

QUANTUM CRYPTOGRAPHY: FROM THEORY TO PRACTICE

by

Xiongfeng Ma

A thesis submitted in conformity with the requirements
for the degree of Doctor of Philosophy Thesis
Graduate Department of Department of Physics
University of Toronto

Copyright © 2008 by Xiongfeng Ma

Abstract

Quantum cryptography: from theory to practice

Xiongfeng Ma

Doctor of Philosophy Thesis

Graduate Department of Department of Physics

University of Toronto

2008

Quantum cryptography or quantum key distribution (QKD) applies fundamental laws of quantum physics to guarantee secure communication. The security of quantum cryptography was proven in the last decade. Many security analyses are based on the assumption that QKD system components are idealized. In practice, inevitable device imperfections may compromise security unless these imperfections are well investigated.

A highly attenuated laser pulse which gives a weak coherent state is widely used in QKD experiments. A weak coherent state has multi-photon components, which opens up a security loophole to the sophisticated eavesdropper. With a small adjustment of the hardware, we will prove that the decoy state method can close this loophole and substantially improve the QKD performance. We also propose a few practical decoy state protocols, study statistical fluctuations and perform experimental demonstrations. Moreover, we will apply the methods from entanglement distillation protocols based on two-way classical communication to improve the decoy state QKD performance. Furthermore, we study the decoy state methods for other single photon sources, such as triggering parametric down-conversion (PDC) source. Note that our work, decoy state protocol, has attracted a lot of scientific and media interest. The decoy state QKD becomes a standard technique for prepare-and-measure QKD schemes.

Aside from single-photon-based QKD schemes, there is another type of scheme based on entangled photon sources. A PDC source is commonly used as an entangled photon source. We propose a model and post-processing scheme for the entanglement-based QKD with a PDC source. Although the model is proposed to study the entanglement-based QKD, we emphasize that our generic model may also be useful for other non-QKD experiments involving a PDC source. By simulating a real PDC experiment, we show that the entanglement-based QKD can achieve longer maximal secure distance than the single-photon-based QKD schemes.

We propose a time-shift attack that exploits the efficiency mismatch of two single photon detectors in a QKD system. This eavesdropping strategy can be realized by current technology. We will also discuss counter measures against the attack and study the security of a QKD system with efficiency mismatch detectors.

Acknowledgements

The research presented in this Doctor of Philosophy thesis is carried out under the supervision of Prof. Hoi-Kwong Lo in the Department of Physics at the University of Toronto. I owe my most sincere thanks to Hoi-Kwong for sharing his extensive knowledge with me. I can still clearly remember the time when I went to his office every week and struggled to understand the GLLP security analysis, how I was disappointed by my first simulation result, and how happy I was when I finished the simulation work for the decoy state method inspired by his conference paper. I am very grateful for his support of my non-academic life as well.

During my graduate study, I was lucky enough to be surrounded by wonderful colleagues: Jean-Christian Boileau, Ryan Bolen, Kai Chen, Marcos Curty, Frédéric Dupuis, Ben Fortescue, Chi-Hang Fred Fung, Leilei Huang, Bing Qi, Li Qian, Kiyoshi Tamaki, Yi Zhao etc. In particular, I would like to thank Bing Qi for enormously helpful and enjoyable discussions about models, experimental setups and security analysis.

I wish to express my warm and sincere thanks to researchers in the field who have helped along the way and influenced the formation of the understanding and approach to quantum cryptography presented in this thesis. I would like to acknowledge that I have benefited very much from thoughtful discussions with Norbert Lütkenhaus, Jian-Wei Pan, Aephraim M. Steinberg, Wolfgang Tittel, Gregor Weihs and the members of their research groups.

I would like to thank Ms. Serena Ma for her suggestions and proofreading. Responsibility for any remaining errors and omissions rests entirely with the author.

I gratefully acknowledge the financial support from the Chinese Government Award for Outstanding Self-financed Students Abroad and the Lachlan Gilchrist Fellowship.

Furthermore, my warm thanks are extended to the members of the Department of Physics, the Chinese Students and Scholars Association at the University of Toronto and the Student Diversity Group. With them, I enjoyed a colorful life as a graduate student at the University of Toronto.

Finally, and most importantly, I would like to thank my family for their constant and unending love and support. This thesis is dedicated to my parents, which without them, none of this would have been even possible.

Contents

1	Introduction	1
1.1	Background	1
1.1.1	Quantum information processing	1
1.1.2	Cryptography	2
1.1.3	Quantum cryptography	4
1.1.4	Cryptanalysis and Quantum Cryptanalysis	6
1.2	Preliminary	6
1.2.1	A QKD scenario	6
1.2.2	QKD performance	7
1.3	Motivation	8
1.3.1	QKD security	8
1.3.2	A gap between theory and experiment	8
1.4	Highlight and Outline	9
1.5	Future outlook	11
2	Security analysis	12
2.1	What are security proofs?	12
2.2	Squash model	13
2.2.1	A calibration problem	13
2.2.2	Squash model	13
2.2.3	Remarks	14
2.3	Entanglement-based QKD	15
2.4	Single-photon-based QKD	16
2.5	GLLP security analysis	19
2.5.1	Tagged and untagged qubits	19
2.5.2	Post-processing	19

2.5.3	An extension	20
2.6	GLLP vs. Lütkenhaus' security analysis	21
3	Setup and Model	23
3.1	QKD setup	23
3.2	QKD model	24
3.2.1	Weak coherent state source	24
3.2.2	Channel and detection	26
3.2.3	Photon number channel model	27
3.3	QKD hardware	28
3.3.1	Laser source	28
3.3.2	Channel	28
3.3.3	Detection	29
4	Decoy state	31
4.1	Decoy state	31
4.1.1	Motivation	32
4.1.2	Solution	32
4.1.3	Discussion	33
4.1.4	Simulation	34
4.2	Upper Bounds	35
4.2.1	Distance upper bound	35
4.2.2	Key rate upper bound	36
4.3	Discussion	37
5	Practical decoy state	38
5.1	Practical proposals	38
5.1.1	Vacuum+Weak decoy	39
5.1.2	One decoy	41
5.1.3	Numerical method	42
5.2	Statistical fluctuation analysis	44
5.2.1	What parameters are fluctuating?	44
5.2.2	Standard Error Analysis	47
5.2.3	Choice of N_s , N_{vac} , N_w and ν	48
5.3	Simulation	49

5.4	Experimental demonstrations	53
5.4.1	How to generate decoy states	53
5.4.2	Experimental data post-processing	54
5.5	Conclusion	55
6	Decoy state QKD with 2-LOCC	56
6.1	2-LOCC EDP	56
6.1.1	Gottesman-Lo EDP	57
6.1.2	Recurrence EDP scheme	60
6.1.3	Bounds of error rates	61
6.2	Decoy + GLLP + Gottesman-Lo EDP	63
6.3	Decoy + GLLP + Recurrence EDP	67
6.4	Conclusion	70
7	Triggering PDC QKD	71
7.1	Background	72
7.2	Experiment setup	74
7.3	Model	76
7.3.1	On Alice's side	76
7.3.2	Threshold detector	77
7.3.3	Perfect photon-number resolving detector	78
7.4	Post-processing	79
7.4.1	Non-decoy states with threshold detectors	80
7.4.2	Infinite active decoy state with threshold detectors	80
7.4.3	Weak active decoy state with threshold detectors	81
7.4.4	Passive decoy state	82
7.4.5	Passive decoy state with threshold detectors	83
7.4.6	With a perfect photon-number resolving detector	84
7.4.7	A few remarks	84
7.5	Simulation	85
7.5.1	Without statistical fluctuations	86
7.5.2	With statistical fluctuations	88
7.6	Conclusion	90

8	Entanglement-based QKD	92
8.1	Introduction	93
8.2	Implementation	94
8.2.1	Source in the middle	95
8.2.2	Source on Alice's side	95
8.3	Model	96
8.3.1	An entangled PDC source	96
8.3.2	Detection	97
8.4	Post-processing	98
8.5	Simulation	99
8.5.1	Comparison of three QKD implementations	99
8.5.2	With two-way classical communication	101
8.5.3	Statistical fluctuations	102
8.6	Conclusion	103
9	Quantum cryptanalysis	105
9.1	Side information	105
9.1.1	Detector inefficiency loophole	105
9.1.2	Timing information	106
9.2	Time-shift attack	107
9.3	Security against time-shift attack	109
9.3.1	A simple solution	109
9.3.2	Security proof for a QKD system with detector efficiency mismatch	109
9.4	Discussion	110
10	Conclusions and outlook	112
10.1	Decoy state QKD	112
10.2	Other topics	113
10.3	Future work outlook	113
A	Abbreviations and mathematical derivations	115
A.1	Abbreviations	115
A.2	Key rate of the recurrence scheme with an ideal single photon source	116
A.2.1	Parity check	116
A.2.2	Error correction	117

A.2.3	Privacy amplification	117
A.3	Security against basis dependent source	119
A.4	Residue for the Decoy+GLLP+Recurrence scheme	120
A.5	QBER for entanglement PDC QKD	123
B	Optimal μ	127
B.1	Coherent state QKD	127
B.1.1	Without decoy states	127
B.1.2	With decoy state	129
B.2	Triggering PDC QKD	131
B.2.1	Without decoy states	131
B.2.2	With decoy states	132
B.2.3	Numerical checking	133
B.3	Entanglement PDC QKD	134
	Bibliography	135

Chapter 1

Introduction

Study the past, if you would divine the future. — Confucius

1.1 Background

In this section, we will give a brief overview of quantum information processing and then discuss one of its subfields that this thesis will focus on which is quantum cryptography¹

1.1.1 Quantum information processing

Quantum information processing or quantum information science is an amalgamation of quantum physics and information science. It concerns information science that depends on quantum effects in physics. It includes theoretical issues in communication and computational models as well as experimental topics in quantum physics, including what can and cannot be done with quantum information. It is an interdisciplinary field, combining ideas in physics, information theory, engineering, computer science, mathematics and chemistry.

A bit; a binary digit, is the base of classical information theory. Regardless of its physical representation, it is always read as either a 0 or 1. For instance, a 1 (true value) is represented by a high voltage, while a 0 (false value) is represented by a low voltage.

A quantum bit, or qubit (sometimes qbit) is a unit of quantum information. That information is described by a state vector in a two-level quantum mechanical system which is formally equivalent to a two-dimensional Hilbert space. A qubit has some

¹I acknowledge that Subsections 1.1.1 and 1.1.2 heavily rely on the Internet to gather information, especially wikipedia.org and quantiki.org.

similarities to a classical bit, but is fundamentally very different. Like a bit, a qubit can have two possible values, normally a 0 or a 1. The difference is that whereas a bit must be either 0 or 1, a qubit can be 0, 1, or a superposition of both.

Subfields of quantum information processing include:

- Quantum computing, which deals on the one hand, with the question how and whether one can build a quantum computer and on the other hand, searching algorithms that harness its power;
- Quantum computation, which investigates computational complexity of various quantum algorithms;
- Quantum error correction, which is used in quantum computing to protect quantum information from errors due to decoherence and other quantum noise;
- Quantum entanglement, which studies entanglement as seen from an information-theoretic point of view;
- Quantum cryptography and its generalization, quantum communication, which is the art of transferring a quantum state from one location to another. Note that this is the first quantum information application to reach the level of mature technology and fit for commercialization. This thesis focuses on quantum cryptography.

1.1.2 Cryptography

Nowadays, distant communications play a crucial role in our daily lives. Secure communications become more and more important in many areas, e.g., online purchases, emails and video chats.

Cryptography is the practice and study of encoding and decoding secret messages to ensure secure communications. There are two main branches of cryptography: secret-(symmetric-) key cryptography and public- (asymmetric) key cryptography.

A key is a piece of information (a parameter) that controls the operation of a cryptographic algorithm. In encryption, a key specifies the particular transformation of plaintext into ciphertext, or vice versa during decryption. Keys are also used in other cryptographic algorithms, such as digital signature schemes and message authentication codes.

In practice, due to significant difficulties of distributing keys in secret key cryptography, public-key cryptographic algorithms are widely used in conventional cryptosystems.

These encryption schemes can only be proven secure based on the presumed difficulty of a mathematical problem, such as factoring the product of two large primes. We emphasize that no public-key encryption scheme can be secure against eavesdroppers with unlimited computational power.

One of the most famous quantum computing algorithms is Shor's algorithm [105], which can factor a number N in $O((\log N)^3)$ time and $O(\log N)$ space. The algorithm is significant because it implies that public key cryptography might be easily broken, given a sufficiently large quantum computer. RSA [98], for example, uses a public key N which is the product of two large prime numbers. One way to crack RSA encryption is by factoring N , but with classical algorithms, factoring becomes increasingly time consuming as N grows large; more specifically, no classical algorithm is known that can factor in time $O((\log N)^k)$ for any k . By contrast, Shor's algorithm can crack RSA in polynomial time. It has also been extended to attack many other public-key cryptosystems.

