two hybrid quantum secret sharing protocols. In fact, in 2012, Chou *et al.* [71] extended the four basic local unitary operations to 16 unitary operations and further proposed an enhanced multiparty quantum secret sharing of classical messages to enhance the transmission efficiency of the whole protocol. Later, Chou *et al.* [72] considered using GHZ-State for multiparty quantum secret sharing without a code table associated with the same idea used in [71].

Inspired by Nascimeto *et al.*, Singh *et al.*, Fortescue et al. and Chou *et al.* [24, 69–72], we propose two dual compressible hybrid quantum secret sharing (HQSS) protocols [122] and a hybrid quantum key distribution (HQKD) protocols using extended unitary

operations, which aim at reducing the number of particles and quantum participants and the size of classical shares while maintaining the security of hybrid quantum secret sharing. In our proposed HQSS protocols, we stipulate that there is only one unique quantum participant called Bob; he first prepares $\lambda' + 1$ EPR pairs (where λ' is the number that can provide an analysis of the error). All of the 1st particles from each EPR pair are to form a photon sequence S_H and all of the 2nd particles from each EPR pair are to form a photon sequence S_T. Then Bob keeps the sequence S_H and sends the sequence S_T to Alice via a quantum channel. After confirming that the quantum channel is secure, Alice performs the correct transition operation on a particle from an EPR pair and sends the encoded particle to Bob (here, we assume that only Alice and Bob know the measured basic operations corresponding to particular transition operations respectively as all the extended unitary operations boil down to the four basic unitary operations corresponding classical bits are transmitted to classical participants in various ways via the classical channel.

For HQKD protocols, we make full use of fountain codes that are used in Chapter 4 to produce control codes and corresponding classical bits. Similarly, control codes can be used to enhance the efficiency of eavesdropping detection and test whether participants are legitimate. Moreover, the n-extended unitary operations can be chosen in a flexible way.

When comparing with Fortescue *et al.*'s [70], Nascimeto et al.'s [24] and Singh et al's [69] protocols, our protocols have the following four advantages:

(1) In our proposed protocols, even if Eve can obtain all the transmitted classical data and quantum data, she is not able to obtain any information about the shared secrets. Because, first, she does not know the second particles which are always kept by Bob; second, she does not know which basic unitary operations correspond to which transition operations.

(2) Due to (1), our protocols are more secure in the face of various attacks such as the photon number attack, the entangle-measure attack, the Trojan horse attack and the faked states attack.

(3) Quantum shares and classical shares do not have a direct relationship with the shared secret, but can determine the secret cooperatively. Moreover, owing to the compressibility of quantum data, our protocols are easier, cheaper and more practical to implement in real life.

(4) Not only can our HQSS protocols reduce the number of quantum participants, but also the number of particles and the size of classical shares. To be exact, the number of particles that are used to carry quantum data is reduced to 1 while the size of classical secret shares is also reduced to $\frac{l-2}{m-1}$ based on $((m+1,n'))$ threshold hybrid quantum secret sharing and to $\frac{l-2}{r_2}$ (where r_2 is the number of maximum unqualified sets) based on an adversary structure. Consequently, our proposed protocols can greatly reduce the cost and difficulty of generating and storing EPR pairs and lower the risk of transmitting encoded particles. Also, our protocols can enhance the efficiency of secret sharing.

5.2 Extended unitary operations

In this section, we present the definition of extended unitary operations and their properties.

Assume that we have n basic unitary operations, where $n \geq 2$. Then it is possible to construct 2^{2n} unitary operations according to the following equation [121, 122]:

$$U_{b_1 b_2 b_3 b_4 \ldots b_{2n-1} b_{2n}} = U_{b_1 b_2} \otimes U_{b_3 b_4} \otimes \ldots \otimes U_{b_{2n-1} b_{2n}}, \tag{5.1}$$

where the sequence $b_1 \ldots b_{2n}$ represents an arbitrary $2n$-bit value. Note that if Equation

(5.1) is used to transform an EPR pair $|\psi^-\rangle_{AB}$, the outcome can be written as

$$U^A_{b_1b_2b_3b_4\ldots b_{2n-1}b_{2n}}|\psi^-\rangle_{AB} = U^A_{b_1b_2} \otimes (U^A_{b_3b_4} \otimes (\ldots \otimes (U^A_{b_{2n-1}b_{2n}}|\psi^-\rangle_{AB}))). \tag{5.2}$$

To illustrate the operations, consider the following example for $n = 2$. We use the basic unitary operations $U_{00}, U_{01}, U_{10}, U_{11}$ and build 2-extended unitary operations as shown below:

$$\begin{aligned} U_{0000} &= U_{00} \otimes U_{00} \\ U_{0001} &= U_{00} \otimes U_{01} \\ &\vdots \\ U_{1111} &= U_{11} \otimes U_{11} \end{aligned}$$

The operations can be used to transform Bell states according to the following relations

$$\begin{aligned} U^A_{0000}|\psi^-\rangle_{AB} &= U^A_{00} \otimes U^A_{00}|\psi^-\rangle_{AB} = U^A_{00}|\psi^-\rangle_{AB} = |\psi^-\rangle_{AB}, \\ U^A_{0001}|\psi^-\rangle_{AB} &= U^A_{00} \otimes U^A_{01}|\psi^-\rangle_{AB} = U^A_{00}|\psi^+\rangle_{AB} = |\psi^+\rangle_{AB}, \\ U^A_{0010}|\psi^-\rangle_{AB} &= U^A_{00} \otimes U^A_{10}|\psi^-\rangle_{AB} = U^A_{00}|\phi^-\rangle_{AB} = |\phi^-\rangle_{AB}, \\ U^A_{0011}|\psi^-\rangle_{AB} &= U^A_{00} \otimes U^A_{11}|\psi^-\rangle_{AB} = U^A_{00}|\phi^+\rangle_{AB} = |\phi^+\rangle_{AB}, \\ &\vdots \\ U^A_{1100}|\psi^-\rangle_{AB} &= U^A_{11} \otimes U^A_{00}|\psi^-\rangle_{AB} = U^A_{11}|\psi^-\rangle_{AB} = |\phi^+\rangle_{AB}, \\ U^A_{1101}|\psi^-\rangle_{AB} &= U^A_{11} \otimes U^A_{01}|\psi^-\rangle_{AB} = U^A_{11}|\psi^+\rangle_{AB} = |\phi^-\rangle_{AB}, \\ U^A_{1110}|\psi^-\rangle_{AB} &= U^A_{11} \otimes U^A_{10}|\psi^-\rangle_{AB} = U^A_{11}|\phi^-\rangle_{AB} = |\psi^+\rangle_{AB}, \\ U^A_{1111}|\psi^-\rangle_{AB} &= U^A_{11} \otimes U^A_{11}|\psi^-\rangle_{AB} = U^A_{11}|\phi^+\rangle_{AB} = |\psi^-\rangle_{AB}. \end{aligned}$$

Basing on their outcomes, the 2-extended unitary operations can be clustered into the

following four groups:

$$\begin{aligned}
&U^A_{0000}|\psi^-\rangle_{AB} = U^A_{0101}|\psi^-\rangle_{AB} = U^A_{1010}|\psi^-\rangle_{AB} = U^A_{1111}|\psi^-\rangle_{AB} = U^A_{00}|\psi^-\rangle_{AB} = |\psi^-\rangle_{AB},\\
&U^A_{0001}|\psi^-\rangle_{AB} = U^A_{0100}|\psi^-\rangle_{AB} = U^A_{1011}|\psi^-\rangle_{AB} = U^A_{1110}|\psi^-\rangle_{AB} = U^A_{01}|\psi^-\rangle_{AB} = |\psi^+\rangle_{AB},\\
&U^A_{0010}|\psi^-\rangle_{AB} = U^A_{0111}|\psi^-\rangle_{AB} = U^A_{1000}|\psi^-\rangle_{AB} = U^A_{1101}|\psi^-\rangle_{AB} = U^A_{10}|\psi^-\rangle_{AB} = |\phi^-\rangle_{AB},\\
&U^A_{0011}|\psi^-\rangle_{AB} = U^A_{0110}|\psi^-\rangle_{AB} = U^A_{1001}|\psi^-\rangle_{AB} = U^A_{1100}|\psi^-\rangle_{AB} = U^A_{11}|\psi^-\rangle_{AB} = |\phi^+\rangle_{AB}.
\end{aligned} \tag{5.3}$$

When we simplify the notation, we can write the groups as follows:

$$\begin{aligned}
U_{0000} = U_{0101} = U_{1010} = U_{1111} = U_{00} &= |0\rangle\langle 0| + |1\rangle\langle 1|,\\
U_{0001} = U_{0100} = U_{1011} = U_{1110} = U_{01} &= |0\rangle\langle 0| - |1\rangle\langle 1|,\\
U_{0010} = U_{0111} = U_{1000} = U_{1101} = U_{10} &= |1\rangle\langle 0| + |0\rangle\langle 1|,\\
U_{0011} = U_{0110} = U_{1001} = U_{1100} = U_{11} &= |1\rangle\langle 0| - |0\rangle\langle 1|.
\end{aligned}$$

For 3−extended unitary operations, the following groups can be obtained.

$$\begin{aligned}
U_{000000} = U_{000101} = U_{001010} = U_{001111} = U_{010001} = U_{010100} = U_{011011} = U_{011110}&\\
= U_{100010} = U_{100111} = U_{101000} = U_{101101} = U_{110011} = U_{111001} = U_{110110}&\\
= U_{111100} = U_{0000} = U_{0101} = U_{1010} = U_{1111} = U_{00} = |0\rangle\langle 0| + |1\rangle\langle 1|&
\end{aligned} \tag{5.4}$$

$$\begin{aligned}
U_{000001} = U_{000100} = U_{001011} = U_{010101} = U_{011010} = U_{011111} = U_{100011} = U_{100110}&\\
= U_{101001} = U_{101100} = U_{110010} = U_{110111} = U_{111000} = U_{101100} = U_{111101}&\\
= U_{010000} = U_{1011} = U_{0100} = U_{1110} = U_{0001} = U_{01} = |0\rangle\langle 0| - |1\rangle\langle 1|&
\end{aligned} \tag{5.5}$$

$$\begin{aligned}
U_{000010} = U_{000111} = U_{111110} = U_{001000} = U_{001101} = U_{010011} = U_{010110} = U_{011001}&\\
= U_{011100} = U_{100000} = U_{100101} = U_{101010} = U_{101111} = U_{110001} = U_{110100}&\\
= U_{111011} = U_{1101} = U_{0010} = U_{1000} = U_{0111} = U_{10} = |1\rangle\langle 0| + |0\rangle\langle 1|&
\end{aligned} \tag{5.6}$$

Table 5.1: Collation table for $n = 2$

	Control bits			
BUO	00	01	10	11
U_{00}	U_{0000}	U_{0101}	U_{1010}	U_{1111}
U_{01}	U_{0001}	U_{0100}	U_{1011}	U_{1110}
U_{10}	U_{0010}	U_{0111}	U_{1000}	U_{1101}
U_{11}	U_{0011}	U_{0110}	U_{1001}	U_{1100}

$$\begin{aligned} U_{000011} = U_{000110} = U_{001001} = U_{001100} = U_{010010} = U_{010111} = U_{011000} = U_{011101} \\ = U_{100001} = U_{100100} = U_{101011} = U_{101110} = U_{110000} = U_{110101} = U_{111010} \\ = U_{111111} = U_{0110} = U_{1001} = U_{0011} = U_{1100} = U_{11} = |1\rangle\langle 0| - |0\rangle\langle 1| \end{aligned} \tag{5.7}$$

Definition 1. *Extended Unitary Operations.* [122] Given an integer n, where $n \geq 2$. A unitary operation that satisfies Equations (5.1) and (5.2) is called an n-extended unitary operation.