In cryptography, the one-time pad is an encryption algorithm where the plaintext is combined with a random key or "pad" that is as long as the plaintext and used only once. A modular addition is used to combine the plaintext with the pad². In 1917, Vernam proposed one-time pad encryption scheme [116]. In 1949, Shannon proved that the one-time pad is information-theoretically secure, no matter how much computing power is available to the eavesdropper [104]. That is, if the key is truly random, never reused and kept secret, the one-time pad provides perfect secrecy. Note that the one-time pad is the only cryptosystem with perfect secrecy.

Despite Shannon's proof of its security, the one-time pad has serious drawbacks in practice:

1. it requires a perfectly random key;
2. secure generation and exchange of the key must be at least as long as the message.

These implementation difficulties have led to one-time pad systems being unpractical and are so serious that they have prevented the one-time pad from being adopted as a widespread tool in information security.

Quantum physics offers a solution to the aforementioned two difficulties for the one-time pad. First, the superposition (uncertainty) nature of quantum mechanics can generate *true* randomness. Secondly, quantum cryptography allows two distant parties to generate secure keys.

²For binary data, the operation XOR amounts to the same thing.

1.1.3 Quantum cryptography

Quantum cryptography or quantum key distribution (QKD) applies fundamental laws of quantum physics to guarantee secure communication. It enables two legitimate users, commonly named Alice and Bob, to produce a shared secret random bit string, which can be used as a key in cryptographic applications, such as message encryption (for instance, the one-time pad) and authentication. Unlike conventional cryptography, whose security often relies on unproven computational assumptions, QKD promises unconditional security based on the fundamental laws of quantum mechanics.

There are mainly two types of QKD schemes. One is the prepare-and-measure scheme, such as BB84 [11], in which Alice sends each qubit in one of four states of two complementary bases; B92 [9] in which Alice sends each qubit in one of two non-orthogonal states; six-state [17] in which Alice sends each qubit in one of six states of three complementary bases. The other is the entanglement based QKD, such as Ekert91 [24] in which entangled pairs of qubits are distributed to Alice and Bob, who then extract key bits by measuring their qubits; BBM92 [12] where each party measures half of the EPR pair in one of two complementary bases. Note that in Ekert91, Alice and Bob estimate the Eve's information based on the Bell's inequality test³; whereas in BBM92, similar to BB84, Alice and Bob make use of the privacy amplification to eliminate Eve's information about the final key [62].

QKD needs a quantum channel and a classical channel. The quantum channel can be insecure whereas the classical channel is assumed to be authenticated. Fortunately, in classical cryptography, unconditionally secure authentication schemes such as the Wegman-Carter authentication scheme [125, 126] exist. Moreover, those unconditionally secure authentication schemes are efficient: to authenticate an N -bit message, only an order $\log N$ bits of the shared key are needed. Since a small amount of pre-shared secure bits is needed between Alice and Bob, the goal of QKD is key growing, rather than key distribution. Notice that in the conventional information theory, key growing is an impossible task. Therefore, QKD provides a fundamental solution to a classically impossible problem.

The procedure of the best-known QKD protocol, BB84, is as follows. We assume that Alice uses polarization encoding.

1. Alice randomly chooses one of the four states (vertical, horizontal, 45-degree and

³In the original proposal [24], the author claimed that the final key is secure when the Bell's inequality is maximally violated. There are many follow-up works, such as [1].

- 135-degree polarizations). Denote the rectangular basis as Z basis and the diagonal basis as X basis. She sends the qubit to Bob through an insecure quantum channel.
2. Bob randomly chooses Z or X basis to measure the received states. He keeps his measurement result secretly.
 3. Through a public classical channel, Alice and Bob compare the basis and only keep the measurement results that they use the same basis. This step is commonly called *basis reconciliation*. If both of them randomly choose bases, they will discard half of the detection results.
 4. Alice and Bob implement error correction and privacy amplification to extract the final secure key. Later, we will show how to realize this step, which is normally the main focus of a security proof.

Eve may tamper the quantum channel and change/measure the states sent by Alice. The last two steps together is called post-processing. It normally requires an authenticated classical channel. That is, Eve can obtain all information about the classical communication during the post-processing but not modify them.

Proving the security of QKD is a difficult problem in theory. Fortunately, this problem was solved in the last decade, see for example, [84, 62, 106, 52]. Many security proofs are based on the assumption of idealized QKD system components, such as a perfect single photon source and well-characterized detectors. In practice, inevitable device imperfections may compromise security unless these imperfections are well investigated. Meanwhile, the security of QKD with realistic devices has been studied, see [85, 70, 15, 25, 41, 54, 35] for examples. For more information about security proofs of QKD, one can refer to Chapter 2. For a review of quantum cryptography, one may refer to [31].

Experimental QKD has been successfully demonstrated over 100 km of transmission distance through both commercial telecom fibers and free space [10, 113, 97, 14, 32, 102]. Commercial QKD systems are already on the market⁴. The main problem in the field is the security and performance of a realistic QKD system.

⁴Note that there are three companies, id Quantique, MagiQ and Smartquantum, that have commercial QKD products. However, the security has not been fully addressed yet.

1.1.4 Cryptanalysis and Quantum Cryptanalysis

Cryptanalysis is the study of methods for obtaining the meaning of encrypted information, without access to the secret information which is normally required to do so. Typically, this involves finding the secret key. In non-technical language, this is the practice of code-breaking or cracking the code, although these phrases also have a specialized technical meaning⁵.

In the quantum analogue, we need to consider loopholes that exist in QKD systems and various attack strategies. The study of attacks has a two-fold meaning. First, it investigates the security in a practical sense. Secondly, it is fundamentally interesting in quantum mechanics. For example, a general physical problem in a practical QKD system with two detectors is the detection efficiency loophole [80, 26]. This loophole underlies not only applied technology, such as QKD, but also fundamental physics, such as Bell's inequality testing. Moreover, in practice, it is difficult to build two detectors that have exactly the same characteristics. Our work of time-shift attack (see Section 9.2) is an illustration of how one can proceed to handle this general problem in the security of QKD.

1.2 Preliminary

In this section, we will provide a general picture of QKD and some terminologies used in the thesis.

1.2.1 A QKD scenario

Let us introduce a few generic figures in QKD that we have already used in Section 1.1.3. Alice, the sender, is the one who starts a key transmission. Bob, the receiver, is the one who receives the quantum states and extracts the key sent by Alice. This is just a convention used in the field, but not a strict definition. In some protocols, such as an entanglement based QKD that will be discussed in Chapter 8, the roles of Alice and Bob are interchangeable.

The third important character is the eavesdropper, Eve, who play a dark side here. Eve is trying to intrude into the QKD and gain information about the key established between Alice and Bob. One conservative assumption in the QKD is that Eve has full

⁵Definition from wikipedia.org.

control of both the quantum and classical channels, knows the characteristics of the QKD components very well⁶ and has a great computational power. For example, Eve may own a quantum computer. Eve's attack is only limited by quantum mechanics and other physics laws.

Unconditional security is the Holy Grail of QKD, which means the security is proven without any restrictions of Eve's computational ability. As mentioned above, in an unconditional security proof, normally, Eve is assumed to own a powerful quantum computer and have full control of the channels. On the other hand, in most of widely used conventional classical cryptography protocols, security is proven by assuming that Eve has a finite computational power. See for example, RSA [98]. Thus, with the development of technology and algorithm, the assumption that is made today about computational power does not guarantee security for tomorrow. For instance, Eve may store the encrypted message and decrypt it in the future with better computational power or algorithm. From this point of view, unconditional security is appealed to many real life applications.

1.2.2 QKD performance

To compare different QKD protocols or setups, one needs to characterize the performance of QKD. There are two important aspects of QKD performance: key rate and maximal secure distance.

We assume that Alice encodes the quantum information into faint laser pulses. If not (e.g., Alice uses a photon source pumped by a continuous wave laser), then Alice and Bob can manually partition the time domain into pulses. The *key rate* is defined to be the average number of final secure key bits from one pulse. By multiplying the pulse repetition rate (frequency), the key rate gives the speed of key generation.

Due to the loss and noise, all practical QKD systems have a limit of secure distance. That is, beyond a certain distance, a QKD setup with a certain post-processing procedure cannot achieve a positive secure key. The *maximal secure distance* is defined for a certain QKD setup and the post-processing scheme as the maximal QKD transmission distance that can yield a positive key rate.

We emphasize that the mentioned key rate and maximal secure distance here is always based on a guaranteed (proven) security. In many cases, we regard this is the lower bound in the sense that this performance as the least that one can achieve. Considering

⁶Eve might be the producer of QKD systems.

a performance upper bound⁷ of QKD setups and protocols is also an interesting topic. For example, one can refer to Refs. [27, 20].

For a real life application, certain performance is required. For instance, the state of the art digital speech coding [94] typically needs a bit rate around 4-10 kbits/sec. A typical city wide area network must cover an area with a radius of 5-25 km. Later, in the conclusion of Chapter 5, we will see that the QKD performance with current technology can achieve these requirements.

1.3 Motivation

The main objective of this thesis is to bring QKD to real-life applications. To do that, we investigate the security issues of practical QKD systems and propose new techniques to improve QKD performance.

1.3.1 QKD security

As discussed in Section 1.1.3, we need to take into account device imperfections to achieve QKD security. For example, an imperfect single photon source may open up loopholes for sophisticated attacks, such as photon number splitting attacks [39, 15, 71].

On the detection side, Eve may launch attacks on the imperfections of detections. For instance, Eve may take advantage of the timing information of signal pulses. We will present a feasible attack with current technology, a time-shift attack, in Section 9.2.

Thus, in order to guarantee the security of a practical system, QKD components are closely investigated and a realistic model is established. Then, we link our model to the existing security proofs. From there, we can learn about the assumptions that are made to prove security and the requirements for QKD experiments.

1.3.2 A gap between theory and experiment

As mentioned in Section 1.2.2, in real-life applications, high QKD performance is required. Naturally, there are two important aspects of QKD performance: key generation speed (in bits/second) and transmission distance. Correspondingly, we will consider the two

⁷Beyond a upper bound, one surely cannot obtain a secure key.

criteria, key rate⁸ and maximal secure distance, as discussed in Section 1.2.2.

On the theory side, much effort has been spent on the security proof of QKD with imperfect devices [85, 70, 41, 54, 35]. By directly applying these security analyses, the QKD performance is very limited. One can refer to the simulation part in Chapter 4.

On the other hand, the transmission distance of QKD experiment has been extended from a few meters in the first QKD experiment to currently more than 150 km. If we apply a standard security analysis, for instance, GLLP, the existing experiment setups can only tolerate a very limited transmission distance (as the simulation results show in Section 4.1.4). The key issue here is the security of the experiment. Thus, there is a big gap between the theory and practice of QKD.

This thesis aims to bridge this gap between theory and practice by guaranteeing the security and improving the performance of practical QKD.

Note that in some cases, security is sacrificed to achieve a better QKD performance. In this thesis, we always guarantee the security first and then enhance the performance.

1.4 Highlight and Outline

During my Ph.D. program, I have completed the following projects by collaborating with my colleagues.

- In Chapter 2, there will be reviews of various QKD security proofs and comparison of two standard security proofs of QKD with realistic devices. This work is published in Ref. [73].
- In Chapter 3, there will be a discussion on a widely used experiment setup and its model. This work is published in Ref. [77]. Here I acknowledge that I benefited very much from discussions about experiment setups with Bing Qi.
- In Chapter 4, the decoy state idea and its security proof will be discussed. This work is published in Ref. [65]. In this work, I applied GLLP security analysis to a decoy state QKD and simulated a QKD experiment [32] to show the improvement given by using decoy states.
- In Chapter 5, practical decoy state protocols will be discussed. This work is published in Ref. [77]. In this work, I applied the idea of the Vaccum+Weak decoy

⁸Note that developing a QKD system with a high repetition rate is an interesting topic in the field, for example, see Ref. [108]. In this thesis, we will always focus on the key rate unless otherwise stated.

state protocol, which was first proposed by Lo [60] and considered statistical fluctuations. Furthermore, I designed the experimental parameters and analyzed data in the decoy state QKD experiment demonstration [131, 132]. Hence, it can be concluded that the decoy state idea is highly practical in real life applications.

- In Chapter 6, two post-processing schemes are studied based on two-way classical communication for the decoy state method. This work is published in Ref. [74]. In this work, I applied the Gottesman-Lo's 2-LOCC⁹ entanglement distillation protocol (EDP) and recurrence scheme to a decoy state QKD and simulated a QKD experiment to show the improvement by using two-way classical communication in a decoy state QKD.
- In Chapter 7, various decoy state protocols are investigated for triggering parametric down-conversion sources. This work is presented in Ref. [76]. In this work, I modeled the QKD setup with a triggered PDC source following Lütkenhaus' work [70] and compared various decoy state proposals of triggering PDC QKD.
- In Chapter 8, QKD with an entangled photon source will be discussed. This work is published in Ref. [75]. In this work, I built an entangled PDC source model, applied Koashi-Preskill's security analysis and simulated a PDC experiment to show the performance of the entanglement-based QKD in comparison with a triggered single photon source and coherent state QKD.
- In Chapter 9, quantum attacks and security against these such attacks will be investigated. These works are published in Refs. [90] and [29]. Aside from the decoy state method, we also studied other methods for improving the QKD performance, such as the dual detector scheme [93, 92]. I am not the main contributor of these works. I joined in discussions and helped work out the details.
- In Chapter 10, a summary of my Ph.D. study is presented and some interesting topics for future research are stated.
- In Appendix A, the common abbreviations used in the thesis is listed and some detailed mathematical derivations are shown.
- In Appendix B, the optimization of the source intensity μ is discussed.