The following corollaries can be formulated.

Corollary 1. [121, 122] When n-extended unitary operations are used to transform one of the Bell states, then the final outcome falls into one of the groups obtained by using the four basic local unitary operations, where n is an integer and $n \geq 2$.

Corollary 2. [121, 122] Assume that Bell states are transformed using a collection of 2^{2n-2} n-extended unitary operations. Then the obtained outcomes are the same when the Bell states are transformed using the collection of all 2^{2n} $n-$extended unitary operations, where n is an integer and $n \geq 2$.

Definition 2. *Transition operations and ultimate operations.* [121,122] Given an integer

Table 5.2: Collation table for $n = 3$.

	Control bits							
BUO	0000	0001	0010	0011	0100	0101	0110	0111
	1000	1001	1010	1011	1100	1101	1110	1111
U_{00}	U_{000000}	U_{000101}	U_{001010}	U_{001111}	U_{010001}	U_{010100}	U_{011011}	U_{011110}
	U_{100010}	U_{100111}	U_{101000}	U_{101101}	U_{110011}	U_{111001}	U_{110110}	U_{111100}
U_{01}	U_{000001}	U_{000100}	U_{001011}	U_{010101}	U_{011010}	U_{011111}	U_{100011}	U_{100110}
	U_{101001}	U_{101100}	U_{110010}	U_{110111}	U_{111000}	U_{101100}	U_{111101}	U_{010000}
U_{10}	U_{000010}	U_{000111}	U_{111110}	U_{001000}	U_{001101}	U_{010011}	U_{010110}	U_{011001}
	U_{011100}	U_{100000}	U_{100101}	U_{101010}	U_{101111}	U_{110001}	U_{110100}	U_{111011}
U_{11}	U_{000011}	U_{000110}	U_{001001}	U_{001100}	U_{010010}	U_{010111}	U_{011000}	U_{011101}
	U_{100001}	U_{100100}	U_{101011}	U_{101110}	U_{110000}	U_{110101}	U_{111010}	U_{111111}

n; $n \geq 2$. If

$$U^A_{b_{i_1}b_{i_2}\ldots b_{i_{2n-1}}b_{i_{2n}}}|\psi^-\rangle_{AB} = U^A_{b_{j_1}b_{j_2}\ldots b_{j_{2n-3}}b_{j_{2n-2}}}|\psi^-\rangle_{AB},$$

where the sequences $b_{i_1}b_{i_2}\ldots b_{i_{2n-1}}b_{i_{2n}}$ and $b_{j_1}b_{j_2}\ldots b_{j_{2n-3}}b_{j_{2n-2}}$ represent $2n$-bit and $(2n-2)$-bit values, respectively, then

- $U_{b_{j_1}b_{j_2}\ldots b_{j_{2n-3}}b_{j_{2n-2}}}$ is called a *transition operation* of $U_{b_{i_1}b_{i_2}\ldots b_{i_{2n-1}}b_{i_{2n}}}$, and
- $U_{b_{i_1}b_{i_2}\ldots b_{i_{2n-1}}b_{i_{2n}}}$ is called the *ultimate operation* of $U_{b_{j_1}b_{j_2}\ldots b_{j_{2n-3}}b_{j_{2n-2}}}$.

Definition 3. *Control bits.* [121, 122] According to Corollary 2, a collection of 2^{2n-2} $n-$extended unitary operations can be listed (see Tables 5.1 and 5.2) in the order given by their $(2n-2)$-bit values $c_{j_1}c_{j_2}\ldots c_{j_{2n-3}}c_{j_{2n-2}}$ from $\underbrace{0000\cdots0000}_{2n-2}$ to $\underbrace{1111\cdots1111}_{2n-2}$. These

bit values are called the *control bits.*

Definition 4. *Corresponding classical bits.* [121, 122] Given two binary sequences

$$b_{j_1}b_{j_2}\ldots b_{j_{2n-3}}b_{j_{2n-2}} \text{ and } c_{j_1}c_{j_2}\ldots c_{j_{2n-3}}c_{j_{2n-2}}$$

described in Definitions 3 and 4. Then the binary sequence obtained by bitwise XOR operation

$$b_{j_1}b_{j_2}\ldots b_{j_{2n-3}}b_{j_{2n-2}} \oplus c_{j_1}c_{j_2}\ldots c_{j_{2n-3}}c_{j_{2n-2}}$$

is called the sequence of *classical bits.*

To illustrate the notions and definitions, consider 2-extended unitary operations. U_{00} is a transition operation of the ultimate operation U_{0000}. The unitary operations given by Equation (5.3) are $U_{0000}, U_{0101}, U_{1010}, U_{1111}$ with control bits 00, 01, 10, 11. The corresponding classical bits 00, 01, 10, 11 can be obtained by applying XOR to 00 from transition operation U_{00} and control bits 00, 01, 10, 11.

We use an algorithm called *build_tables* (in MATLAB) to generate a collation table for a given $n \geq 2$. The basic idea of the algorithm is as follows. First we generate a collection of 2^{2n} n-extended unitary operations. Next we divide them into four groups of 2^{2n-2} elements in each group (see Corollary 2). Each group creates a single row of the table. The (four) rows are indexed by the basic unitary operations (BUO) U_{00}, U_{01}, U_{10} and U_{11}. They constitute the first column of the table. The pseudocode of the algorithm is given as follows.

Algorithm: build_tables

input: n; **output:** collation table Q

---

for all 2^(2∗n) n−extended unitary operations;

s=cell(1,2^(2∗n));

```
    for i=1:2^(2*n)
        s(i) = {num2str(dec2bin(i-1,2*n))};
        for j=1:n
            str=char(s(i));
            x(j)=bin2dec(str((2*j-1):2*j));
        for j=1:n-1
            [y]=fun(x(j),x(j+1));
            x(j+1)=y;
        z(i)=x(n);
A=sym(zeros(1,2^(2*n-2))); atr=1; B=sym(zeros(1,2^(2*n-2))); btr=1;
C=sym(zeros(1,2^(2*n-2))); ctr=1; D=sym(zeros(1,2^(2*n-2))); dtr=1;
for i=1:2^(2*n)
    if z(i)==0
        A(1,atr)=sym(['U',num2str(dec2bin(i-1,2*n))]);
        atr=atr+1;
    elseif z(i)==1
        B(1,btr)=sym(['U',num2str(dec2bin(i-1,2*n))]);
        btr=btr+1;
    elseif z(i)==2
        C(1,ctr)=sym(['U',num2str(dec2bin(i-1,2*n))]);
        ctr=ctr+1;
    elseif z(i)==3
        D(1,dtr)=sym(['U',num2str(dec2bin(i-1,2*n))]);
        dtr=dtr+1;
P=[A;B;C;D]; M=sym(zeros(4,2^(2*n-2)+1)); for i=1:4
    M(i,1)=sym(['U',num2str(dec2bin(i-1,2))]);
```

```
for j=2: 2^(2*n-2)+1
    M(i,j)=P(i,j-1);
Q=sym(zeros(1,2^(2*n-2)+1));
len=length(num2str(dec2bin(2^(2*n-2)-1))); Q(1,1)='BUO'; for j=2:
2^(2*n-2)+1
    Q(1,j)=sym([num2str(dec2bin(j-2,len))]);
return Q
```

5.3 Hybrid QKD based on extended unitary operations and fountain codes

In this section, we describe the applications of the extended unitary operations and distributed fountain codes used in Chapter 4 to design a hybrid quantum key distribution by dense coding in detail.

5.3.1 Assumptions

We assume that the following facts hold.

1. An adversary Eve is powerful enough to intercept the quantum communication and to perform block processing of quantum data transmitted via the quantum channel. Besides, she can listen to all messages transmitted via the classical channel but cannot modify them (without being detected with a very high probability).

2. Alice and Bob agree beforehand on a binary sequence $S = \{a_1, a_2, \ldots, a_N\}$, where $(a_i \in \{0,1\}; i = 1, \ldots, N)$ using the Bennett-Brassard protocol from [3]. The se-

quence is used as the set of source symbols to produce the corresponding classical bits and the indices of the positions of the particles (see Figure 2.1). Next they design an appropriate fountain code, which is used to prepare classical bits from the source symbols. As Eve does not know the exact number of the source symbols, the number of the source symbols can be quite small, say 50. Even if Eve is able to determine (somehow) the degrees and the positions of the source symbols (see Figure 2.1), she has no information about the generated classical bits. For Eve, the classical bits are just a random sequence, so she has no choice but to guess them one by one. The fact that when the number of generated classical bits is large, such as 200, the probability of a successful guess is 2^{-200}, which is negligible.

3. Alice is using the first two classical bits b_1b_2 to verify the correctness of the following equation

$$U^A_{b_{i_1}b_{i_2}b_{i_3}b_{i_4}\ldots b_{i_{2n-3}}b_{i_{2n-2}}}|\psi^-\rangle_{AB} = U^A_{b_1b_2}|\psi^-\rangle_{AB}$$

Note that the equation holds when Alice chooses an appropriate selection of transition operations. Moreover, the first bit b_1 can be used as control codes, that is, Alice and Bob agree that if "$b_1 = 0$" denotes that measurement base"$\oplus$" should be used and "$b_1 = 1$" denotes that measurement base "$\otimes$" should be used. Consequently, the bits b_1 and b_1b_2 can be used to detect eavesdropping and authenticate Alice's identity respectively, while our proposed protocol works over noisy and lossy quantum channels.

4. Alice and Bob agree that each of the four basic unitary operations corresponds to a particular transition operation for different extended unitary operations in advance. For example, for 3-extended unitary operations, $U_{01} = U_{110111}$.

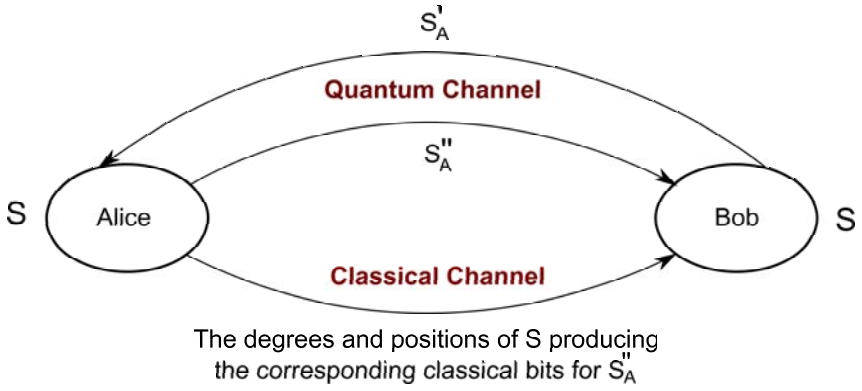

Figure 5.1: The schematic illustration of our hybrid QKD protocol

5.3.2 Hybrid QKD protocol

The steps of our protocol are described below (see Figure 5.1).