⁹See Appendix A.1 for the definition of LOCC.

1.5 Future outlook

An interesting topic is the natural extension of the current work: further enhancement of the performance of practical QKD systems. Continuous variable QKD is proposed to achieve a higher key rate in short and medium transmission distance. An open question is the security of continuous variable QKD. This is an appealing topic in the field. Modeling and simulations for continuous variable QKD are also interesting.

Another crucial point is that in real life, one needs to consider some extra disturbances (e.g., quantum signals may share the channel with regular classical signals). The final goal is to achieve a customer friendly QKD system that can be easily integrated with the Internet, for instance.

Statistical fluctuations need to be considered in QKD with a finite key length. There is some work on this topic recently, e.g., [96]. An interesting topic is applying Koashi's complementary idea [53] to a finite key QKD and compare it with prior results.

An interesting topic outside quantum cryptography is whether the techniques developed in QKD can be useful in quantum computation. For example, do such models and post-processing schemes also help quantum computation by linear optics realizations?

Finally, quantum information processing is related to the foundation of quantum mechanics. As we know, quantum information (e.g., von Neumann entropy) can help us in understanding quantum entanglement. What about other principles in quantum mechanics?

Chapter 2

Security analysis

In this chapter, we will review various security proofs. We start with the objective of security proofs and the underlying assumptions in current security proofs. We compare two standard security proofs of the QKD with realistic devices. This work is published in Ref. [73].

2.1 What are security proofs?

To serve as a secure key in cryptographic uses, there are two criteria:

- (a) Alice and Bob share the same key; that is, an *identical key*.
- (b) Eve has no information about the key; that is, a *secure key*.

With regards to a careful analysis and the formulation of security, see [96]. For necessary and sufficient conditions for security, see [38].

The first criterion can be satisfied by performing a classical error correction, for example, by using the Cascade code [16]. After that, Alice and Bob will share an identical key. Next, Alice and Bob will perform privacy amplification, for instance, by random hashing, to eliminate Eve's information about the key.

The goal of current security analyses is to show how much privacy amplification needs to be performed after a certain error correction procedure.

The main task for a security analysis is to figure what the length of the final secure key is and perform hashing to obtain the final key.

2.2 Squash model

In this section, we will formalize the widely used squash model in security proofs. Note that the squash model is used in the security proof proposed by Gottesman, Lo, Lütkenhaus, and Preskill (GLLP) [35], see also [51, 114, 7].

2.2.1 A calibration problem

In all the existing QKD security proofs, certain characteristics of sources and detectors are assumed to be known or measurable. However, in reality, such a calibration procedure is a very difficult task. For example, on Alice’s side, a good single photon source is not available with current technology although much effort has been made in this field [46, 68, 57, 43, 23, 127]. On Bob’s side, most of security proofs rely on the assumption that Bob measures two conjugate bases (for instance, X and Z) of *a qubit*. In real QKD experiments, threshold detectors¹ are widely used. In summary, devices calibration form a gap between the theory and practice of QKD.

In the experiment, to test (calibrate) a source, we need a good (well-characterized) detection system. On the other hand, to characterize a detector, we need a well-tested source. In QKD, we may even want to test these devices in real-time, which makes the task even more difficult.

In most QKD proposals², one needs to make sure that Bob’s (and sometimes also Alice’s) measurement is performed in a two-dimensional Hilbert space. This assumption is another way to state the squash model. We can see that this squash model assumption is *not* easy to avoid. Note that even throwing away the squash model, one needs to have certain assumptions about the side information. Later in Chapter 9, we will see that some side information (e.g., timing) may cause fatal security issues in QKD.

2.2.2 Squash model

In theory, the squash model is proposed to avoid the aforementioned calibration problem. As shown in Figure 2.1, the scenario that we are talking about here is as follows: Alice prepares her own system ρ_{AB}^0 . In a prepare-and-measure scheme (e.g., BB84), $\rho_A =$

¹A threshold detector can only tell whether the input signal is vacuum or non-vacuum. For a strict mathematical definition, one can refer to Section 7.3.2.

²One exception approach is the so-called device-independent QKD protocol [1] based on Bell’s inequality [8]. However, no strict security analysis has been yet provided for this type of QKD protocols. For recent developments of realistic threshold detector models, one can refer to Ref. [51].

$\text{Tr}_B(\rho_{AB}^0)$ determines the basis and key bit value that she will pick up. She then sends the system $\rho_{B0} = \text{Tr}_A(\rho_{AB}^0)$ to Bob, which is intercepted by Eve. Eve performs some operations and/or measurements on the system and resends a system ρ_{B1} to Bob. After passing through a filter, the state received by Bob is ρ_B . That is, Eve prepares a system ρ_B for Bob, generally depending on the system sent by Alice. Finally, Alice and Bob will extract a key from measurements on ρ_A and ρ_B . Alice and Bob's detection system follows the squash model.

Squash model: The detection system first performs a filter, projecting the incoming state ρ (with an arbitrary dimension of Hilbert space) into a two-dimensional Hilbert space state ρ_2 or output a “failure” signal. If the projection succeeds, a projection measurement will be performed in a basis³ in a two-dimensional Hilbert space.

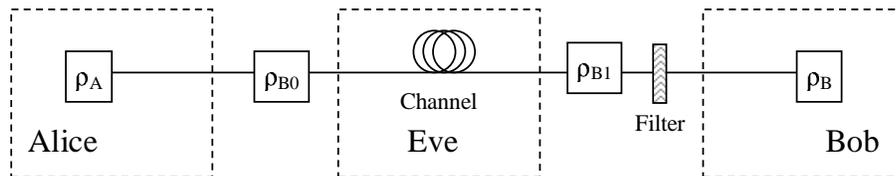


Figure 2.1: A schematic diagram for the squash model. The filter is the key component of the squash model.

The schematic diagram of the squash model is shown in Figure 2.1. As we can see that in the squash model, Bob always receives a qubit or vacuum. In other words, in the squash model, Eve always sends a qubit or vacuum to Bob.

2.2.3 Remarks

1. The squash model is reasonable (but not necessarily correct) for threshold detector cases. After treating the double click as a random click event, a threshold detector's response can always be described by a qubit or vacuum measurement outcome.
2. Even with only one photon, the squash model is still required in the existing security proofs. This is because there are lots of degrees of freedom of a photon, for instance, timing, polarization, phase [66] and space [91]. Thus, by using a perfect photon number resolving detector, one cannot avoid the squash model.

³This basis can be randomly chosen from a conjugated bases set.

3. The filter acts as a key component of the squash model. One can model the channel losses and detector efficiency into the failure probability of the filter.
4. In the squash model, when double clicks⁴ happen, we assume that Alice and Bob will assign a random bit when they get a double click, due to the strong pulse attack [69].
5. In a rigorous security analysis, one needs to experimentally verify whether the squash model gives a good description of a certain detection system. Take a widely used threshold detector for example. One needs to open the detector, examine the components carefully, then write down the quantum operations and compare the operations described by the squash model. Again, we want to emphasize that testing the model is a highly non-trivial task in the experiment.
6. Another way to avoid the device calibration problem is to propose so called device independent QKD protocols, see for example, Ref. [1]. Up until now, a strict security proof of these device independent QKD protocols is still missing. This is an interesting prospective topic. Recently, security proofs of QKD with a more realistic model, threshold detector model, are presented [51, 114, 7]. An interesting theoretical question is whether the threshold detector model is equivalent to the squash model.

2.3 Entanglement-based QKD

In this section, we will review the idea of the Lo-Chau type security proof [62] of QKD based on entanglement distillation protocols (EDP) [13].

In the following discussion, we will use X and Z to represent two conjugate bases, which are the Pauli operators:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (2.1)$$

to represent two conjugate bases. The QKD scenario in Lo-Chau's security proof can be described as follows:

⁴This is when more than one detector have detection events for one key bit transmission. In general, a double click probability is very small in comparison to dark count probability and detector efficiency.

1. Alice prepares n EPR pairs in one of the four Bell states,

$$\begin{aligned}
 |\psi_{00}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
 |\psi_{10}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\
 |\psi_{11}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \\
 |\psi_{01}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),
 \end{aligned} \tag{2.2}$$

for instance, in $|\psi_{00}\rangle^{\otimes n}$.

2. Alice sends half of each EPR pair to Bob and keeps the other half in her quantum memory.
3. After he receives the half EPR pairs, Bob stores all the qubits into his quantum memory.
4. Alice and Bob perform an EPD protocol [13] to distill m ($m \leq n$) into nearly perfect EPR pairs.
5. Alice and Bob measure the EPR pairs in the Z basis to obtain a shared secret key.

The key point of Lo-Chau's security proof is that if in Step 4, Alice and Bob share nearly perfect EPR pairs, the final key is secure. With a quantum computer, the amount of EPR pairs that Alice and Bob can distill is given by:

$$m = n - r_{err}, \tag{2.3}$$

where r_{err} is the amount of information (in bits) cost in the quantum error correction process. Here, r_{err} can be regarded as the number of encrypted bits communicated between Alice and Bob in the post-processing⁵.

2.4 Single-photon-based QKD

In this section, we will review Shor-Preskill's security proof [106]. In Lo-Chau's security, the main drawback is that quantum computers (or at least quantum memories) are required, which are not available with current technology. Based on Lo-Chau's security

⁵In this case, we assume that Alice and Bob encrypt the communication for the error correction.

proof, Shor and Preskill proposed a special EDP scheme, which can be reduced to a prepare-and-measure scheme.

The EDP protocol proposed by Shor and Preskill is based on the Calderbank-Shor-Steane (CSS) code [18, 107]. The basic idea of Shor-Preskill's security proof is to replace Step 4 of Lo-Chau's security proof (see Section 2.3) by the following procedures:

- (4.a) Alice and Bob pick up k testing EDP pairs randomly and both measure in Z basis to estimate bit error rate, δ_b . We call the procedure that corrects this type of error, *bit error correction*.
- (4.b) They pick up another k testing EDP pair randomly and both measuring in X basis to estimate the phase error rate, δ_p . Correspondingly, we call the procedure that corrects this type of error, *phase error correction*.
- (4.c) They abort the protocol if the error rates are too high. Otherwise, they apply a quantum CSS code to correct the bit and phase errors separately. It is here that an important property of the quantum CSS codes is applied: they can decouple the phase correction from the bit correction [106].
- (4.d) They can distill m ($m \leq n$) nearly perfect EPR pairs by the quantum error correction procedure.

The key argument in Shor-Preskill's security proof is that since the final Z measurement (see Step 5 in Section 2.3) commutes with Steps 1-4, Alice and Bob can move this Z measurement ahead of Step 1. Note that this is the reason why CSS codes are applied to decouple bit and phase error corrections⁶. After this move, the bit error error correction becomes a regular classical error correction and the phase error correction becomes a privacy amplification. Now the modified procedure will be exactly the same as the BB84 protocol.

1. Alice prepares n qubits, each in one of the four eigenstates of X and Z . Here, the reason for preparing X eigenstate is to make a symmetry between the bit and phase error rates.
2. Alice sends the states to Bob.

⁶Note that the CSS code is a linear quantum error correction code. It uses two classical error correction codes (e.g., C_1 and C_2^\perp with $C_2 \subset C_1$) to protect bit and phase errors separately. For a detailed discussion of the reason why the CSS code can decouple bit and phase error corrections for QKD, one can refer to Ref. [106].

3. After he receives the states, Bob measures the states in X or Z bases randomly.
4. Alice and Bob perform a post-processing scheme to distill m ($m \leq n$) into bits of secure key.
 - (4.a) Alice and Bob pick up k measurement results to estimate the bit error rate, δ_b .
 - (4.b) Due to the symmetry of BB84, they can estimate the phase error rate⁷ by $\delta_p = \delta_b$.
 - (4.c) If the error rates are too high, they abort the protocol. Otherwise, they apply a classical error correction code to correct all the bit errors.
 - (4.d) They apply a privacy amplification (for instance, random hashing) according to the phase error rate, δ_p .

After the error correction and privacy amplification, the key rate is given by [106]:

$$R = qQ_\mu [1 - H_2(\delta_b) - H_2(\delta_p)], \quad (2.4)$$

where q is the basis reconciliation factor ($1/2$ for the BB84 protocol due to the fact that half of the time, Alice and Bob disagree with the bases, and if one uses the efficient BB84 protocol [63], $q \approx 1$), Q_μ is the filter success probability in the squash model⁸ and $H_2(x)$ is the binary entropy function,

$$H_2(x) = -x \log_2(x) - (1 - x) \log_2(1 - x). \quad (2.5)$$

In summary, there are two main parts of the post-processing, error correction (for bit error correction) and privacy amplification (for phase error correction). These two steps can be understood as follows. First, Alice and Bob apply an error correction, after which they share the same key strings, but Eve may still keep some information about the key. Alice and Bob then perform a privacy amplification to expunge Eve's information from the key.