Step 1 Bob prepares m (which is determined in an actual situation) EPR pairs and each EPR pair is supposed to be $|\psi^-\rangle_{A_jB_j} = \frac{1}{\sqrt{2}}(|0\rangle_{A_j}|1\rangle_{B_j} - |1\rangle_{A_j}|0\rangle_{B_j})$, where $j = 1, 2, \ldots, m$. All first particles of each EPR pair are to form an ordered photon sequence S_A and all second particles of each EPR pair are to form an ordered photon sequence S_B.

Step 2 Bob keeps the sequence S_B, shuffles at random S_A to obtain a new sequence S'_A and sends it to Alice via a quantum channel.

Step 3 After receiving the sequence S'_A, Alice randomly chooses an ultimate operation for every particle in S'_A, say $U_{b_1b_2b_3b_4\ldots b_{2n-1}b_{2n}}$, $n \geq 2$, (the subscript represents $2n$ bits of key information). Next Alice picks up its transition operation in such a way that Assumption 3 holds. For instance, she selects $U_{b_{i_1}b_{i_2}b_{i_3}b_{i_4}\ldots b_{i_{2n-3}}b_{i_{2n-2}}}$. Knowing the control bits $c_{i_1}c_{i_2}c_{i_3}c_{i_4}\ldots c_{i_{2n-3}}c_{i_{2n-2}}$ from the collation table, she computes the corresponding classical bits

$$b_{i_1}b_{i_2}b_{i_3}b_{i_4}\ldots b_{i_{2n-3}}b_{i_{2n-2}} \oplus c_{i_1}c_{i_2}c_{i_3}c_{i_4}\ldots c_{i_{2n-3}}c_{i_{2n-2}}.$$

Finally, Alice performs the transition operation $U_{b_{i_1}b_{i_2}b_{i_3}b_{i_4}\ldots b_{i_{2n-3}}b_{i_{2n-2}}}$ on particle $A_j; j = 1, 2, \ldots, m$. According to Corollary 1, the state can be changed into one of the following possibilities:

$$\begin{aligned}
U^{A_j}_{b_{i_1}b_{i_2}b_{i_3}b_{i_4}\ldots b_{i_{2n-3}}b_{i_{2n-2}}}|\psi^-\rangle_{A_jB_j} &= U^{A_j}_{00}|\psi^-\rangle_{A_jB_j} = |\psi^-\rangle_{A_jB_j};\\
U^{A_j}_{b_{i_1}b_{i_2}b_{i_3}b_{i_4}\ldots b_{i_{2n-3}}b_{i_{2n-2}}}|\psi^-\rangle_{A_jB_j} &= U^{A_j}_{01}|\psi^-\rangle_{A_jB_j} = |\psi^+\rangle_{A_jB_j};\\
U^{A_j}_{b_{i_1}b_{i_2}b_{i_3}b_{i_4}\ldots b_{i_{2n-3}}b_{i_{2n-2}}}|\psi^-\rangle_{A_jB_j} &= U^{A_j}_{10}|\psi^-\rangle_{A_jB_j} = |\phi^-\rangle_{A_jB_j};\\
U^{A_j}_{b_{i_1}b_{i_2}b_{i_3}b_{i_4}\ldots b_{i_{2n-3}}b_{i_{2n-2}}}|\psi^-\rangle_{A_jB_j} &= U^{A_j}_{11}|\psi^-\rangle_{A_jB_j} = |\phi^+\rangle_{A_jB_j},
\end{aligned}$$

where the superscript A_j denotes the photon on which transition operation is performed.

Step 4 Alice also shuffles at random the encoded S'_A and obtains a new sequence S''_A. The sequence S''_A is sent to Bob via a quantum channel. At the same time, Alice sends the degrees and positions of the set of source symbols S to Bob via a classical channel. The set is used to produce the corresponding classical bits and the indices of positions of the particles in S''_A.

Step 5 Using the received degrees and positions of the set of source symbols S, Bob obtains the right positions of particles in S''_A and the corresponding classical bits. According to them and Assumption 3, Bob can use the same measuring basis as Alice's to measure the corresponding photons in the S''_A and checks with the results of Alice's. If no eavesdropping exists, their results should be completely opposite, i.e., if Alice gets 0 (1), then Bob gets 1 (0). Next knowing S''_A and S_B, Bob can read out the basic local operations corresponding to the Alice transition operations performed. According to Assumption 3, Bob tests whether the subscripts of the basic local operations are equal to the first two bits from the corresponding classical bits. If the test does not hold, Bob aborts the operation. Otherwise, Bob concludes

that Alice is honest and there is no eavesdropper. As Assumptions 3 and 4 hold, Bob knows the transition operations and calculates their subscripts. Then he obtains the control bits by applying XOR to the corresponding classical bits and the subscript of the transition operation (that is, $b_{i_1}b_{i_2}b_{i_3}b_{i_4}\ldots b_{i_{2n-3}}b_{i_{2n-2}}$).

Step 6 Bob produces the table using the algorithm build_tables to obtain the key message.

To illustrate the construction of our protocol and its steps, consider an example. Suppose Alice wants to communicate the key messages 0010, 000111, 110000 to Bob. Note that the messages are equivalent to $U_{0010}, U_{000111}, U_{110000}$ (see Tables 5.1 and 5.2). She needs to perform U_{10}, $U_{1000}(= U_{10})$ (see Eq (5.6)), $U_{1100}(= U_{11})$ (see Eq (5.7)) on three particles $\{p_1, p_2, p_3\}$ from S'_A, which are

$$\begin{aligned} U_{10}^{A_j}|\psi^-\rangle_{A_jB_j} &= |\phi^-\rangle_{A_jB_j}, \\ U_{1000}^{A_j}|\psi^-\rangle_{A_jB_j} &= U_{10}^{A_j}|\psi^-\rangle_{A_jB_j} = |\phi^-\rangle_{A_jB_j}, \\ U_{1100}^{A_j}|\psi^-\rangle_{A_jB_j} &= U_{11}^{A_j}|\psi^-\rangle_{A_jB_j} = |\phi^+\rangle_{A_jB_j}. \end{aligned}$$

Next Alice shuffles $\{p'_1, p'_2, p'_3\}$ and obtains a new sequence $\{p''_1, p''_3, p''_2\}$. The sequence is sent to Bob via a quantum channel. The degrees and positions of source symbols for generating corresponding classical bits 10 (10$\oplus$00), 1001 (0001$\oplus$1000), 1111 (0011$\oplus$1100) and the indices of the correct positions of the three encoded particles are sent to Bob via a classical channel.

After having received the information, Bob first computes the corresponding classical bits 10, 1001, 1111, and the indices of the correct positions of the three encoded particles. According to the right positions of particles in $\{p''_1, p''_3, p''_2\}$ and the first bit from 10, 1001, 1111, Bob can use the same measuring basis as Alice to measure the corresponding photons in the $\{p''_1, p''_3, p''_2\}$ and checks with the results of Alice's. If no eavesdropping exists, their

results should be completely opposite, i.e., if Alice gets 0 (1), then Bob gets 1 (0). Then he uses S_B and $\{p_1'', p_3'', p_2''\}$ and their correct positions to discover the basic unitary operations, and detect whether the bit values from the subscript of the basic unitary operations is equal to 10,10,11 (which are the first two bits from the corresponding classical bits 10, 1001, 1111). If the check holds, he concludes that there is no eavesdropper and Alice is honest. According Assumption 4, Bob can obtain the correct transition operations, then he uses XOR to the subscripts of these transition operations and the corresponding classical bits 10, 1001, 1111 to obtain the control bits. Finally, Bob produces the collation table using the algorithm build_tables to obtain the key messages 0010 000111 110000.

5.3.3 Security analysis of our hybrid QKD protocol

In this section, we analyse the security of our proposed protocol.

We assume that Eve knows the details of Bob's measurement device but she does not know the set of source symbols S, which is agreed beforehand by Alice and Bob using the Bennett-Brassard protocol. Consequently, Eve does not know the indices of the correct positions of the encoded particles and the corresponding classical bits. If Eve wants to eavesdrop, intercept or replace the transmitted photons, she is going to disturb the states when she chooses a wrong measurement basis (the same occurs in the Bennett-Brassard protocol) (also see Step 5). This is easily detected by Bob in terms of the set of source symbols S. Thus, S plays a triple role in our protocol: (1) to authenticate the identity of Alice; (2) to detect eavesdropping; (3) to determine the key message. So our protocol enforces the physical conditions that are necessary to satisfy the no-cloning principle for quantum key distribution protocols. Therefore, our protocol is immune against cheating, man-in-the-middle and intercept-resend attacks.

Note that the particle sequence sent from Bob to Alice and the particle sequence sent from Alice to Bob are shuffled. The original sequences are kept secret by their respective

owners Alice and Bob. As the result, our protocol can effectively resist Trojan horse attacks (the specific proof can be found in [20, 68, 123, 124]) and dense coding attacks (see [120]). Most importantly, S''_A and the degrees and positions of source symbols can be transmitted on-line simultaneously to Bob through quantum and classical channels (see Assumptions 3 and 4). Even if quantum channels are noisy and lossy, Bob can still obtain the key messages.

Here we must stress that, unlike the existing quantum key distribution protocols, where the key messages are determined exclusively by quantum data, our protocol obtains the key messages using simultaneously quantum and classical data. Although in our protocol, a photon carries many more bits of key messages than in other general protocols, the task of Eve to discover them seems to be no easier than guessing them. Alternatively, Eve can (successfully) guess both the transition unitary operations and the corresponding classical bits with the same probability of success 2^{2-2n}.

Note that for the corresponding classical bits, as they are generated by using the pre-shared sequence S between Alice and Bob in a flexible and random way, Eve has no means of decoding the source symbols. As the result, without S, Eve cannot do much better than to randomly guess it with the probability of 2^{2-2n}. Moreover, without the corresponding classical bits, the probability of guessing the transition operation is 2^{2-2n}. Because the probability of guessing the basic unitary operation is $\frac{1}{4}$. So the overall probability of guessing ultimate unitary is 2^{-2n}. For instance if $n = 100$, then the probability of guessing is 2^{-200}.

According to the security analysis of the Bennett-Brasard protocol [3], even if Eve can guess the operation from the classical data, then she obtains no useful information without knowing the correct transition unitary operations. So our protocol is free from the photon number attack [125] and the entangle-measure attack [68].

To emphasize again, the pre-shared sequence is very important in our protocol. We

should also stress that due to the flexible and random way of generating classical data, the number of source symbols that is used to prepare classical data can be very small, and hundreds of blocks are enough for many purposes. Because, unlike in classical cryptography, Eve cannot decode the encoding symbols just from their positions and degrees.

5.3.4 Features of our hybrid QKD protocol

High-capacity – the protocol uses extended unitary operations to make a photon transport as many or as few classical bits of the key message. The number of classical bits depends on a particular need and compares favourably with other protocols where the number is equal to 2 (see [126] for instance). Moreover, the key messages in the protocol not only depend on the transition operations, but also on the corresponding classical bits. The protocol works over noisy and lossy channels. While a photon can carry as many key messages as in [22, 23], the key will be destroyed over noisy and lossy quantum channels. Most importantly, the protocol demonstrates that classical cryptography and quantum cryptography can be combined.

Authentication with physical mechanism – classical key distribution cannot address the problem of eavesdropping. Moreover, the security of classical key distribution is based on intractability assumptions of some computational problems. Some of these problems are proved to be easy on quantum computers. The protocol addresses both the mutual authentications of the parties and eavesdropping detection simultaneously. This is done by combining operations on classical bits with no-cloning principle for quantum bits.

Efficiency – the protocol allows a photon to carry an arbitrary number of classical bits instead of two in most existing protocols. This dramatically improves its efficiency.

Recall that the information-theoretic efficiency is defined in [127] as

$$\eta = \frac{b_s}{q_t + b_t},$$

where b_s is the number of secret bits received by Bob, q_t is the number of qubits used, and b_t is the number of classical bits exchanged between Alice and Bob during the quantum key distribution protocol. The number of classical bits used for the detection of eavesdropping in our protocol is negligible. As shown in [127], for the Bennett-Brasard protocol, $b_s = 0.5$, $q_t = 1$ and $b_t = 1$. Hence, the efficiency of the Bennett-Brasard protocol is 25%. After similar calculations, we can conclude that the efficiency of the EPR protocol is 50% [7]. However, in our protocol, $b_s = 2n$, $q_t = 1$ and $b_t = 2n$, so, the efficiency approaches 100% when $n \to +\infty$.

It is worth noting that the implementation of our protocol requires Bell-state measurement only, which has been implemented in an experiment described in [128]. Due to the use of fountain codes, the classical data is obtained by a simple XOR operation. Clearly, this does not increase the complexity of the protocol.

5.4 Hybrid QSS protocols using extended unitary operations

In this section, we first provide some definitions, and then the corresponding protocols are presented.

Definition 5. [122] A QSS is said to be hybrid only when a sufficient number of quantum participants with their quantum shares and enough classical participants with their classical shares together can recover a secret.

In hybrid quantum secret sharing (HQSS) protocols, the secret shares are composed of quantum and classical shares. We name the former q-shares and the latter c-shares. A

participant who holds only c-shares is called a c-participant and a participant who holds only q-shares is named a q-participant.

5.4.1 $((m+1, n'))$ threshold hybrid QSS protocol

In this subsection, we present a definition and a theorem for hybrid quantum secret sharing based on $((m+1, n'))$ threshold, that is, there are exactly one q-participant and $n'-1$ c-participants. Moreover, only when the q-participant and at least $m \leq n'-1$ c-participants cooperate, the secret can be recovered.

A definition and a theorem based on $((m+1, n'))$ threshold

Definition 6. [122] A HQSS achieving $((m+1, n'))$ among a set of participants $\mathbb{P} = \{P_1, P_2, \ldots, P_{n'}\}$ is said to be dual compressible threshold HQSS if only one q-participant with one q-share and at least m c-participants with c-shares with the size of $\frac{l}{m-1}$ can share a secret cooperatively, where l is the length of the shared secret.

According to definition 6, we can obtain the following theorem. It formalizes the scenario when new participants join in.

Theorem 1. [122] A $((m+1, n'))$-HQSS can be inflated only conformally, i.e., to threshold protocols having the form $((m+\lambda+1, n'+\lambda))$ where λ ($\lambda \in \mathbb{N}$) are all new c-participants.

Proof. As the given conformally-HQSS meets the no-cloning theorem, then obviously does the $((m+\lambda_m+1, n'+\lambda_{n'}))$-HQSS, where $\lambda_m \geq \lambda_{n'} \geq 0$ and $m+\lambda_m+1 \leq n'+\lambda_{n'}$. Moreover, according to Lemma 1 of Ref [69], a restriction of the $((m+\lambda_m+1, n'+\lambda_{n'}))$-QTS by λ c-participants necessarily yields a conformally reduced, $((m+\lambda_m+1-\lambda, n'+\lambda_{n'}-\lambda))$-QTS. The restricted scheme has a different access structure from $((m+1, n'))$ unless $\lambda_m = \lambda_{n'} = \lambda$. Hence, just a conformal inflation of $((m+1, n'))$-HQSS is possible, where it is inflated to a $((m+\lambda+1, n'+\lambda))$-HQSS by the addition of λ c-participants.

The proposed protocol

In this subsection, we propose a dual compressible $((m+1,n'))$ hybrid quantum secret sharing protocol in which we assume that: 1) Bob is the q-participant and $Charlie_1, ...,$ $Charlie_{n'-1}$ are $n'-1$ c-participants. 2) Alice and Bob agree that each of the four basic unitary operations corresponds to a particular transition operation in advance. 3) The shared secret is $s_A = \{s_A^1, s_A^2, \ldots, s_A^l\}, l = 2n, s_A^{i_1} \in \{0,1\}, i_1 = 1,2,\ldots,l$. 4) Classical channels are supposed to be authenticated classical channels.

(1) Bob first prepares $\lambda'+1$ EPR pairs (where λ' is the number that can provide an analysis of the error.) Every EPR pair is supposed to be $|\psi^-\rangle_{h_j t_j} = \frac{1}{\sqrt{2}}(|0\rangle_{h_j}|1\rangle_{t_j} - |1\rangle_{h_j}|0\rangle_{j_j})$. All of the 1st particles of each EPR pair are to form a photon sequence S_H and all of the 2nd particles of each EPR pair are to form a photon sequence S_T. Then Bob keeps the sequence S_H and sends the sequence S_T to Alice via a quantum channel.

(2) After receiving the sequence S_T from Bob, Alice first finds the correct $n-$extended unitary operation in terms of the shared secret $s_A = \{s_A^1, s_A^2, \ldots, s_A^l\}$, which can be determined by the transition operation $U_{b_{i_1}b_{i_2}b_{i_3}b_{i_4}\ldots b_{i_{2n-3}}b_{i_{2n-2}}}$ and control bits. Then Alice performs the transition operation $U_{b_{i_1}b_{i_2}b_{i_3}b_{i_4}\ldots b_{i_{2n-3}}b_{i_{2n-2}}}$ on particle t_j. Under the transition operation, this state can be changed to one of the following states according to (2.21) in Chapter 2:

$$U^{t_j}_{b_{i_1}b_{i_2}b_{i_3}b_{i_4}\ldots b_{i_{2n-3}}b_{i_{2n-2}}}|\psi^-\rangle = U^{t_j}_{00}|\psi^-\rangle = |\psi^-\rangle;$$
$$U^{t_j}_{b_{i_1}b_{i_2}b_{i_3}b_{i_4}\ldots b_{i_{2n-3}}b_{i_{2n-2}}}|\psi^-\rangle = U^{t_j}_{01}|\psi^-\rangle = |\psi^+\rangle;$$
$$U^{t_j}_{b_{i_1}b_{i_2}b_{i_3}b_{i_4}\ldots b_{i_{2n-3}}b_{i_{2n-2}}}|\psi^-\rangle = U^{t_j}_{10}|\psi^-\rangle = |\phi^-\rangle;$$
$$U^{t_j}_{b_{i_1}b_{i_2}b_{i_3}b_{i_4}\ldots b_{i_{2n-3}}b_{i_{2n-2}}}|\psi^-\rangle = U^{t_j}_{11}|\psi^-\rangle = |\phi^+\rangle.$$

where the superscript t_j denotes the photon on which unitary operation is performed.

(3) In order to check eavesdropping in this transmission, Alice randomly chooses some particles from remaining S_T to detect eavesdropping and performs one of the four basic unitary operations on them at random. Then Alice transmits these encoded particles to

Bob while telling him the positions of these particles and the type of the basic unitary operations on them. Bob performs Bell-basis measurement on the encoded particles and their counterparts from S_H. Bob computes the error rates by checking the EPR pairs from which Alice chooses particles. If the error rates of the chosen EPR pairs are lower than the predefined value, Alice transmits the encoded particle t'_j to the q-participant Bob via a quantum channel. Otherwise, Alice continues to check the quantum channel in the same way until the qubit t'_j encoded by the transition operation is sent to Bob safely.

(4) Then Alice allocates the corresponding classical bits obtained by applying XOR to the bit values from the subscript of the transition operation and the control bits with the size of $2n-2$ to the $n'-1$ c-participants $Charlie_1, ..., Charlie_{n'-1}$ through a classical channel in the following way.

(5) Let c denote the corresponding classical bits, Alice allocates c in the way that used in [129], which is as follows:

1. Alice cuts the corresponding classical bits into $m-1$ pieces. These pieces are denoted as $c_1, c_2, \ldots, c_{m-1}$ and $c = c_1 \| c_2 \| \ldots \| c_{m-1}$ where each $c_{i_2}, i_2 = 1, 2, \ldots, m-1$, is the binary representation of a decimal number.

2. Alice allocates the corresponding classical bits in the following way:

2.1 Choose a prime p, $p > max(c_{max}, n'-1)$, where $c_{max} = max\{c_1, c_2, ..., c_{m-1}\}$.

2.2 Randomly and uniformly choose a number $a_1 \in Z_p$ and generate a polynomial: $f_1(x) = a_1 x + c_1$.

2.3 Sample $f_1(x)$ at two points $A_{c_1 1} = f_1(1)$ and $A_{c_1 2} = f_1(2)$ which represent two shares of c_1.

2.4 Do for $2 \leq i_2 \leq (m-1)$.

(a) Generate a polynomial

$f_{i_2}(x) = A_{c_{i_2-1} i_2} x^{i_2} + A_{c_{i_2-1}(i_2-1)} x^{i_2-1} + \cdots + A_{c_{i_2-1}1} x + c_{i_2}$

(b) Sample $f_{i_2}(x)$ to create new shares.

i. If $i_2 < m-1$, sample at i_2+1 points such that

$A_{c_{i_2}1} = f_{i_2}(1)$, $A_{c_{i_2}2} = f_{i_2}(2)$, ..., $A_{c_{i_2}(i_2+1)} = f_{i_2}(i_2+1)$.

ii. If $i_2 = m-1$, sample at $n'-1$ points such that

$A_1 = f_{i_2}(1)$, $A_2 = f_{i_2}(2)$, ..., $A_{n'-1} = f_{i_2}(n'-1)$

(c) Delete old shares: $A_{c_{i_2-1}1}, \cdots, A_{c_{i_2-1}i_2}$.

2.5 The final $n'-1$ shares are given by (i_2, A_{i_2}), for $1 \leq i_2 \leq n'-1$.

(6) A group of the q-participant and any m c-participants together are able to reconstruct the secret. First, the q-participant measures (h_j, t'_j) to obtain the transition operation in terms of their agreement. Then, the m c-participants interpolate their m shares (i_2, A_{i_2}) to generate the polynomial of degree $m-1$ and thus obtain the corresponding classical bits.

$f(x) = c_{\alpha_{m-1}} x^{m-1} + c_{\alpha_{m-2}} x^{m-2} + \cdots + c_{\alpha_1} x + c_{m-1}$.