⁷Note that $\delta_p = \delta_b$ is true for the case of infinite long key BB84. Later in Section 8.5.3, we will see that this may not be true for a finite key length with statistical fluctuations. Note also that for other protocols, such as the SARG04 protocol [101], it is no longer true that $\delta_p = \delta_b$ [109, 28].

⁸Basically, Q_μ is the probability for Bob to obtain a detection (not a vacuum) in a pulse of key transmission. Later, in Section 3.2, one can see why we use the notation Q_μ here.

2.5 GLLP security analysis

In this section, we will review the Gottesman-Lo-Lütkenhaus-Preskill (GLLP) security analysis idea [35]. It gives a security proof of BB84 QKD when realistic devices (such as imperfect single photon sources) are used.

2.5.1 Tagged and untagged qubits

In the original proposal of the BB84 protocol (as well as in Shor-Preskill's security proof), a perfect single photon source is required. Unfortunately, single photon sources are still not available with current technology. For the development of a single photon source, one can refer to Refs. [46, 68, 57, 43, 23, 127]. Thus, intuitively, we can think there are two components in an imperfect single photon source, one is good for BB84 and the other is bad. Separating these two components is the main idea of GLLP.

There are two kind of qubits discussed in GLLP, tagged qubits and untagged qubits. Tagged qubits are those that have their basis information revealed to Eve, i.e. tagged qubits are not secure for QKD. On the other hand, untagged qubits are secure for QKD. Note that the idea of the tagged state was (perhaps implicitly) introduced by Lütkenhaus [70].

The untagged qubits basically come from the idea of a basis-independent source [54]. A basis-independent source means that, to Eve, the quantum states transmitted through the channel are independent of the bases that Alice and Bob are choosing. Whereas the tagged qubits come from basis-dependent sources, whose basis information may be revealed to Eve.

Let us show a concrete example about tagged and untagged qubits. In BB84, qubits coming from single-photon states are untagged, while those from multi-photon states are tagged. This is because Eve, for instance, can perform photon-number splitting attacks [39, 15, 71] to the multi-photon states. This may not true for other protocols. For example, in SARG04 [101, 109], two-photon states can be used to extract secure keys.

2.5.2 Post-processing

The GLLP post-processing is performed as follows. First, Alice and Bob apply error correction to all qubits, sacrificing a fraction $H_2(E_\mu)$ of the raw key, which is represented in the first term of Eq. (2.6) below. Secondly, in principle, Alice and Bob can distinguish the tagged and untagged qubits (for instance, by measuring the photon numbers on

Alice's side), so they can apply the privacy amplification on the tagged state and untagged state separately. One can imagine executing privacy amplification on two different strings, the qubits s_{tagged} and $s_{untagged}$ arising from the tagged qubits and the untagged qubits respectively. Since the privacy amplification is linear (for instance, by linear hashing), the key obtained is the bitwise *XOR*

$$s_{untagged} \oplus s_{tagged}$$

of keys that could be obtained from the tagged and untagged qubits separately. If $s_{untagged}$ is private and random, then it does not matter if Eve knows anything about s_{tagged} , the sum will be still private and random. Thus, one only needs to apply privacy amplification to the untagged bits.

We define the key generation rate as the ratio of the final key length to the total number of pulses sent by Alice. Applying the GLLP idea to our model, Q_1 is the amount of untagged qubits. Thus, the key generation rate is given by [65]:

$$R \geq q\{-f(E_\mu)Q_\mu H_2(E_\mu) + Q_1[1 - H_2(e_1)]\}, \quad (2.6)$$

where q is the basis reconciliation factor as discussed in Eq. (2.4), Q_μ and E_μ are the overall gain (or filter success probability) and QBER, Q_1 and e_1 are the gain and error rate of untagged qubits, and $f(x)$ is the error correction inefficiency (see, for example, [16]) as a function of the error rate, normally $f(x) \geq 1$ with the Shannon limit $f(x) = 1$. For detailed definitions of Q_μ , E_μ , Q_1 and e_1 , one can refer to Section 3.2.

Note that one can add Q_0 into Eq. (2.6) by considering other security analysis [61], see also [51].

2.5.3 An extension

The original GLLP idea only considers two types of qubits: tagged and untagged. For BB84, it sets a phase error rate, $\delta_p = 1/2$ for tagged qubits and $\delta_p = \delta_b$ for the untagged qubits. The idea of applying separate privacy amplification (GLLP) can be naturally extended to the case of more than two classes of qubits [74], i.e. several kinds of qubits with tag g , which generalizes the concept of tagged and untagged qubits. The procedure of data post-processing is similar, an overall error correction step followed by privacy amplification to each case. Therefore, the key generation rate is given by:

$$R \geq q\{-f(E_\mu)Q_\mu H_2(E_\mu) + \sum_g Q_g[1 - H_2(e_g)]\} \quad (2.7)$$

where Q_g is the gain of the qubits with tag g and e_g is the corresponding phase error rate. Here, we want to emphasize that e_g is not equal to the bit error rate of the qubits with tag g in general, unless the qubits come from a basis-independent source.

This extension is useful for some post-processing schemes, e.g., SARG04 [101] and 2-LOCC post-processing schemes [74] (see Chapter 6).

The above discussion is a review of various security analysis. Next, we will compare two standard security analysis schemes.

2.6 GLLP vs. Lütkenhaus' security analysis

In this section, we will compare two data post-processing schemes, Lütkenhaus [70] versus GLLP [35]. Here, we use Lütkenhaus' security analysis, to refer to his work, see Ref. [70]⁹. Note that Lütkenhaus' security analysis proves the security against individual attacks, while GLLP offers unconditional security. This work is published in Ref. [73].

We can rewrite the formula of the key generation rate by Lütkenhaus' security analysis scheme [70]

$$R \geq q\{-Q_\mu H_2(E_\mu) + Q_1[1 - \log_2(1 + 4e_1 - 4e_1^2)]\}, \quad (2.8)$$

where the privacy amplification term $\log_2(1 + 4e_1 - 4e_1^2)$ comes from collision probability.

Now, we can compare Eqs. (2.6) and (2.8). In both key rate formulae, the first term in the bracket is for error correction and the second term is for privacy amplification. The privacy amplification is only performed on the single photon part. In this manner, Lütkenhaus [70] has already applied the idea of separate privacy amplification.

We can see that the only difference between the Lütkenhaus and GLLP results appears in the privacy amplification part. We compare $H_2(e)$ with $\log_2(1 + 4e_1 - 4e_1^2)$ in Figure 2.2. We can see that the difference of the two functions is quite small. For this reason, in fact, Lütkenhaus and GLLP give very similar results in the simulations of real experiments [73].

Based on this observation, we find that there is little to gain by restricting the security analysis to individual attacks, given that the two schemes; Lütkenhaus vs. GLLP, provide very close performances. In other words, our view is that one is better off considering unconditional security, rather than restricting to individual attacks.

⁹We acknowledge that Lütkenhaus has worked on many security analysis schemes, including ILM [41] and GLLP [35].

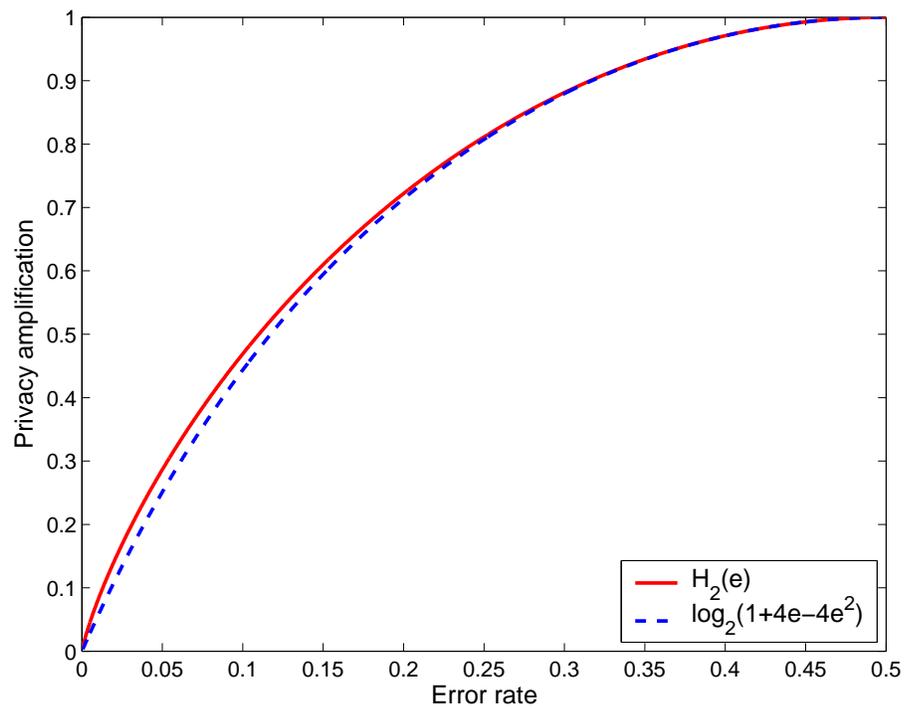


Figure 2.2: Plot of the privacy amplification parts of GLLP and Lütkenhaus. The maximal deviation of the two curves is 15.36% when the error rate is 3.85%.

Chapter 3

Setup and Model

In this chapter, we will discuss a widely used QKD setup and model. For now, we will focus on the case where a weak coherent state source is used as an imperfect single photon source by Alice. Nevertheless, many concepts from this generic model is useful for other QKD setups. For example, in Chapter 7, we will modify this model to fit the case of the QKD with triggered single photon sources.

This work is published in Ref. [77]. I acknowledge that I benefited very much from discussions about experiment setups with Bing Qi.

3.1 QKD setup

As we pointed out earlier, due to the lack of a perfect single photon source for BB84, a weak coherent state source is widely used. We call this setup a coherent state QKD implementation. Similarly, perfect single photon detectors are commonly replaced by threshold detectors. The setup is shown in Figure 3.1.

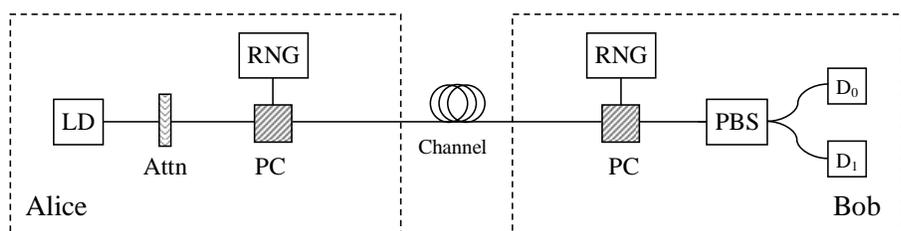


Figure 3.1: A schematic diagram for the coherent state QKD implementation. LD: laser diode; Attn: optical attenuator; RNG: random number generator; PC: polarization controller; PBS: polarization beam splitter; DB₀, DB₁: single photon detectors.

As shown in Figure 3.1, the coherent state QKD implementation works as follows.

1. Alice uses a weak coherent state photon source. She attenuates the laser beam from a laser diode (LD) with an optical attenuator (Attn). She uses a random number generator (RNG) to generate random bits for her choice of basis and bit values. She encodes one of four polarizations (eigenstates of X and Z bases) by a polarization controller (PC).
2. Bob receives the quantum states from the channel. He uses a PC as a polarization rotator for choosing his measurement basis, which is also controlled by a RNG. Then he uses a polarization beam splitter (PBS) followed by two single photon detectors (DA_1 and DA_2) to perform the measurement.

3.2 QKD model

There are three main parts for a QKD system: source, channel and detection. In this section, we present a widely used QKD system model that follows Ref. [70]. See also Ref. [77]. In the model, we assume that Alice sends out quantum signals in pulses. In the case where Alice uses a continuous source, we assume that Alice and Bob manually fit detections into pulses. This model is originally designed for the coherent state QKD, but the channel and detection parts can also be used for other QKD implementations. For example, in Chapter 8, we will modify the source part of this model to fit the case of QKD with entangled photon sources.

3.2.1 Weak coherent state source

Highly attenuated lasers are often used as an imperfect single photon source in QKD. This type of source can be well described by a weak coherent state, which is a superposition of number states (aka Fock states) [103],

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \quad (3.1)$$

Assuming that the phase of the laser is randomized for each pulse, the density matrix of the state emitted by Alice is given by:

$$\begin{aligned}
\rho_A &= \frac{1}{2\pi} \int_0^{2\pi} d\theta |\alpha|e^{i\theta}\rangle\langle\alpha|e^{i\theta}| \\
&= \frac{1}{2\pi} \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} \frac{|\alpha|^{n+m}}{\sqrt{n!m!}} e^{-|\alpha|^2} |n\rangle\langle m| \int_0^{2\pi} d\theta e^{i(n-m)\theta} \\
&= \sum_{n=0}^{\infty} \frac{\mu^n}{n!} e^{-\mu} |n\rangle\langle n|
\end{aligned} \tag{3.2}$$

where θ is the phase of the coherent state and $\mu = |\alpha|^2$, defined to be the intensity of the photon source. The photon number follows a Poisson distribution:

$$P(n) = \frac{\mu^n}{n!} e^{-\mu}. \tag{3.3}$$

From here, we can see that there are three types of photon states:

1. vacuum state: $|0\rangle\langle 0|$
2. single photon state: $|1\rangle\langle 1|$
3. multi photon state: $|n\rangle\langle n|$ for $n \geq 2$.

Here, we assume the squash model [35] as discussed in Section 2.2. That is, Eve receives all the pulses sent by Alice. Eve performs some arbitrary operations and sends either a vacuum or a qubit to Bob. Consequently, we denote the qubits coming from these three states as vacuum, single photon and multi photon qubits.

A vacuum qubit is a qubit sent by Eve when Alice sends a vacuum state. In the case without Eve's presence, it is some random qubit stemmed from the dark counts of Bob's detector or other background contributions. Thus, it does not contribute positively to the final secure key. Due to photon-number splitting attacks [39, 15, 71], multi photon states are not secure for the BB84 protocol. Here is a key observation of this QKD model: *the final secure key can only be extracted from single photon qubits*. Aside from BB84, this is true for most present QKD protocols, such as the B92 [9], six-state [17] and N -state [49] scheme. One exception is the SARG04 protocol [101], in which two-photon states can also contribute to the secure key generation rate [109].

3.2.2 Channel and detection

We use a beam splitter followed by a perfect single photon detector to model the channel and detection. We define η to be the transmittance of the beam splitter. The loss is composed by channel loss, internal loss in Bob's detection system and detector efficiency. We assume that the channel loss is related to the transmission distance by a loss coefficient β measured in dB/km. The transmittance η is given by:

$$\eta = \eta_B 10^{-\frac{\beta l}{10}}. \quad (3.4)$$

where η_B denotes the transmittance on Bob's side, including the internal transmission efficiency of optical components and detector efficiency. Here, we assume Bob uses threshold detectors. That is to say, we assume that Bob's detector can tell whether there is a click or not, but not the actual photon number of the received signal.

In the simulation, we assume independence between the behaviors of the i photons in i -photon states. Therefore, the transmittance of the i -photon state η_i with respect to a threshold detector is given by:

$$\eta_i = 1 - (1 - \eta)^i \quad (3.5)$$

for $i = 0, 1, 2, \dots$.

Yield: Defines Y_i as the yield of an i -photon state, i.e., the conditional probability of a detection event at Bob's side, given that Alice sends out an i -photon state. Note that Y_0 is the background rate which includes detector dark counts and other background contributions.

The yield of the i -photon states Y_i mainly comes from two parts, the background and the true signal. Assuming that the background counts are independent of the signal photon detection, then Y_i is given by:

$$\begin{aligned} Y_i &= Y_0 + \eta_i - Y_0 \eta_i \\ &\cong Y_0 + \eta_i. \end{aligned} \quad (3.6)$$

Here, we assume Y_0 (typically 10^{-5}) and η (typically 10^{-3}) are small.

The *gain* of i -photon states Q_i is given by:

$$Q_i = Y_i \frac{\mu^i}{i!} e^{-\mu}. \quad (3.7)$$

The gain Q_i is the probability that Alice sends out an i -photon state and Bob obtains a detection. Then the overall gain, the probability for Bob to obtain a detection event in

one pulse, is the sum over all Q_i s:

$$Q_\mu = \sum_{i=0}^{\infty} Y_i \frac{\mu^i}{i!} e^{-\mu}. \quad (3.8)$$

The overall gain Q_μ can also be understood as the filter success probability of the squash model that we discussed in Section 2.2.

Quantum Bit Error Rate (QBER): The error rate of i -photon states e_i is given by

$$e_i = \frac{e_0 Y_0 + e_d \eta_i}{Y_i} \quad (3.9)$$

where e_d is the probability that a photon hits the erroneous detector. e_d characterizes the alignment and stability of the optical system. Experimentally, even at distances as long as 120 km, e_d is relatively independent of the distance [32]. In the following, we assume that e_d is independent of the transmission distance and the background clicks are random. Thus, the error rate of the background is $e_0 = 1/2$. Then the overall QBER is given by:

$$E_\mu = \frac{1}{Q_\mu} \sum_{i=0}^{\infty} e_i Y_i \frac{\mu^i}{i!} e^{-\mu}. \quad (3.10)$$

In the QKD scenario that we are considering, as discussed in Section 1.2.1, Eve can change Y_i and e_i for her attacks. Without Eve, in a normal QKD, Eqs. (3.5), (3.6), (3.7) and (3.9) are satisfied for all $i = 0, 1, 2, \dots$. Thus, the gain and QBER are given by:

$$\begin{aligned} Q_\mu &= Y_0 + 1 - e^{-\eta\mu} \\ E_\mu Q_\mu &= e_0 Y_0 + e_d (1 - e^{-\eta\mu}). \end{aligned} \quad (3.11)$$

Due the fact that Q_μ and E_μ can be measured or tested from the experiment, we will use Eq. (3.11) in later simulations.

3.2.3 Photon number channel model

The model described above can be understood in another equivalent model.

Photon number channel model: Alice and Bob have an infinite number of channels. For channel i , Alice sends out an i -photon state to carry the qubit information, $i = 0, 1, 2, \dots$. In the aforementioned model, Alice chooses which channel to use with a Poisson distribution, shown in Eq. (3.3), which is determined by her photon source.

Then Y_i and e_i can be regarded as the yield and error rate of channel i . Again, in our QKD scenario, Eve has full control of all these channels and she can change the values of Y_i and e_i .

Note that one condition for these two models being equivalent is that Alice randomizes the phase of each pulse. It turns out that in some situations, this phase randomization procedure is crucial for security [66].

3.3 QKD hardware

Let us examine QKD system elements from a hardware point of view. In the model, we can see that there are a few key components: laser source, channel link and detection system. By having the knowledge of the characteristics of these components, we can fit the model and perform simulations.

3.3.1 Laser source

In QKD experiments, two types of laser pulses are mostly used: telecom wavelength ($\sim 1550\text{nm}$) and visible light ($\sim 760\text{nm}$). Note that the 1310nm light was also used for QKD experiments. For example, see Ref. [97]. Later, we will see that the choice of the wavelength, λ , determines the channel loss coefficient and detector efficiency.

3.3.2 Channel

There are mainly two types of QKD links: fiber and free space.

For fiber based QKD, the transmission distance is easy to vary. Thus, one can define the channel loss coefficient, β in dB/km, which characterizes the loss dependence on transmission distance. For example, the loss coefficient of telecom fiber is $\beta = 0.2$ dB/km. For the visible light, the fiber loss is high, $\beta = 2.5$ dB/km [113].

Since commonly used fibers are made of birefringent materials, it is difficult to maintain the polarization. Thus, phase encoding is widely used in fiber based QKD systems. Note that phase encoding¹ is equivalent to the polarization encoding [9].

For free space based QKD, in general, it is difficult to define β in dB/km. Instead, the total link loss in dB is commonly used. One main source of loss for the free space QKD implementation is the collection efficiency. Due to atmosphere scattering, the light beam is widened on the receiver arm. For a detailed discussion on how the atmosphere affects the light, one can refer to [86]. Note that the atmosphere is almost transparent to

¹In a phase encoding scheme, Alice encodes her information into the relative phase between two pulses [9].

the visible light and it is a good medium for polarization maintenance. Later, we will see that the detector efficiency for visible light is normally higher than the one for telecom wavelength. Thus, in general, visible light is commonly chosen for free space based QKD.

3.3.3 Detection

For a detection system, four parameters are important.

- η_B : detection efficiency, including detector efficiency and the internal transmission (coupling) efficiency of optical components inside Bob's box. The typical detection efficiency for a telecom wavelength² is $1 \sim 5\%$, while for a visible wavelength, it can be as high as 20%.
- Y_0 : background count rate (probability), including dark counts and other background contributions. Note that if two detectors are used in a QKD system, then Y_0 should be the sum of the dark count rates of the two detectors in addition to other background contributions.
- e_d : intrinsic detector error probability, which characterizes the alignment and stability of the optical system. In our model, we assume that e_d is independent of the transmission distance.
- repetition rate: in practice, the repetition rate of detectors limits the key transmission speed. The product of key rate R and repetition rate gives the key generation speed in bits/second. Normally, in an experiment, the laser pulses can be designed to be fast. The repetition rate is mainly limited by the detection system, e.g., the detector dead time and detection time-resolution.

In the model, we assume that there are two main sources of QBER, one from Y_0 , which depends on channel loss³ and the other from e_d , which is independent of channel loss.

Note that there are a few developments in building single photon detectors during recent years, such as superconducting materials based detectors [100] and up-conversion detectors [59, 111]

²Here, we consider a widely used detection system with single photon detectors based on InGaAs/InP avalanche photodiodes.

³This part is roughly determined by the ratio Y_0/η .

Later in the simulations, we use setup parameters from the QKD experiment completed by Gobby, Yuan and Shields (GYS) [32]. The key parameters of the experiment setup are listed in Table 3.1.

λ [nm]	β [dB/km]	η_B	e_d	Y_0
1550	0.21	4.5%	3.3%	1.7×10^{-6}

Table 3.1: Parameters of the QKD experiment setup from GYS [32].

Chapter 4

Decoy state

The decoy state method was first proposed by Hwang [40] to improve the performance of the coherent state QKD. We have proven the security of the QKD with decoy states [60, 72, 65] and demonstrated its practical advantage. In Hwang's original decoy state method, she suggested the use of a strong coherent state (with $\nu > \mu$) for decoy states. In contrast, we propose using weak coherent states. Subsequently, some practical decoy state protocols with only one or two decoy states are proposed [77]. We highlight that practical decoy state protocols were also proposed by Wang [123, 124], Harrington, Ettinger, Hughes and Nordholt [36].

The experimental demonstrations for the decoy state method have been completed recently [131, 132, 99, 115, 88, 129, 128]. Note that aside from the decoy state method, we also studied other methods to improve the QKD performance, such as the dual detector scheme [93].

This work is published in Ref. [65]. By collaborating with Hoi-Kwong Lo and Kai Chen, I apply the GLLP security analysis to a decoy state QKD. With the model described in Section 3.2, I simulate a QKD experiment [32] to show the improvement given by using decoy states.

4.1 Decoy state

In this section, we present the QKD with decoy states. By simulating a real experiment setup, we compare two cases: a decoy and non-decoy state QKD.

4.1.1 Motivation

As discussed in Section 2.5, in the GLLP security analysis, Alice and Bob need to determine the portion of tagged and untagged qubits to implement privacy amplification.

From Eq. (2.6), we can see that Q_μ and E_μ can be measured or tested from the experiment. Alice and Bob need to estimate Q_1 and e_1 to determine the amount of privacy amplification that is needed.

On the other hand, as we presented in Section 3.2, Eve has full control of the channel. Thus, she might block out single photon states, which is not good for her attack and make the channel transparent to the multi photon states. Thus, one pessimistic assumption is that all losses and errors come from a single photon state [70, 35]. That is, set $Y_i = 1$ and $e_i = 0$ for $i \geq 2$ in Eqs. (3.8) and (3.10). Thus, the estimations of Q_1 and e_1 without decoy states are:

$$\begin{aligned} Q_1 &\geq Q_\mu - \sum_{i=2}^{\infty} \frac{\mu^i}{i!} e^{-\mu} \\ e_1 &\leq \frac{E_\mu Q_\mu}{Q_1} \end{aligned} \tag{4.1}$$

Here, note that since Alice and Bob cannot distinguish vacuum (background) contribution and single photon state contribution¹, they have to consider these two states together. For a vacuum qubit, since it is a random state, $\delta_b = \delta_p = 1/2$. Thus, for the combined state (single photon state and vacuum state), we still have $\delta_b = \delta_p$.

Later in the simulation, we will see that the key rate and maximal secure distance of a coherent state QKD without decoy states are quite limited. In order to lower the amount of necessary privacy amplification, one needs to have a better estimation of Q_1 and e_1 . From Eq. (3.7), we know that in order to estimate Q_1 , one needs to estimate Y_1 . Therefore, the question is: *how can Alice and Bob estimate Y_1 and e_1 accurately?* This is the motivation of the decoy state scheme.

4.1.2 Solution

From the model described in Section 3.2, there are two observations. First, Y_i and e_i can be changed by Eve, so they are unknowns to Alice and Bob. Secondly, Q_μ and E_μ can be determined by Alice and Bob. Thus, Alice and Bob need to estimate Y_1 and e_1 by using the knowledge of Q_μ and E_μ . If Eqs. (3.8) and (3.10) are just considered, then Alice and

¹Or, they cannot estimate the detection contributions from vacuum qubits, Q_0 .

Bob have to assume the worst scenario: all losses and errors come from the single photon state.