Hence, the control bits can be obtained by applying the XOR operation on the corresponding classical bits and bit values knowing from the subscript of the transition operation. Finally, they can recover the ultimate operation by checking the algorithm build_table in Appendix A, that is, Alice's secret $s_A = \{s_A^1, s_A^2, \ldots, s_A^l\}$.

It is worth noting that the dual compressible threshold hybrid quantum secret sharing protocol can be easily converted into a $((m+1, n'))$ threshold hybrid quantum multi-secret sharing protocol. But $c_1, c_2, ..., c_{m-1}$ should be replaced with $s_1, s_2, \ldots, s_{m-1}$. The rest of the processes remain unchanged.

5.4.2 Hybrid QSS protocol based on adversary structure

In this section, a dual compressible hybrid quantum secret sharing protocol based on adversary structure is presented, in which all participants from any minimal qualified set can recover the secret.

Definitions and a theorem based on access structure and adversary structure

Let $\mathbb{P} = \{P_1, P_2, \ldots, P_{n'}\}$ be the set of participants. Let $\alpha \subseteq \mathbb{P}$. α is called a qualified set if the q-participant and any designated c-participants in α together can recover the secret; otherwise, it is called an unqualified set. An access structure, denoted by Γ, is a collection of qualified subsets of $\mathbb{P}$ satisfying the monotone ascending property: for any $A' \in \Gamma$ and $A \in 2^{\mathbb{P}}$, $A' \subseteq A$ implies $A \in \Gamma$. An adversary structure, denoted by $\mathbb{A}$, is a collection of unqualified subsets of $\mathbb{P}$ satisfying the monotone descending property: for any $A' \in \mathbb{A}$ and $A \in 2^{\mathbb{P}}, A \subseteq A'$ implies $A \in \mathbb{A}$.

By the definition of qualified and unqualified subsets, for any given access structure Γ and adversary structure $\mathbb{A}$ over $\mathbb{P}$, we have that $\Gamma \cap \mathbb{A} = \emptyset$. Because of the monotone properties, for any access structure Γ and any adversary structure $\mathbb{A}$, it is sufficient to consider the minimum access structure:

$$\Gamma_{min} = \{A \in \Gamma \mid \forall B \subset A \Rightarrow B \notin \Gamma\},$$

and the maximum adversary structure:

$$\mathbb{A}_{max} = \{B \in \mathbb{A} \mid \forall A \supset B \Rightarrow A \notin \mathbb{A}\}.$$

In this thesis, we consider the complete situation, that is $\mathbb{A} \bigcup \Gamma = 2^{\mathbb{P}}$ [130].

Based on the above-mentioned concepts, Definition 3 and Theorem 2 are presented as follows.

Definition 7. [122] A HQSS achieving the minimum access structure $\Gamma_{min} = \{\alpha_1, \alpha_2, \ldots, \alpha_{r_1}\}$ (where $\alpha_{j_1}, j_1 = 1, 2, \ldots, r_1$ is a minimal qualified set of participants) with its maximum adversary structure $\mathbb{A}_{max} = \{\beta_1, \beta_2, \ldots, \beta_{r_2}\}$ (where $\beta_{j_2}, j_2 = 1, 2, \ldots, r_2$ is a maximal unqualified set of participants) among a set of participants $\mathbb{P} = \{P_1, P_2, \ldots, P_{n'}\}$ is said to be dual compressible if only one q-participant with one q-share and all c-participants from $\alpha_{j_1}(j_1 = 1, 2, \ldots, r_1)$ who hold the c-shares with the size of $\frac{t-2}{r_2}$ can share a secret cooperatively.

According to definition 7, we can obtain the following theorem 2. It formalizes the scenario when new participants join in.

Theorem 2. [122] A HQSS achieving the minimum access structure $\Gamma_{min} = \{\alpha_1, \alpha_2, \ldots, \alpha_{r_1}\}$ (where $\alpha_{j_1}, j_1 = 1, 2, \ldots, r_1$, is a minimal qualified set of participants.) among a set of participants $\mathbb{P} = \{P_1, P_2, \ldots, P_{n'}\}$ can be always inflatable.

Proof. Suppose that m new c-participants $P_{n'+1}, P_{n'+2}, \ldots, P_{n'+m}$ are added into $\mathbb{P}$ to form $\mathbb{P}' = \{P_1, P_2, \ldots, P_{n'+m}\}$. The new minimum access structure $\Gamma'_{min} = \{\alpha'_1, \alpha'_2, \ldots, \alpha'_{r_1}\}$ can be achieved by adding any new c-participants to any of the $\alpha_{j_1}, j_1 = 1, 2, \ldots, r_1$. The corresponding classical bits are shared among $n' + m - 1$ c-participants in terms of the classical scheme performing Γ'. To recover the secret, the q-participant from $\alpha'_{j_1}, j_1 = 1, 2, \ldots, r_1$ can obtain the transition operation and all the c-participants from $\alpha'_{j_1}, j_1 = 1, 2, \ldots, r_1$ can reconstruct the corresponding classical bits. The shared secret is obtained through the q-participant's and c-participants' collaboration. Hence, the new scheme HQSS (Γ') is an inflatable one of the given scheme HQSS (Γ).

Notations

In this dual compressible hybrid quantum secret sharing, we use the following notations.

Alice: a trusted dealer who wants to share the corresponding classical bits among the c-participants;

$\mathbb{P}$: $\mathbb{P} = \{P_1, P_2, \ldots, P_{n'}\}$ is the set of all the participants;

c: the corresponding shared classical bits;

Γ_{min}: $\Gamma_{min} = \{\alpha_1, \alpha_2, \ldots, \alpha_{r_1}\}$ is the minimum access structure corresponding to c ;

$\mathbb{A}_{max}$: $\mathbb{A}_{max} = \{\beta_1, \beta_2, \ldots, \beta_{r_2}\}$ is the maximum adversary structure corresponding to c;

$c_1, c_2, \ldots, c_{r_2}$: the pieces of c;

r_2: $r_2 = |\mathbb{A}_{max}|$, that is, the number of elements in $\mathbb{A}_{max}$.

The Alice's phase

The first three steps (1)-(3) in the protocol are the same as those in (section 5.3.1) as they just involve Alice and Bob. Steps (4)-(6) are similar that used in [130], which is as follows:

(4) Alice selects H: a suitable strongly collision-free hash function, which takes as input a binary string of an arbitrary length, and produces as output a binary string of a fixed length q, where q is the length of the pieces of the corresponding classical bits, and computes $H(c_{i_3})$.

(5) Alice computes:

$x_1 = c_1 \oplus H(c_2)$, $x_2 = c_2 \oplus H(c_3)$, ..., $x_{r_2-1} = c_{r_2-1} \oplus H(c_{r_2})$, $x_{r_2} = H(x_1) \oplus H(x_2) \oplus \ldots \oplus H(x_{r_2-1}) \oplus c_{r_2}$.

Then Alice generates $n' - 1$ identical arrays $H_{i_3} = \{x_1, x_2, \ldots, x_{r_2}\}$, for $i_3 = 1, 2, \ldots, n' - 1$.

(6) Alice allocates c-shares in such a way that each participant in β_1 has no secret share x_1, each participant in β_2 has no secret share x_2, ..., and each participant in β_{r_2} has no secret share x_{r_2}. Then Alice distributes the remaining c-shares in H_{i_3} to the c-participant P_{i_3}, for $i_3 = 1, 2, \ldots, n' - 1$, secretly.

Note that even if the number of participants is large, it is still possible to obtain the minimum access structure and the maximum adversary structure using linear codes (see [131]).

The recovery phase

Suppose a group of participants from α_{j_1} want to recover the secret.

C-participants from α_{j_1} delete the redundant x_{i_3}, for $i_3 = 1, 2, \ldots, r_2$ and compute:

$c_{r_2} = H(x_1) \oplus H(x_2) \oplus \ldots \oplus H(x_{r_2-1}) \oplus x_{r_2}$, $c_{r_2-1} = x_{r-1} \oplus H(c_{r_2})$, ..., $c_2 = x_2 \oplus H(c_3)$, $c_1 = x_1 \oplus H(c_2)$.

So, the c-participants from α_{j_1} recover $c = c_1 \parallel c_2 \parallel \cdots \parallel c_{r_2-1} \parallel c_{r_2}$ while the q-participant obtains the transition operation by measuring (h_j, t'_j). Consequently, they can recover the ultimate operation by checking the algorithm build_table in Appendix A, that is, Alice's secret $s_A = \{s_A^1, s_A^2, \ldots, s_A^l\}$.

Likewise, it is worth noting that the dual compressible quantum secret sharing protocol based on adversary structure can be easily converted into a hybrid quantum multi-secret sharing protocol based on on adversary structure. The protocol can be realized by just regarding every piece of classical bits of a secret in section 5.3.1 as the classical bits of every single secret.

5.4.3 The security analysis and the features of hybrid QSS protocols

As is known, on the one hand, classical secret sharing protocols cannot address the problem of eavesdropping and their security is guaranteed by the difficulty of computation, which might be susceptible to the strong ability of quantum computation. Fortunately, quantum secret sharing can address this issue and eavesdropping detection simultaneously. On the other hand, quantum data is much more prohibitive and difficult to cope with than classical data. Hence, we have proposed two dual compressible hybrid quantum secret sharing protocols, which make full use of the advantages of classical secret sharing protocols and quantum secret sharing protocols. These protocols can be surprisingly easy to implement because they just need to perform the correct transition operation on an EPR pair and to allocate the corresponding classical messages. Though collation tables are required in our protocols, this is easily achieved by an algorithm.

Recursion is used to implement dual compressible hybrid quantum secret sharing based

on $((m+1, n'))$ threshold and adversary structure. That is to say, just one q-participant with q-shares and at least m c-participants (or all participants from any minimal qualified set with c-shares with the size of $\frac{l-2}{r_2}$) with c-shares with the size of $\frac{l-2}{m-1}$ can share one secret in a secure way. The obvious merit of the protocols is that they can curtail the cost of generating, transmitting and storing EPR pairs and classical bits. Moreover, a hybrid quantum multi-secret sharing protocol can be designed in the same way, i.e., one q-participant and any m or over m c-participants can share $m-1$ secrets simultaneously.

In our hybrid protocols the shared secret is determined by classical data and quantum data simultaneously, that is, the shared secret cannot be obtained by either classical data or quantum data alone. On the other hand, in our hybrid protocols, it is much simpler and faster to allocate shares without weakening the security in contrast to quantum secret sharing. Compared with the existing hybrid quantum secret sharing protocols [24,69,70], not only does the number of also the number of particles needed and the size of c-shares reduce. Most importantly, even if Eve is able to obtain all the classical obtain all the classical messages, our proposed protocols are still secure. Because in our protocols, the c-participants do not know the used transition operations by Alice. Then, if these c-participants want to obtain the secret, they have to guess the used transition operation and the basic unitary operation. The probability of a successful guess is $\frac{1}{2^{2n-2}} \times \frac{1}{2^2} = \frac{1}{2^{2n}}$ which is in fact equal to the probability of conventional quantum secret sharing protocols. Moreover, the distribution of q-shares is the same as that in quantum secret sharing protocols. That is to say, the security of transmitting one particle can match that of n particles. Therefore, when conventional quantum secret sharing protocols are secure, our proposed hybrid quantum secret sharing protocols are also secure.