We can see that Eqs. (3.8) and (3.10) are linear equations of Y_i and $Y_i e_i$. In addition to the regular signal state, if Alice sends out extra pulses with different intensities, μ , they will obtain more than one linear equation in the form of Eqs. (3.8) and (3.10). Here comes the key assumption of the decoy state method:

$$\begin{aligned} Y_i(\text{decoy}) &= Y_i(\text{signal}) \\ e_i(\text{decoy}) &= e_i(\text{signal}). \end{aligned} \tag{4.2}$$

These extra pulses are called *decoy states*. In the infinite decoy case [65], Alice and Bob perform an infinite number of decoy states, and then they can solve an infinite number of linear equations to obtain Y_1 and e_1 accurately. We call this case the infinite decoy state protocol. Here, note that with the infinite decoy state, one can strictly show [64] that the beam-splitting channel model discussed in Section 3.2.2 is a valid assumption.

An intuition on why this can be done: from Eqs. (3.8) and (3.10), we can see that the contribution from high order terms of Y_i and e_i converge to 0 exponentially². If one only focuses on Y_1 and e_1 , the number of unknowns can be chopped off to a finite number. In the next chapter, we will see that one or two decoy states are sufficient for practical use. In the simulation, we will use Eqs. (3.6) and (3.9) for the infinite decoy state case. For a detailed procedure of the decoy state method, one can refer to Section 5.4.2.

In the following discussion, μ always refers to the intensity (expected photon number) of the signal state used for real key transmission. We will use ν for the expected photon number of decoy states.

4.1.3 Discussion

In a large parameter regime when the background contribution can be negligible and the error rate is not large, the key rate is roughly in the order of $R = O(\mu\eta)$ from Eq. (2.6).

In Appendix B.1.1, we show that the optimal μ for the non-decoy state case is $\mu = O(\eta)$. Thus, the key rate is $R = O(\eta^2)$. That is, the key rate is quadratically dependent on the channel transmission. Note that in general, the channel transmission is quite low, typically less than 1%. This is the intrinsic reason why the performance of a QKD without decoy states is very limited.

²Actually, $n!$ is quicker than exponential convergence.

On the other hand, in Appendix B.1.1, we show that the optimal μ for the infinite decoy state case is $\mu = O(1)$. Thus, the key rate is $R = O(\eta)$. That is, the key rate is linearly dependent on the channel transmission. Note that even with a perfect single photon source, the highest order the key rate can reach is $R = O(\eta)$. Hence, with decoy states, one can treat a weak coherent state as a good single photon source for a QKD.

Note that this conclusion is also true for other photon sources, e.g., triggering PDC sources [76], see discussions in Chapter 7.

4.1.4 Simulation

We simulate a recent coherent state QKD experiment [32]. This is to compare the cases with and without decoy states. The parameters of the experiment setup are listed in Table 3.1.

For both cases, the key rate formula is the same, see Eq. (2.6). By using the Cascade protocol [16], the error correction efficiency is $f(E_\mu) = 1.22$. The gain Q_μ and QBER E_μ can be measured or tested from the experiment. Therefore, for both cases, we use the same formulae, Eqs. (3.8) and (3.10). The estimations of Q_1 and e_1 are different. For the case without decoy states, we use the formulae of Eq. (4.1). For the case with decoy states, we assume that Alice and Bob can estimate Q_1 and e_1 accurately. In the simulation, we use the formulae of Eqs. (3.6) and (3.9).

As shown in Appendix B.1, we choose $\mu = 0.48$ for the case with decoy states and $\mu = \eta$ for the case without decoy states. The simulation result is shown in Figure 4.1.

From the simulation result, we can see that the decoy state method can improve the QKD performance dramatically.

1. With decoy states, the maximal distance can reach 142 km. For comparison, we find that with the prior art method, the maximal secure distance is only about 32 km.
2. At 0 km distance, the key rates for decoy and no decoy cases are: 2.55×10^{-3} and 7.97×10^{-5} . As we can clearly see, the gap between two curves increases when the distance increases.
3. By comparing the upper bound of the key rate, which is discussed in the next section, one can see that in a large parameter regime (for instance, the distance between 0 km and 120 km), the decoy state protocol can achieve a close performance as the upper bound shown in Section 4.2.2.

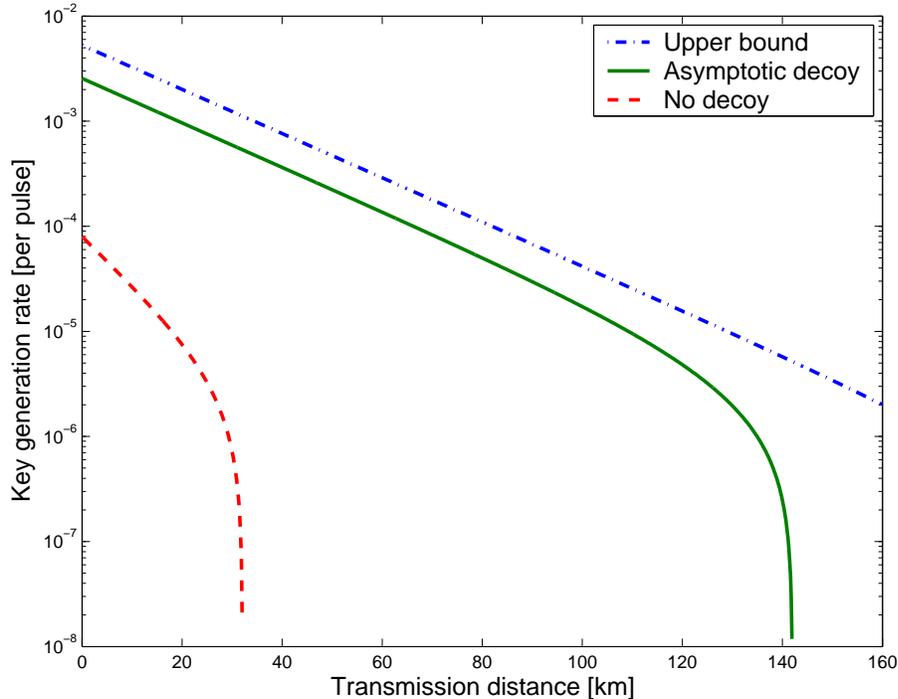


Figure 4.1: Plot of the key rate as a function of the transmission distance, comparing the coherent state QKD with decoy states and without decoy states. The calculation of the upper bound is shown in Section 4.2.2. The experiment setup parameters are listed in Table 3.1.

4. We checked that our results are stable to small perturbations of the background count rate Y_0 and average photon number μ (both up to a 20% change).

4.2 Upper Bounds

As we mentioned in Section 1.2.2, we are interested in maximizing two quantities, key rate and maximal secure distance. In this section, we investigate the upper bounds of these two quantities. By comparing the upper bound performance and the decoy state QKD performance, we want to investigate how much room is left for further improvement.

4.2.1 Distance upper bound

Due to a simple intercept-and-resend attack, an upper bound on the bit error rate of the BB84 protocol with single photon states is 25%. The maximal secure distance then can be bounded by the distance when the bit error rate of the single photon states e_1 reaches

25%. According to our model, Eq. (3.9):

$$e_1 = \frac{e_d \eta + \frac{1}{2} Y_0}{\eta + Y_0}$$

where e_d is the intrinsic error rate of Bob's detectors, η is the overall transmittance, and Y_0 is the background rate. Thus, e_1 exceeds 25% when

$$\eta \leq \frac{0.25 Y_0}{0.25 - e_d}. \quad (4.3)$$

In GYS [32]'s case, the upper bound of the secure distance is 208 km by considering the parameters listed in Table 3.1.

4.2.2 Key rate upper bound

As for the BB84 protocol, the final secure key can only be derived from single photon qubits. To derive the upper bound of a key generation rate, we assume that Alice and Bob can distinguish the single photon qubits from other qubits (vacuum and multi photon qubits). Therefore, they can perform the classical data post-processing only onto the single photon qubits. One simple upper bound³ of key generation rate is given by the *mutual information* between Alice and Bob [83]:

$$R^U = Q_1 [1 - H_2(e_1)], \quad (4.4)$$

where Q_1 and e_1 are the gain and error rate of single photon states, respectively. The simulation result is shown in Figure 4.1.

Note that the above two upper bounds, Eqs. (4.3) and (4.4), rely on two assumptions.

- Alice and Bob cannot distinguish background counts and true signal counts. That is, they cannot decouple e_d from e_1 in Eq. (3.9).
- A secure key can only be extracted from single photon states. This is true for BB84 and many other protocols. An exception is the SARG04 protocol [101].

Note that these two bounds are general upper bounds, regardless of the technique used for combating the effect of imperfect devices, such as the decoy state technique.

³Note that this upper bound is true for any post-processing (based on 1-LOCC or 2-LOCC) Alice and Bob use in BB84.

4.3 Discussion

First, from the simulation, we can see that the decoy state technique can dramatically improve the QKD performance. Later, we will discuss practical protocols for the decoy state QKD and experiment demonstrations. From there, we show that the decoy state method is highly practical.

In comparison to the key rate upper bound, in a large distance regime (for instance, the distance between 0 km and 120 km), the decoy state protocol achieves a close performance to the theoretical limit. Compared to the maximal secure distance upper bound, 208 km, there is a 60 km gap between the theoretical limit and decoy state protocol. Later, by combining two-way classical communication post-processing schemes, we push this maximal secure distance for the infinite decoy state protocol beyond 180 km. From here, we can see that the decoy state protocol pushes the QKD performance close to the theoretical limit.

Therefore, we expect the decoy state protocol to be a standard technique for prepare-and-measure QKD scheme implementations.

Let us recap the key assumptions underlying the security proof for the decoy state QKD: first, there is the squash model and secondly, there is the assumption that Eve cannot distinguish decoy and signal states during key transmission. The second assumption is equivalent to Eq. (4.2). Later in Section 5.4, we can see that verifying this assumption is a nontrivial task in real experiments. On the other hand, in Chapter 7, we show that this assumption can be loosened by using other single photon sources.

Chapter 5

Practical decoy state

In this chapter, we will discuss practical proposals of the decoy state QKD and experimental demonstrations. Here again, we will focus on the coherent state BB84 QKD.

The work of practical decoy state proposals is published in Ref. [77]. In this work, I apply the idea of the Vacuum+Weak decoy state protocol, which was first proposed by Lo [60], and consider statistical fluctuations. Here, I would like to highlight the theoretical contributions to the practical decoy state QKD from other groups [36, 123, 124].

The work for the experimental demonstration is published in Refs. [131, 132]. In this work, I designed the experimental parameters and analyzed data in the decoy state QKD experiment demonstration. Here, I would like to highlight the experimental demonstrations completed by other groups [131, 132, 99, 115, 88, 129, 128].

Note that aside from the decoy state method, we also studied other methods to improve the QKD performance, such as the dual detector scheme [93].

5.1 Practical proposals

The general question in a decoy state scheme with m decoy states can be described by the following mathematical question.

Question: Given $2(m + 1)$ constraints in the form of Eqs. (3.8) and (3.10), how do we obtain the lower bound of R given by Eq. (2.6)?

When $m \rightarrow \infty$, Alice and Bob can solve Y_1 and e_1 accurately, in principle. This is the infinite case described in Section 4.1.

In the following, we will present three practical decoy methods, the Vacuum+Weak decoy state and one decoy state, and a numerical method. For a general discussion of the

two decoy state methods, one can refer to Ref. [77]. Note that in Ref. [77], we proved that the Vacuum+Weak decoy state protocol is optimal within the two decoy state methods.

5.1.1 Vacuum+Weak decoy

In this method, two decoy states are performed to bound Y_1 and e_1 separately. First, Alice and Bob implement a vacuum decoy state where Alice simply shuts off her photon source. In this case, all detections that Bob obtains are background counts

$$\begin{aligned} Q_{vacuum} &= Y_0 \\ E_{vacuum} &= e_0 = \frac{1}{2}. \end{aligned} \quad (5.1)$$

The background counts occur randomly, thus its error rate is $e_0 = 1/2$. The vacuum decoy state allows Alice and Bob to estimate the background rate Y_0 .

Secondly, they perform a weak decoy state where Alice uses a weaker intensity ν ($\nu < \mu$) for the decoy state. In this case, Bob's detections mainly come from two parts: background and single photon contributions. This is because when the intensity is weak, the probability of obtaining a multi photon state is small. With the estimation from the vacuum decoy state, one can estimate Y_1 and e_1 from the weak decoy state.

Now, let us strictly solve the problem. The gains of the signal state and decoy state are given by Eq. (3.8)

$$\begin{aligned} Q_\mu e^\mu &= Y_0 + \mu Y_1 + \frac{\mu^2}{2} Y_2 + \frac{\mu^3}{3!} Y_3 + \dots \\ Q_\nu e^\nu &= Y_0 + \nu Y_1 + \frac{\nu^2}{2} Y_2 + \frac{\nu^3}{3!} Y_3 + \dots \end{aligned} \quad (5.2)$$

Considering $\mu^2 Q_\nu e^\nu - \nu^2 Q_\mu e^\mu$, we find that:

$$\mu^2 Q_\nu e^\nu - \nu^2 Q_\mu e^\mu = (\mu^2 - \nu^2) Y_0 + \mu\nu(\mu - \nu) Y_1 + \mu^2 \nu^2 \frac{\nu - \mu}{3!} Y_3 + \dots, \quad (5.3)$$

thus:

$$Y_1 \geq Y_1^L = \frac{\mu}{\mu\nu - \nu^2} (Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0) \quad (5.4)$$

since $\nu < \mu$ and all $Y_i \in [0, 1]$.

The upper bound of e_1 can be simply derived by Eq. (3.10):

$$e_1 \leq e_1^U = \frac{E_\nu Q_\nu e^\nu - e_0 Y_0}{Y_1^L \nu}. \quad (5.5)$$

Substituting the normal case (without Eve) values, Eqs. (3.11), into these estimations, in the limit of $\nu \ll \mu$, we get:

$$\begin{aligned} Y_1^L &\rightarrow \eta + Y_1 \\ e_1 Y_1 &\rightarrow e_0 Y_0 + e_d \eta \end{aligned} \quad (5.6)$$

which is consistent with the expected value given by Eqs. (3.6) and (3.9). Thus, asymptotically, the Vacuum+Weak decoy method gives a tight lower bound of the key rate. In other words, the infinite decoy state protocol described in Section 4.1 is the asymptotic limit of the Vacuum+Weak decoy state protocol.

Now let us examine how good these two bounds are by using the parameters listed in Table 3.1. Here, we define the deviation of the bounds:

$$\begin{aligned} \beta_{Y_1} &\equiv \frac{Y_1 - Y_1^L}{Y_1} \\ \beta_{e_1} &\equiv \frac{e_1^U - e_1}{e_1}. \end{aligned} \quad (5.7)$$

The simulation result is shown in Figure 5.1.

From the simulation, we can see that both deviations are relatively independent of the channel transmission distance. The deviation of e_1^U is larger than the one of Y_1^L . The choice of a weak decoy state ν is not very constrained since even with $\nu/\mu \approx 1/4$, the deviation is small. In Table 5.1, we can see that with $\nu/\mu \approx 1/4$, the key rate from the Vacuum+Weak decoy state protocol achieves a very close performance of the infinite decoy state case.

Distance	Y_1	e_1	R_{inf}	Y_1^L	e_1^U	R_{vw}
0 km	4.50×10^{-2}	3.30%	2.55×10^{-3}	4.34×10^{-2}	3.88%	2.19×10^{-3}
70 km	1.53×10^{-3}	3.35%	8.28×10^{-5}	1.47×10^{-4}	3.95%	6.99×10^{-5}
130 km	8.55×10^{-5}	4.23%	1.96×10^{-6}	8.23×10^{-5}	4.91%	1.24×10^{-5}

Table 5.1: List of the simulation results for three distances: 0 km, 70 km and 130 km, comparing the Vacuum+Weak protocol with the case of the infinite (asymptotic) decoy state. For both protocols, we use $\mu = 0.48$. For the Vacuum+Weak decoy state protocol, we use $\nu = 0.13$. Parameters of the QKD experiment setup are listed in Table 3.1.

Here, we compare Eqs. (3.6), (3.9), (5.4) and (5.5) by simulating the GYS experiment. We can see that the deviation of the key rate given by the Vacuum+Weak decoy state protocol and infinite decoy state protocol increases when the distance reaches the maximal secure distance. Similar to the conclusion from Figure 5.1, the deviation of Y_1^L from Y_1 is small throughout the whole distance regime.

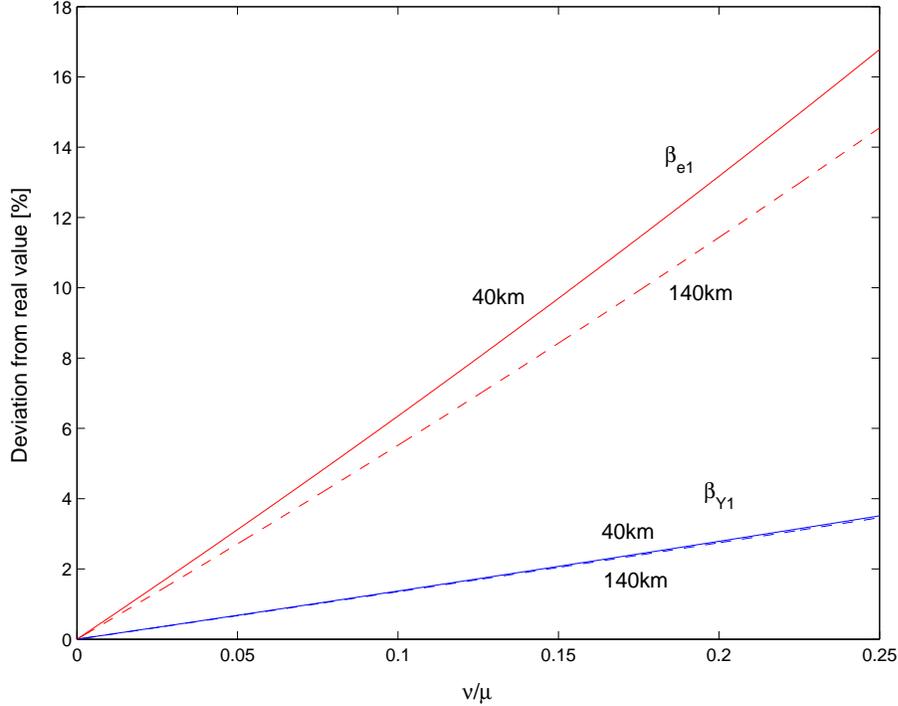


Figure 5.1: Plot of the relative deviations of Y_1^L and e_1^U from the expected values (i.e., the case $\nu \rightarrow 0$) as functions of ν/μ with the fiber length 40 km (solid lines) and 140 km (dashed lines). The bounds Y_1^L and e_1^U are given by Eqs. (5.4) and (5.5), and the expected values are given by Eqs. (3.6) and (3.9). We consider the Vacuum+Weak protocol here. The expected photon number is $\mu = 0.48$ from the optimization calculation of Eq. (B.4) in Appendix B.1.2. The experiment setup parameters are from GYS [32], listed in Table 3.1.

5.1.2 One decoy

In some realistic situations, a vacuum decoy state may not be easy to perform, or the background count rate cannot be estimated accurately due to the fact that Y_0 is small (typically 10^{-5}). Consequently, one needs to consider a case without the vacuum decoy state. That is, Alice and Bob only perform a weak decoy state.

We treat the one decoy state method as an imperfect case of the Vacuum+Weak method. Assume that Alice and Bob perform the Vacuum+Weak decoy method, but they prepare very few states as vacuum decoy states. Therefore, they cannot estimate Y_0 very well. The one decoy protocol is the same as a Vacuum+Weak decoy state protocol, except that the value of Y_0 is unknown. Since Alice and Bob do not know Y_0 , Eve can pick Y_0 as she wishes. We argue that, on physical grounds, it is advantageous for Eve to pick Y_0 to be zero. This is because Eve may gather more information on the single-

photon signal than the vacuum. Therefore, the bound for the case $Y_0 = 0$ should apply to our one decoy protocol. For this reason, Alice and Bob can derive a bound on the key generation rate, R , by substituting $Y_0 = 0$ in Eqs. (5.4) and (5.5).

Mathematically, one can treat Y_0 as an unknown variable in Eqs. (5.4) and (5.5), and determine the lower bound of the key generation rate, Eq. (2.6), for all possible Y_0 . By taking the derivative of Eq. (2.6), one can find that

$$\begin{aligned} Y_1^{trial} &= \frac{\mu}{\mu\nu - \nu^2} (Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2}) \\ e_1^{trial} &= \frac{E_\nu Q_\nu e^\nu}{Y_1^{trial} \nu} \end{aligned} \quad (5.8)$$

gives a lower bound of the key rate.

Later, in the next subsection, we will present a numerical method to estimate the key rate R . Now we can compare Eq. (5.8) with the numerical method by simulating the GYS experiment. In this case, we consider three distances: 0 km, 70 km and 130 km.

Distance	Y_1^{trial}	e_1^{trial}	R_{one}	Y_1^{num}	e_1^{num}	R_{num}
0 km	4.34×10^{-2}	3.89%	2.19×10^{-3}	4.36×10^{-2}	3.84%	2.22×10^{-3}
70 km	1.48×10^{-3}	4.40%	6.55×10^{-5}	1.48×10^{-3}	3.76%	7.26×10^{-5}
130 km	9.93×10^{-5}	13.0%	0	8.33×10^{-5}	4.34%	1.65×10^{-6}

Table 5.2: List of simulation results for three distances: 0 km, 70 km and 130 km, comparing the one decoy state protocol with the numerical optimization method shown in the next subsection. For both protocols, we use $\mu = 0.48$ and $\nu = 0.13$. Parameters of the QKD experiment setup are listed in Table 3.1.

By comparing Tables 5.1 and 5.2, we can see that the numerical method, shown in the next subsection, can give the highest key rate of the three practical decoy state protocols. However, note that all four methods; infinite decoy, Vacuum+Weak, one-decoy and numerical method, achieve a close QKD performance in a large parameter regime. Here, we have not considered the statistical fluctuations. After considering the statistical fluctuations, the simulation result is shown in Figure 5.3.

5.1.3 Numerical method

Both the Vacuum+Weak and one decoy state protocols presented above bound Y_1 and e_1 separately. With reference to the original question that we were trying to solve in

the beginning of this section, what we really want to bound is the key rate of Eq. (2.6) instead of Y_1 and e_1 separately.

One natural practical decoy state protocol will be a numerical solution to the question stated in the beginning of this section. To do that, one need to find the lower bound R of Eq. (2.6) given the constraints of Eqs. (3.8) and (3.10):

$$\begin{aligned}
Q_\mu e^\mu &= Y_0 + \mu Y_1 + \frac{\mu^2}{2} Y_2 + \frac{\mu^3}{3!} Y_3 + \dots \\
Q_\nu e^\nu &= Y_0 + \nu Y_1 + \frac{\nu^2}{2} Y_2 + \frac{\nu^3}{3!} Y_3 + \dots \\
E_\mu Q_\mu e^\mu &= Y_0 e_0 + \mu Y_1 e_1 + \frac{\mu^2}{2} Y_2 e_2 + \frac{\mu^3}{3!} Y_3 e_3 + \dots \\
E_\nu Q_\nu e^\nu &= Y_0 e_0 + \nu Y_1 e_1 + \frac{\nu^2}{2} Y_2 e_2 + \frac{\nu^3}{3!} Y_3 e_3 + \dots .
\end{aligned} \tag{5.9}$$

The difference between the Vacuum+Weak and one decoy state protocols is whether Y_0 is known or not.

In order to solve this question numerically, one needs to put a cut-off of Y_i and e_i . Later in the simulation, we will consider a cut-off of $i = 20$. That is, $Y_i = e_i = 0$ for $i \geq 20$. Note that for $i = 20$ and $\mu = 1$, the probability is $P(20) = 1.51 \times 10^{-19}$ according to the Poisson distribution of the source photon number given by Eq. (3.3). For a reasonable finite key transmission, the higher order terms can be neglected.

We present the numerical solutions in Table 5.3 by using the parameters in Table 3.1.

Distance	Y_1	Y_2	Y_3	e_1	e_2	R
0 km	4.36×10^{-2}	1.15×10^{-1}	5.86×10^{-13}	3.84%	5.86×10^{-13}	2.22×10^{-3}
70 km	1.48×10^{-3}	4.01×10^{-3}	5.45×10^{-4}	3.76%	4.47×10^{-3}	7.26×10^{-5}
130 km	8.33×10^{-6}	2.15×10^{-5}	5.86×10^{-13}	4.34%	3.17%	1.65×10^{-6}

Table 5.3: Comparison of the numerical result with the infinite decoy state (asymptotic) case and the Vacuum+Weak protocol. For all three protocols, we use $\mu = 0.48$. For the two practical decoy state protocol, we use $\nu = 0.1$. Parameters of the QKD experiment setup from GYS [32].

Here, we have not considered the statistical fluctuations. From Table 5.3, we have following remarks:

1. If we only consider Eq. (5.4), Eve's optimal attack will be setting $Y_i = 0$ for $i \geq 3$. However, if we consider the numerical decoy state method as shown in Table 5.3,

Eve might choose $Y_i \neq 0$ for $i \geq 3$ ¹.

2. The result for the numerical decoy state method is relatively stable with a choice of a cut-off n . If we choose $n = 30$ or $n = 40$, the result fluctuates within 3%. Note that the numerical optimization algorithm that we used here might not be optimal.

5.2 Statistical fluctuation analysis

In this section, we will discuss the effect of finite data size on our estimation process for Y_1 and e_1 . We will also discuss how statistical fluctuations might affect our choice of the weak decoy state intensity ν .

All real-life experiments are implemented within a finite period of time. Ideally, we would like to consider a QKD experiment that can be performed within, for instance, a few hours or so. This means that the experiment data size is finite. Shortly, we will see that the statistical fluctuation analysis is a rather complex problem. We do not have a full solution to the problem. Nonetheless, we will provide some rough estimation based on the standard error analysis which suggests that the statistical fluctuation problem of the practical decoy state methods for a QKD experiment appears to be under control, if the experiment is run over only a few hours.