Moreover, we present a table (see Tab. 5.3) to compare the performance among Nascimento *et al.*'s [24], Singh *et al.*'s [69], Fortescue *et al.*'s [70] and our proposed protocols.

Table 5.3: Performance comparison of HQSS.

Protocols	Nascimento *et al.*'s [24]	Singh *et al.*'s [69]	Fortescue *et al.*'s [70]	Our protocol [50]
Threshold	Yes	Yes	Yes	Yes
Adversary structure	No	No	No	Yes
Access structure	Yes	Yes	No	No
Imperfect "ramp"	No	No	Yes	No
Termed inflation	No	Yes	No	Yes
dual compression	No	No	Yes	Yes
Twin-thresholding	No	Yes	No	Yes
one quantum participant	Yes	No	No	Yes
one quantum share	Yes	No	No	Yes

5.5 Summary

Distributed fountain codes and extended unitary operations can be used to perform efficient, authenticated and high-capacity hybrid quantum key distribution with the present technology. It is worth mentioning that the discovery of security of determining key distribution by transition operations and corresponding classical bits simultaneously and the repeated use of a short sequence of source symbols to generate classical bits is crucial. It enables quantum key distribution to be achieved in a more secure, efficient and practical way. Also, based on the extended unitary operations, two dual compressible hybrid quantum secret sharing protocols have been proposed. Compared with the other proposed hybrid quantum secret sharing protocols, the main contributions of the hybrid protocols are that: 1) Not only can they reduce the number of q-participants, but also the number of particles and the size of c-shares, which is a very important issue in hybrid quantum

secret sharing. 2) The corresponding classical bits and the transition operations that are used to determine the shared secret jointly do not have a direct relationship, which, to some extent, makes our protocols more secure. 3) The prepared EPR pairs can be reused in our hybrid quantum secret sharing protocols. 4) Our protocols are more feasible to implement in a practical setting.

Chapter 6

Conclusions and Future Work

This chapter provides a summary of the main contributions of the thesis and discusses several future research directions.

6.1 Summary of the contributions

As quantum computers develop, the requirements for secure protocols are becoming more and more demanding. As a result, it is necessary and significant to make adjustments on the existing secure models. In this thesis, the research work has concentrated on the design and analysis quantum key distribution protocols. We have studied high-capacity quantum key distribution and quantum secret sharing of secure direct communication, HQKD and HQSS, and have obtained the following results.

In Chapter 3, with the relationship among Lucas numbers, Chebyshev maps and k-Chebyshev maps observed, we have found that a more efficient high-capacity QKD protocol can be achieved based on Simon et al.'s work [22]. To be exact, we encode key messages with the Chebyshev-map values corresponding to Lucas numbers, and then use k-Chebyshev maps to achieve consecutive and flexible key expansion, and apply the locking of classical information and fountain codes to privacy amplification to solve the

security of the exchange of classical information via the classical channel. Consequently, our lower-dimensional high-capacity protocol can be also without the limitation of orbital angular momentum and down-conversion bandwidths, and meet the requirements for longer distances and lower error rates simultaneously. In Chapter 3, we have also studied high-capacity QKD protocols in noisy settings. We have extended the four basic unitary operations to sixteen 2-extended unitary operations based on collective noise. With sixteen 2-extended unitary operations based on collective noises used, we proposed a high-capacity QKD protocol against a collective-dephasing noise and one against a collective-rotation noise. Both are easier to implement and have higher qubit efficiency compared to those in [40, 41, 43, 44, 46] and [42, 45].

Furthermore, we studied QSS, which is the generalization of quantum key distribution to more than two parties in Chapter 4. We mainly focus on quantum secret sharing protocol of secure direct communication. In a detailed analysis in 1999, Cleve et al. pointed out that it was unlikely for (2,3) threshold quantum state sharing to be achieved. However, in 2001, Tyc and Sanders [80] showed explicitly how to achieve a continuous variable (2,3) threshold quantum state sharing protocol. In 2002, Lance *et al.* [81] extended Tyc and Sanders' protocol by utilizing an electro-optic feedforward technique and further proposed two protocols. When recurrence is used, we have proved that, a (2,3) discrete variable threshold quantum secret sharing protocol of secure direct communication can also be achieved using the same devices as in BB84. Besides, we use the idea of distributed fountain codes to let participants know the positions of inserted nonorthogonal state particles and the control codes for the implementation of no-cloning principle for eavesdropping-check and authentication. The proposed protocol is inherently immune to Trojan horse attacks. Moreover, every particle can on average carry nearly up to 1.5-bit messages because the shares of smaller secret pieces are all accumulated into the shares of the largest secret piece, and Bobs can detect eavesdropping by themselves without

exchanging classical messages due to the generated control codes, thereby enhancing the efficiency of quantum secret sharing. Moreover, we have generalized the (2,3) discrete variable threshold quantum secret sharing protocol of secure direct communication to non-threshold quantum secret sharing protocol. The proposed protocol uses the properties of fountain codes to allow a realization of the physical conditions necessary for the implementation of no-cloning principle for eavesdropping-check and authentication.

Finally, with applications of n-extended unitary operations used, a hybrid quantum key distribution and two hybrid quantum secret sharing protocols have been proposed in Chapter 5. Distributed fountain codes and extended unitary operations can be used to perform efficient, authenticated and high-capacity hybrid quantum key distribution with the present technology. It is worth mentioning that the discovery of security of determining key distribution by transition operations and corresponding classical bits simultaneously and repeated use of a short sequence of source symbols to generate classical bits is crucial. It enables quantum key distribution to be achieved in a more secure, efficient and practical way. Also, based on the extended unitary operations, two dual compressible hybrid quantum secret sharing protocols have been proposed. Compared with the hybrid quantum secret sharing protocols proposed in [24, 69, 70], the main contributions of the hybrid protocols are that: 1) Not only can they reduce the number of q-participants, but also the number of particles and the size of c-shares, which is a very important issue in hybrid quantum secret sharing. 2) The corresponding classical bits and the transition operations that are used to determine the shared secret jointly do not have a direct relationship, which, to some extent, makes our protocols more secure. 3) The prepared EPR pairs can be reused in our hybrid quantum secret sharing protocols. 4) Our protocols are more feasible to implement in a practical setting.

6.2 Future work

In the future, we plan to work towards: enhancing the performance of practical quantum key distribution protocols. Further improvements, both in key rate, message capacity rate and secure transmission distances, are required for most applications.

In order to defend against the possible attacks from quantum computers, quantum cryptography has been proposed [3, 6–21]. However, it is hard and expensive to prepare single photons and entangled states and quantum information is fragile (here it means that it is easy to be broken physically) in nature. We think that high-dimensional and hybrid ways may provide two good solutions. Though there are many high-dimensional QKD protocols have been proposed, their efficiency is not high. This is because that Alice and Bob choose polarisation bases for each photon with equal probability randomly and independently, which causes Alice and Bob to use different bases half of the times; and all the accepted data are put together and a single error rate is computed.

However, Lo *et al.* [132] (originally submitted to arXiv on 14 Nov 2000 (v1), last revised 8 Jul 2005 (this version, v3)) have shown that the efficiency of the BB84 protocol can be asymptotically close to 100% by choosing the rectilinear basis and diagonal basis with substantially different probabilities. In 2002, Xue *et al.* [133] proposed a two-user QKD protocol with three nonorthogonal states, which incorporates Lo *et al.*'s idea. The efficiency of Xue *et al.*'s protocol can also be asymptotically close to 100%. In their two-user protocol (in which there are three participants, i.e., the center Alice and the users Bob and Carol), Alice prepares a sequence of photon pairs that are in one of the three states $|BC\rangle_1$, $|BC\rangle_2$, $|BC\rangle_3$ with probabilities of $\frac{1-\epsilon_1}{2}$, $\frac{1-\epsilon_1}{2}$ and ϵ_1 respectively, and Bob and Carol choose two types of measurements with probabilities of $1-\epsilon_2$ and ϵ_2 respectively. Moreover, Xue *et al.* have shown that their protocol is secure using similar arguments to those applied by Shor and Preskill [134] in their proof of security of the modified version of Lo *et al.*'s protocol (see [135]).

In our future work, we will consider an efficient and flexible lower-dimensional high-capacity quantum key distribution and controllable quantum private queries based on [22]. In such protocols, entangled particles that are produced using the recurrence relation $L_{n+2} = F_{n+1} + F_{n-1}$ are used for key generation or key query with the probability of $1-\epsilon_1$ and Chebyshev-map values corresponding to Lucas numbers for key expansion. Entangled particles that are produced using the recurrence relation $F_{n+2} = F_{n+1} + F_n$ are used for eavesdropping detection with the probability of ϵ_1. Alice and Bob also choose two types of measurements with probabilities of $1-\epsilon_2$ and ϵ_2, respectively. Also, it may be worthwhile to design a pseudo-random sequence generator, which can allow Alice and Bob to produce the corresponding classical bits with the pre-shared sequence synchronously and make the classical channel unnecessary in sending quantum data in hybrid QKD protocols.

Bibliography

[1] P. 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, Nov. 20-22,1994 IEEE Computer Society Press, pp. 124-134

[2] N. Gershenfeld, I. L. Chuang, Quantum computing with molecules, Scientific American, 66-71, 1998.

[3] C. H. Bennett, and G. Brassard, Quantum cryptography: public-key distribution and coin tossing, Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing (Bangalore, India) (New York: IEEE) 175-179, 1984.

[4] C. H. Bennett, G. Brassard, S. Breidbard, and S. Wiesner, Quantum cryptography or unforgeable subway tokens, Advances in Cryptology: Proceedings of Crypto 82, 267-275, 1982.

[5] W. Tittel, H. Zbinden, and N. Gisin, Experimental demonstration of quantum secret sharing, Phys. Rev. A., 63, 042301-042306, 2001.

[6] C. H. Bennett, Quantum cryptography using any two nonorthogonal states, Phys. Rev. Lett., 68, 3121-3124, 1992.

[7] A. K. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett., 67, 661-663, 1991.

[8] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod Phys., 74, 145-190, 2002.

[9] L. Goldenberg, and L. Vaidman, Counterfactual quantum key distribution without polarization encoding, Phys. Rev. Lett., 75, 1239-1241, 1995.

[10] L. Allen, M. W. Beijersbergen, R. J. C. Spreeuw, and J. P. Woerdman, Orbital angular momentum of light and the transformation of Laguerre-Gaussian laser modes, Phys. Rev. A., 45, 8185, 1992.

[11] P. G. Kwiat, A. M. Steinberg, and R. Y. Chiao, High-visibility interference in a Bell-inequality experiment for energy and time, Phys. Rev. A., 47, 2472-2475, 1993.

[12] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden, Pulsed energy-time entangled twin-photon source for quantum communication, Phys. Rev. Lett., 82, 2594-2597, 1999.

[13] G. Gibson, J. Courtial, M. J. Padgett, M. Vasnetsov, V. Pas'ko, S. M. Barnett, and S. Franke-Arnold, Free-space information transfer using light beams carrying orbital angular momentum, Opt Express., 12, 5448, 2004.

[14] A. Mair, I. A. Vazir, G. Weihs, and A. Zeilinger, Entanglement of the orbital angular momentum states of photons, Nature., 412, 313, 2001.

[15] G. Molina-Terriza, J. P. Torres, and L. Torner, Management of the angular momentum of light: preparation of photons in multidimensional vector states of angular momentum, Phys. Rev. Lett., 88, 013601, 2002.

[16] H. K. Lau, and C. Weedbrook, Quantum secret sharing with continuous-variable cluster states, Phys. Rev. A., 88, 042313, 2013.

[17] R. Cleve, D. Gottesman, and H. K. Lo, How to share a quantunm secrte, Phys. Rev. Lett., 83, 648-652, 1999.

[18] K. *Boström*, and T. Felbinger, Deterministic secure direct communication using entanglement, Phys. Rev. Lett., 89-93, 2002.

[19] Z. C. Wei, W. L. Wang, Z. Zhang, M. Gao, Z. Ma, and X. F. Ma, Decoy-state quantum key distribution with biased basis choice, Science Report, 2453, 1-3, 2013.

[20] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Trojan horse attacks on quantum key distribution systems, Phys. Rev. A., 73, 022320, 2006.

[21] A. Vaziri, G. Weihs, and A. Zeilinger, Experimental two-photon, three-dimensional entanglement for quantum communication, Phys. Rev. Lett., 89, 240401, 2002.

[22] D. S. Simon, N. Lawrence, J. Trevino, L. DalNegro, and A. V. Sergienko, High-capacity quantum Fibonacci coding for key distribution, Phys. Rev. A., 87, 032312, 2013.

[23] D. S. Simon, and A. V. Sergienko, High capacity quantum key distribution via hyperentangled degrees of freedom, New J. Phys., 16, 063052, 2014.

[24] A. C. A. Nascimento, J. Mueller-Quade, and H. Imai, Improving quantum secret-sharing schemes, Phys. Rev. A., 64, 042311-042515, 2001.

[25] A. Tanaka, W. Maeda, S. Takahashi, A. Tajima, and A. Tomita, Ensuring quality of shared keys through quantum key distribution for practical application, IEEE J. Sel. Top. Quant. Electron., 15, 1622-1629, 2009.

[26] A. Tajima, A. Tanaka, W. Maeda, S. Takahashi, and A. Tomita, Practical quantum cryptosystem for metro area applications, IEEE J. Sel. Top. Quant. Electron., 13, 1031-1038, 2007.

[27] S. Wiesner, Conjugate Coding, Sigact News, 15, (1), 78-88, 1983.

[28] D. Mayers, Unconditional security in quantum cryptography, Journal of the ACM., 48(3), 351406, 2001.

[29] P. W. Shor, and J. Preskill, Simple proof of security of the BB84 quantum key distribution protocol, Phys. Rev. Lett., 85(2), 441, 2000.

[30] X. F. Ma, Quantum cryptography: from theory to practice, Ph.D thesis, 2008, 1-157.

[31] X. B. Wang, A decoy-state protocol for quantum cryptography with 4 intensities of coherent states, Phys. Rev. A., 72, 012322, 2005.

[32] L. Masanes, S. Pironio, A. Acin, Secure device-independent quantum key distribution with causally independent measurement devices, Nature Communications, 2010, 238.

[33] A. Muller, J. Breguet, and N. Gisin, Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km, Europhys. Lett., 23(6), 383-388, 1993.

[34] T. Inagaki, N. Matsuda, O. Tadanaga, Y. Nishida, M. Asobe, and H. Takesue, Long distance distribution of entangled photon pair over 300 km of Fiber, CLEO: QELS Fundamental Science San Jose, California United States June 9-14, 2013 ISBN: 978-1-55752-972-5 Quantum Key Distribution (QTu2C).

[35] G. M. Nikolopoulos, K. S. Ranade, and G. Alber, Error tolerance of two-basis quantum key-distribution protocols using qudits and two-way classical communication, Phys. Rev. A., 73, 032325, 2006.

[36] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Security of quantum key distribution using d-level systems, Phys. Rev. Lett., 88, 127902, 2002.

[37] J. T. Barreiro, and P. G. Kwiat, Hyperentanglement for advanced quantum communication. 7092. Proceedings-SPIE The International Society for Optical Engineering; 7092P (2008); 6th, Quantum communications and quantum imaging conference.

[38] M. Mafu, A. Dudley, S. Goyal, D. Giovannini, M. McLaren, and M. j. Padgett, Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases, Phys. Rev. A., 88, 032305, 2013.

[39] R. W. Boyd, A. Jha, M. Malik, C. O'Sullivan, B. Rodenburg, and J. D. Gauthier, Quantum key distribution in a high-dimensional state space: exploiting the transverse degree of freedom of the photon, Proc. SPIE 7948, Advances in Photonics of Quantum Computing, Memory, and Communication IV, 79480L, February 11, 2011.

[40] X. H. Li, F. G. Deng, and H. Y. Zhou, Efficient quantum key distribution over a collective noise channel, Phys. Rev. A., 78, 022321, 2008.

[41] J. C. Boileau, D. Gottesman, R. Laflamme, D. Poulin, and R. W. Spekkens, Robust polarization-based quantum key distribution over a collective-noise channel, Phys. Rev. Lett., 92, 017901, 2004.

[42] C. Y. Li, and Y. S. Li, Fault-tolerate quantum key distribution over a collective-noise channel, Int. J. Quantum Inf., 8(7), 1101-1109, 2010.

[43] Y. Sun, Q. Y. Wen, F. Gao, and F. C. Zhu, Robust variations of the Bennett-Brassard 1984 protocol against collective noise, Phys. Rev. A., 80, 032321, 2009.

[44] X. M. Xiu, L. Dong, Y. J. Gao, and F. Chi, Quantum key distribution protocols with six-photon states against collective noise, Opt. Commun., 282, 4171-4174, 2009.

[45] X. H. Li, B. K. Zhao, Y. B. Sheng, F. G. Deng, and H. Y. Zhou, Fault tolerant quantum key distribution based on quantum dense coding with collective noise, Int. J. Quantum Inf., 7, 1479-1489, 2009.

[46] C. W. Yang, and T. Hwang, Fault tolerant quantum key distributions using entanglement swapping of GHZ states over collective-noise channels, Quantum Inf Process., 12, 3207-3222, 2013.

[47] W. Huang, Q. Y. Wen, B. Liu, and F. Gao, General method for constructing unitary operations for protocols with collective detection and new QKD protocols against collective noise, http://arxiv.org/abs/1210.1332v2 2012.

[48] X. J. Duan, R. Zhou, and X. Li, Efficient fault-tolerant quantum secret sharing over two collective channel, International Journal of Quantum Inf., 8, 1347-1354, 2010.

[49] Z. Zhao, Y. A. Chen, A. N. Zhang, T. Yang, H. J. Briege, and J. W. Pan, Experimental demonstration of five-photon entanglement and open-destination teleportation, Nature., 430, 54-58, 2004.

[50] H. Lai, M. A. Orgun, J. H. Xiao, and L. Y. Xue, Fault-tolerant high-capacity quantum key distribution over a collective-noise channel, Quantum Inf Process., 13, 1523-1535, 2014.

[51] M. Hillery, V. *Bužek*, and A. Berthiaume, Quantum secret sharing, Phys. Rev. A., 59(3), 1829-1834 1999.

[52] A. Shamir, How to share a secret, Commun. ACM., 22(11), 612-613, 1979.

[53] G. R. Blakley, Safeguarding cryptographic keys, In: Proceedings of National Computer Conference, vol. 48, pp. 313-317. AFI-PS Press, Montvale, NJ, 1979.

[54] A. Karlsson, M. Koashi, and N. Imoto, Quantum entanlement for secret sharing and secret splitting, Phys. Rev. A., 59, 162-168, 1999.

[55] S. Bandyopadhyay, Teleportation and secret sharing with pure entangled states, Phys. Rev. A., 62, 012308-012320, 2000

[56] D. Gottesman: Theory of quantum secret sharing, Phys. Rev. A., 61, 042311, 2000.

[57] L. Xiao, G. L. Long, F. G. Deng, and J. W. Pan, Efficient multiparty quantum-secret-sharing schemes, Phys. Rev. A., 69, 052307-052311, 2004.

[58] Z. J. Zhang, Y. Li, and Z. X. Man, Multiparty quantum secret sharing, Phys. Rev. A., 71, 044301-044304, 2005.

[59] Y. Tokunaga, T. Okamoto, and N. Imoto, Threshold quantum cryptography, Phys. Rev. A., 71, 012314-012323, 2005.

[60] Z. J. Zhang, and Z. X. Man, Multiparty quantum secret sharing of classical messages based on entanglement swapping, Phys. Rev. A., 72, 022303-022306, 2005.

[61] J. Benaloh, and J. Leichter, Generalized secret sharing and monotone functions, Proc. Crypto 1988, 27, 1990.

[62] Q. Lin, W. H. Chan, and D. Y. Long, Semiquantum secret sharing using entangled states, Phys. Rev. A., 82, 022303-022308, 2010.

[63] V. Gheorghiu, Generalized semiquantum secret sharing schemes, Phys. Rev. A., 85, 052309-052319, 2012.

[64] P. Sarvepalli, and R. Raussendorf, Matroids and quantum-secret-sharing scheme, Phys. Rev. A., 81, 052333-052341, 2010.

[65] M. H. Dehkordi, and E. Fattahi, Threshold quantum secret sharing between multi-party and multiparty using Greenberger-Horne-Zeilinger, Quantum Inf Process., 12, 1299-1306, 2013.

[66] N. B. An, Efficient, effivtive and flexible multiparty quantum secret sharing, Commu in Phys., 2, 65-74, 2008.

[67] Y. G. Yang, X. Jia, H. Y. Wang, and H. Zhang, Verifiable quantum (k, n) threshold secret sharing, Quantum Inf Process., 11, 1619-1625, 2012.

[68] J. Lin, and T. Hwang, New circular quantum secret sharing for remote agents, Quantum Inf Process., 12, 685-697, 2013.

[69] S. D. Singh, and R. Srikanth, Generalized quantum secret sharing, Phys. Rev. A., 71, 012328-012334, 2005.

[70] B. Fortescue, and G. Gour, Reducing the quantum communication cost of quantum secret sharing, IEEE Trans on Inf Theory., 58(10), 6659-6666, 2012.

[71] Y. H. Chou, C. Y. Chen, R. K. Fan, H. C. Chao, and F. J. Lin, Enhanced multiparty quantum secret sharing of classical messages by using engtanglement swapping, IET. 6(2), 84-92, 2011.

[72] Y. H. Chou, S. M. Chen, Y. T. Lin, C. Y. Chen, and H. C. Chao, Using GHZ-state for multiparty quantum secret sharing without code table, The computer journal advance access published. February 1, 1-9, 2012.

[73] F. G. Deng, H. Y. Zhou, and G. L. Long, Bidirectional quantum secret sharing and secret splitting with polarized single photons, Phys. Lett. A., 337, 329-334, 2005.

[74] F. G. Deng, G. L. Long, and H. Y. Zhou, An efficient quantum secret sharing scheme with Einstein-Podolsky-Rosen pairs, Phys. Lett. A., 340, 43-50, 2005.

[75] F. G. Deng, H. Y. Zhou, and G. L. Long, Circular quantum secret sharing, J. Phys. A: Math Gen. 39, 14089-14099, 2006.

[76] L. Hao, C. Wang, and G. L. Long, Quantum secret sharing protocol with four state Grover algorithm and its proof-of-principle experimental demonstration, Opt. Commun., 284, 3639-3642, 2011.

[77] K. J. Wei, H. Q. Ma, and J. H. Yang, Experimental circular quantum secret sharing over telecom fiber network, Optics Express., 21, 16664-16669, 2013.

[78] Z. J. Zhang, Y. Li, and Z. X. Man, Multiparty quantum secret sharing, Phys. Rev. A., 71, 044301-044306, 2005.

[79] A. Beige, B. G. Englert, C. Kurtsiefer, and H. Weinfurter, Secure communication with a publicly known key, Acta. Physica. A., 101, 357-370, 2002.

[80] T. Tyc, and B. C. Sanders, How to share a continuous-variable quantum secret by optical interferometry, Phys. Rev. A., 65, 042310, 2002.

[81] A. M. Lance, T. Symul, W. P. Bowen, T. Tyc, B. C. Sanders, and P. K. Lam, Continuous variable (2,3) threshold quantum secret sharing schemes, New J. Phys., 5 2003.

[82] H. Lai, M. A. Orgun, J. H. Xiao, L. Y. Xue, J. Pieprzyk, Dynamic (2,3) threshold quantum secret sharing of secure direct communication, Communications in Theoretical Physics, 459-465, 2015(63).

[83] R. G. Buschman, http://www.fq.math.ca/Scanned/1-4/buschman-a.pdf (last accessed 27//11/2014)

[84] J. W. Byers, M. Luby, and M. Mitzenmacher, A. Rege, A digital fountain approach to reliable distribution of bulk data, In Proceedings of the ACM SIGCOMM '98 con-

ference on Applications, technologies, architectures, and protocols for computer communication (SIGCOMM '98), Martha Steenstrup (Ed.). ACM, New York, NY, USA, pages 56-67, 1998.

[85] Y. Lin, B. Liang, and B. Li, Data Persistence in Large-Scale Sensor Networks with Decentralized Fountain Codes, In INFOCOM 2007. 26th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies, 6-12 May 2007, Anchorage, Alaska, USA. pages 1658-1666, IEEE, 2007.

[86] A. Joux, Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions, LNCS 3152/2004, 306-316.

[87] H. Tseng, R. Jan, and W. Yang, A chaotic maps-based key agreement protocol that preserves user anonymity. In: IEEE International Conference on Communications, ICC2009, Dresden, Germany, pp. 1-6 2009.

[88] T. Kohda, and A. Tsuneda, Pseudonoise sequences by chaotic nonlinear maps and their correlation properties, IEICE Trans. Commun, 855-862, 1993.

[89] T. Koshy, John Wiley and Sons, New York (2001).

[90] E. W. Weisstein, Lucas Number. http://mathworld.wolfram.com/LucasNumber.

[91] A. Grudka, and Wójcik, Symmetric scheme for superdense coding between multiparties, Phys. Rev. A., 66 (1):014301, 2002.

[92] L. Zhang, C. Silberhorn, and I. A. Walmsley, Secure quantum key distribution using continuous variables of single photons, Phys. Rev. Lett., 100(11), 110504, 2008.

[93] H. Bechmann-Pasquinucci, and W. Tittel, Quantum cryptography using larger alphabets, Phys. Rev. A., 61(6), 062308 , 2000.

[94] D. Bruss, Optimal eavesdropping in quantum cryptography with six states, Phys. Rev. Lett., 81, 3018, 1998.

[95] M. Curty, M. Lewenstein, and N. Lükenhaus, Entanglement as precondition for secure quantum key distribution, Phys. Rev. Lett., 92, 217903, 2004.

[96] S. Félix, N. Gisin, A. Stefanov, and H. Zbinden, Faint laser quantum key distribution: eavesdropping exploiting multiphoton pulses, Journal of Modern Optics, 48(13), 2009, 2001.

[97] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Quantum cryptography with coherent States, Phys. Rev. A., 51, 1863, 1995.

[98] K. Inoue, E. Waks, and Y. Yamamoto, Differential phase shift quantum key distribution, Phys. Rev. Lett., 89, 037902, 2002.

[99] P. Kok, and S. L. Braunstein, Postselected versus nonpostselected quantum teleportation using parametric down-conversion, Phys. Rev. A., 61, 042304, 2000.

[100] E. Knill, R. Laflamme, and G. J. Milburn, A scheme for efficient quantum Computation with linear optics, Nature, 409, 46, 2001.

[101] N. Yu, P. Genevet, M. A. Kats, F. Aieta, J. P. Tetienne, F. Capasso, and Z. Gaburro, Light propagation with phase discontinuities: generalized laws of reflection and refraction, Science., 334, 333-337, 2011.

[102] L. Dal Negro, N. Lawrence, and J. Trevino, Analytical light scattering and orbital angular momentum spectra of arbitrary Vogel spirals, Opt Express., 20(16), 18209-18223, 2012.

[103] J. Romero, D. Giovannini, S. Franke-Anold, S. M. Barnett, and M. J. Padgett, Increasing the dimension in high-dimensional two-photon orbital angular momentum entanglement, arXiv:1205.1968v1.

[104] R. Fickler, R. Lapkiewicz, W. N. Plick, M. Krenn, C. Schaeff, S. Ramelow, and A. Zeilinger, Quantum entanglement of high angular momenta, Science., 338, 640, 2012.

[105] C. Lupo, and S. Lloyd, Quantum-locked key distribution at nearly the classical capacity rate, Phys. Rev. Lett., 113, 160502 (2014).

[106] F. Dupuis, J. Florjanczyk, P. Hayden, and D. Leung, Locking Classical Information, Proc. R. Soc. A. 469, 2159, 2013.

[107] C. H. Bennett, G. Brassard, and J.-M. Robert, SIAM J. Comput. 17, 210, 1988.

[108] S. Guha, P. Hayden, H. Krovi, S. Lloyd, C. Lupo, and J. H. Shapiro, Phys. Rev. X., 4, 011016, 2014.

[109] F. G. Deng, G. L. Long, and X. S. Liu, Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block, Phys. Rev. A., 68, 042317, 2003.

[110] F. G. Deng, and G. L. Long, Secure direct communication with a quantum one-time pad, Phys. Rev. A., 69, 052319, 2004.

[111] C. Wang, F. G. Deng, Y. S. Li, X. S. Liu, and G. L. Long, Quantum secure direct communication with high-dimension quantum superdense coding, Phys. Rev. A., 71, 044305, 2005.

[112] Q. Y. Cai, and B. W. Li, Improving the capacity of the *Boström*-Felbinger protocol, Phys. Rev. A., 69, 054301, 2004.

[113] T. Gao, F. L. Yan, and Z. X. Wang, A simultaneous quantum secure direct communication scheme between the central party and other M parties, Chin. Phys. Lett., 22, 2473, 2005.

[114] H. Lee, J. Lim, and H. J. Yang, Quantum direct communication with authentication, Phys. Rev. A., 73, 042305, 2006.

[115] C. Wang, F. G. Deng, and G. L. Long, Multi-step quantum secure direct communication using multi-particle Green-Horne-Zeilinger state, Opt. Commun., 15, 253, 2005.

[116] L. F. Han, Y. M. Liu, J. Liu, and Z. J. Zhang, Multiparty quantum secret sharing of secure direct communication using single photons, Opt. Commun., 281, 2690-2694, 2008.

[117] R. G. Du, Z. W. Sun, B. H. Wang, and D. Y. Long, Quantum secret sharing of secure direct communication using one-time pad. Int. J. Theor. Phys., 51, 2727-2736, 2012.

[118] B. K. Li, Y. G. Yang, and Q. Y. Wen, Threshold quantum secret sharing of secure direct communication, Chin. Phys. Lett., 26(1), 010302, 2009.

[119] H. Lai, J. H. Xiao, M. A. Orgun, L. Y. Xue, and J. Pieprzyk, Quantum direct secret sharing with efficient eavesdropping-check and authentication based on distributed fountain codes, Quantum Inf. Proc., 13, 895-907, 2014.

[120] F. Gao, S. Qin, F. Guo, and Q. Y. Wen, Dense-coding attack on threeparty quantum key distribution protocols, IEEE J. Quantum Electron., vol. 47(5), 630-635, 2011.

[121] H. Lai, L. Y. Xue , M. A. Orgun, J. H. Xiao, and J. Pieprzyk, A hybrid quantum key distribution using extended unitary operations and distributed fountain codes, Quantum Inf. Proc., 697-713, 2015(14).

[122] H. Lai, M. A. Orgun, L. Y. Xue, J. H. Xiao, and J. Pieprzyk, Dual compressible hybrid quantum secret sharing schemes based on extended unitary operations, Proc. SPIE 9123, Quantum Information and Computation XII, Baltimore, USA, May, 2014.

[123] H. K. Lo, and T. M. Ko, Some attacks on quantum-based cryptographic protocols. Quantum Inf. Comput., 5, 41-48, 2005.

[124] R. Duan, Y. Feng, and M. Ying, Entanglement is not necessary for perfect discrimination between unitary operations, Phys. Rev. Lett., 98(10), 100503-100507, 2007.

[125] D. Gottesman, H. K. Lo, N. L*ü*tkenhaus, and J. Preskill, Security of Quantum Key Distribution with Imperfect Devices, ISIT 2004. http:ieeexplore.ieee.org/iel5/9423/29909/01365172.pdf?arnumber=1365172

[126] G. Long, and X. Liu, Theoretically efficient high-capacity quantum-key distribution scheme, Phys. Rev. A., 65, 032302-32305, 2002.

[127] A. Cabello, Quantum Key Distribution in the Holevo Limit, Phys. Rev. Lett., 85, 5635-5638, 2000.

[128] Y. H. Kim, S. P. Kulik, and Y. Shih, Quantum teleportation of a polarization state with a complete Bell state measurement, Phys. Rev. Lett., 86, 1370-1373, 2001.

[129] A. Parakh, and S. Kak, Space efficient secret sharing for implicit data security, Inf. Sci., 181, 335-341, 2011.

[130] H. Lai, J. H. Xiao, L. X. Li, and Y. X. Yang, Recursive hiding of biometrics-based secret sharing scheme using adversary structure, Inf. Proc. Lett., 112, 683-687, 2012.

[131] C. S. Ding, D. Kohel, and S. Ling, Secret sharing with a class of ternary codes, Theoret. Comput. Sci., 246, 285-298, 2000.

[132] H. K. Lo, H. F. Chau, and M. Ardehali, Efficient quantum key distribution scheme and a proof of its unconditional security, Journal of Cryptology, 18(2), 133-165, 2005.

[133] P. Xue, C. F. Li, and G. C. Guo, Conditional efficient multiuser quantum cryptography network, Phys. Rev. A., 65, 022317, 2002.

[134] P. W. Shor, and J. Preskill, Simple proof of security of the BB84 quantum key distribution protocol, Phys. Rev. Lett., 85, 441, 2000.

[135] H. K. Lo, and H. F. Chau, Unconditional security of quantum key distribution, Science, 283, 2050, 1999.