5.2.1 What parameters are fluctuating?

Recall that in Eq. (2.6), there are four key parameters: the gain Q_μ and QBER E_μ of the signal state and the gain Q_1 and error rate e_1 of the single photon state.

After key transmission, Bob can count the exact number of clicks and knows the total number of pulses. Hence, the gain of signal state Q_μ , the ratio of the aforementioned two numbers, is measured directly from the experiment. Therefore, they do not need to consider the fluctuation of Q_μ .

In practice, Alice and Bob do not really need to sacrifice testing bits to estimate E_μ . They can directly apply some classical error correction code, for instance, the Cascade [16] code, to correct all bit errors. Then they check whether the error correction is successful or not². Afterwards, they can calculate (if necessary) E_μ by counting the number of errors. Thus, there is no fluctuation for E_μ as well.

¹In the numerical result, we find that Y_3 is always relatively small in comparison to Y_2 , but the values of Y_i for $i \geq 4$ are in the same order of Y_2 .

²This can be done efficiently by random parity check.

Thus, there is no fluctuation in the error correction part. The difficult part of the statistical fluctuation analysis is in the privacy amplification part. In the following discussion, we will focus on the statistical fluctuation analysis of the Vacuum+Weak decoy state method. To show the complexity of the problem, we will now discuss the following five sources of fluctuations.

1. In practice, the intensity of the lasers used by Alice will be fluctuating. In other words, even the parameters μ and ν suffer from fluctuations. Without hard experimental data, it is difficult to pinpoint the extent of their fluctuations. Furthermore, the source may not even be a strict coherent state. To simplify our analysis, we will ignore their fluctuations in this thesis.
2. Up until now, in our analysis, we have assumed that the distribution of the photon number eigenstates (Fock states) in each type of state is fixed, see Eq. (3.3). For instance, if N signal states of intensity μ are emitted, we assume that exactly $N\mu e^{-\mu}$ out of the N signal states are single photons. In real-life, the value of $\mu e^{-\mu}$ is only a probability, the actual number of single photon signals will fluctuate statistically. This fluctuation is dictated by the law of large number. Hence, this problem should be solvable³. For simplicity, we will neglect this source of fluctuations in this thesis.
3. The yield Y_i may fluctuate in the sense that Y_i for the signal state might be slightly different from Y'_i of the decoy state. Note that if one uses the vacuum state as one of the decoy states, then by observing the yield of the vacuum decoy state, conceptually, one has a very good handle on the yield of the vacuum component of the signal state (in terms of hypergeometric functions). However, note that the background rate is generally rather low (typically 10^{-5}). Therefore, to obtain a reasonable estimation on the background rate, a rather large number (for instance, 10^7) of the vacuum decoy states will be needed⁴. Note that, with the exception of the case $i = 0$ (the vacuum case), neither Y_i and Y'_i are directly observable in an experiment. In a real experiment, one can measure only some *averaged* properties. For instance, the gain Q_μ of the signal state, which can be experimentally mea-

³It was subsequently pointed out to us by Gottesman and Preskill that the above two sources of fluctuations can be combined into the fluctuations in the photon number frequency distribution of the underlying signal and decoy states. These fluctuations will generally be averaged out to zero in the limit of a large number of signals, provided that there is no systematic error in the experimental set-up.

⁴As noted in Ref. [65], even a 20% fluctuation in the background will have a small effect on the QKD performance.

sured, has its origin as the weighted averaged yields of the various photon number eigenstates Y_i s whereas the Q_ν for the decoy state is given by the weighted averaged of Y_i' s. Relating the observed averaged properties, e.g., Q_μ , to the underlying values of Y_i s is a challenge. In summary, owing to the fluctuations of Y_i for $i \geq 1$, it is not clear to us how to derive a closed form solution to the problem.

4. The error rates, e_i s, for the signal can also be different from the error rates e_i s for the decoy state, due to underlying statistical fluctuations. Actually, the fluctuation of e_1 appears to be the dominant source of errors in the estimation process. (See, for example, Table 5.4.) This is because the parameter e_1 is rather small (for instance, a few percent) and it appears in combination with another small parameter Y_1 in Eq. (3.10) for QBER.
5. In the GLLP analysis [35] shown in Eq. (2.6), Alice and Bob need to correct phase errors, other than bit-flip errors. From Shor-Preskill's proof [106], we know that the bit-flip error rate and the phase error rate are suppose to be the same only in the asymptotic limit. Therefore, for a finite data set, one has to consider statistical fluctuations. This problem is well studied [106]. Since the number of signal states is generally very large, we will ignore this fluctuation from now on.

Qualitatively, the yields of the signal and decoy states tend to decrease exponentially with distance. Therefore, statistical fluctuations tend to become more and more important as the transmission distance of QKD increases. In general, as the distance of QKD increases, an increasingly larger data size will be needed for the reliable estimation of Y_1 and e_1 (and hence R), thus requiring a longer QKD experiment.

Here, we will neglect the fluctuations due to the first two and the fifth sources listed above. Even though we cannot find any closed form solution for the third and fourth sources of fluctuations, it should be possible to tackle the problem by simulations. Here, we are content with a more elementary analysis. We will simply apply a standard error analysis to perform a rough estimation on the effects of fluctuations due to the third and fourth sources. Note that the origin of the problem is strictly classical statistical fluctuations. There is nothing quantum in this statistical analysis. While standard error analysis (using essentially normal distributions) may not give a completely correct answer, we expect that it is correct at least in the order of magnitude.

Our estimation, which will be presented below, shows that for a long-distance (> 100 km) QKD with our Vacuum+Weak decoy state protocol, the statistical fluctuations effect

(from the third and fourth sources only) appears to be manageable. This is so, provided that a QKD experiment is run for a reasonable period of time of only a few hours. Our analysis supports the viewpoint that our Vacuum+Weak decoy state protocol is practical for real-life implementations.

We remark on passing, that the actual classical memory space requirement for Alice and Bob is rather modest ($< 1GBytes$) because at long distances, only a small fraction of the signals will give rise to detection events.

We emphasize that we have not fully solved the statistical fluctuation problem for the decoy state QKD. This problem has turned out to be quite complex. There is other work being done to address the statistical fluctuation problem in the decoy state QKD [123, 37].

5.2.2 Standard Error Analysis

In the following, we will present a general procedure for studying the statistical fluctuations (due to the third and fourth sources noted in the previous subsection) by using the standard error analysis.

Denote the number of pulses (sent by Alice) for signal as N_s , for the vacuum decoy state as N_{vac} and for the weak decoy state as N_w . Then, the total number of pulses sent by Alice is given by:

$$N = N_s + N_{vac} + N_w. \quad (5.10)$$

Following that, the parameter q in Eq. (2.6) is given by:

$$q = \frac{N_s}{2N}. \quad (5.11)$$

Here, we assume that Alice and Bob perform standard BB84, so there is a factor of $1/2$.

In practice, since N is finite, the statistical fluctuations of Q_1 and e_1 cannot be neglected. All these additional deviations will be related to data sizes N_s , N_{vac} and N_w and in principle, can be obtained from statistic analysis. A natural question prompted by such is as follows. Given the total data size $N = const$, how do we distribute it to N_s , N_{vac} and N_w for maximizing the key generation rate R ? This question also relates to another one: how do we choose an optimal weak decoy ν to give a good lower bound of R ?

In principle, our optimization procedure should look like the following. First, one needs to derive a lower bound of Q_1 and an upper bound of e_1 (as functions of data size N_s , N_{vac} , N_w and ν), taking into account statistical fluctuations. Secondly, one

substitutes these bounds into Eq. (2.6) to calculate the lower bound of the key generation rate, denoted by R^L . Thus, the key rate lower bound R^L is a function of N_s , N_{vac} , N_w and ν , and will be maximized when the optimal distribution satisfies

$$\frac{\partial R^L}{\partial N_s} = \frac{\partial R^L}{\partial N_{vac}} = \frac{\partial R^L}{\partial N_w} = 0, \quad (5.12)$$

given that $N = N_s + N_{vac} + N_w = \text{const.}$

In this statistical fluctuation analysis, our assumptions are as follows:

1. Alice knows the exact value of the average photon pair number μ and ν , which is a fixed number during key transmission.
2. The distribution of the photon number, Eq. (3.3), does not fluctuate.
3. Assume that the QKD transmission is part of an infinite length experiment. Hence, $Q_\mu(E_\mu)$ can be regarded as a tested value of the true gain (QBER). Thus, we can use the standard error analysis to address statistical fluctuations.

5.2.3 Choice of N_s , N_{vac} , N_w and ν

From the theoretical deviations of Y_1 and e_1 , shown in Figure 5.1, reducing ν may decrease the theoretical deviations. On the other hand, given a fixed N_w , reducing ν will decrease the number of detection events of the decoy states, which in turn, causes a larger statistical fluctuation. Thus, for fixed N_s , N_{vac} and N_w , there exists an optimal choice of ν which maximizes the lower bound of the key generation rate R^L :

$$\frac{\partial R^L}{\partial \nu} = 0$$

which can be simplified to:

$$\frac{\partial}{\partial \nu} \{ \hat{Y}_1^L [1 - H_2(\hat{e}_1^U)] \} = 0 \quad (5.13)$$

where \hat{Y}_1^L and \hat{e}_1^U are lower bound to Y_1 and upper bound to e_1 when statistical fluctuations are considered.

As defined in Eq. (5.11), choosing a larger N_s leads to a larger factor q in Eq. (2.6). On the other hand, choosing large values of N_{vac} and N_w can help with better estimations of Y_1 and e_1 . Thus, there is trade-off between N_s , N_{vac} and N_w . In order to achieve an optimal R , one needs to choose an appropriate set of values N_s , N_{vac} , N_w and ν . Given the total data size in Eq. (5.10), in principle, one can solve Eqs. (5.12) and (5.13) to get N_s , N_{vac} , N_w and ν . In the later simulation, we will numerically optimize these four parameters.

5.3 Simulation

In practice, solving Eq. (5.12) is a complicated problem. One problem that we have mentioned in Section 5.2.1 is that the relations between N_s , N_{vac} , N_w and estimations of Q_1 and e_1 are difficult to describe strictly. In the following, we will be content with a rough estimation procedure using the standard error analysis. We will focus the Vacuum+Weak decoy method.

One observation is that Alice and Bob should compare all their detection events of decoy states publicly. In principle, they can also use decoy states to generate the final key. Note that the signal state is chosen to be optimal for key rate generation. In other words, decoy states are not as efficient as signal states to generate the final key. Therefore, it is more efficient for Alice and Bob to use decoy states only for estimations of Y_1 and e_1 .

Two assumptions:

1. We assume that the decoy state used in the actual experiment is conceptually only a part of an infinite population of decoy states. There are underlying values for Q_ν and E_ν as defined by the population of decoy states. In each realization, the decoy state allows us to obtain some estimates for those underlying Q_ν and E_ν . Alice and Bob can use the fluctuations of Q_ν , E_ν to calculate the fluctuation of the estimates of Y_1 and e_1 .
2. When the number of events (e.g. the total detection event of the vacuum decoy state) is large (for instance, > 50), we assume that the statistical characteristic of a parameter can be described by a *normal* distribution.

We will use the experiment parameters in Table 3.1, and show numerical solutions of Eqs. (5.10), (5.12) and (5.13). We pick the total data size (the number pulses sent by Alice) to be $N = 6 \times 10^9$. The GYS experiment [32] has a repetition rate of 2 MHz and an uptime of around 50%⁵. Therefore, it should take only a few hours to perform our proposed experiment. The optimal $\mu = 0.48$ can be calculated by Eq. (B.4) and we use $f(e) = 1.22$.

In a fiber length of 103.6 km ($\eta = 3 \times 10^{-4}$), the optimal weak decoy state intensity ν , pulses distribution of data, and the deviations from the infinite decoy method are listed in Table 5.4.

⁵Z. L. Yuan, private communication.

l	μ	u	N	N_s	N_{vac}	N_w
103.62 km	0.479	10	6×10^9	3.98×10^9	1.76×10^9	2.52×10^8
η	ν	$\tilde{B}[\text{bits}]$	β_{Y0}	β_{Y1}	β_{e1}	β_R
3×10^{-4}	0.127	2.17×10^4	48.31%	7.09%	97.61%	74.11%

Table 5.4: List of the optimal choice of ν and pulse number distribution for the Vacuum+Weak decoy state protocol with statistical fluctuation analysis. The pulse number distribution, N_s , N_{vac} and N_w , is calculated by Eq. (5.12). The optimal weak decoy state intensity is calculated by Eq. (5.13). \tilde{B} is the lower bound of the number of the final key bits. All results are obtained by numerical programming using MatLab. The variable β_{Y1} denotes the relative deviation in our estimation process of Y_1 from its true value by using the data from a finite experiment. This relative deviation originates from finite data with statistical fluctuations. This definition contrasts with the definition of β_{Y1} in Eq. (5.7) which refers to the relative difference between the values of Y_1 for case i) where ν is finite and case ii) where ν approaches zero. Similarly, other β s denote the relative deviations in our estimates for the corresponding variables in the subscript of β . We assume that all the statistical fluctuation belongs to the confidence interval of $u = 10$ standard deviations (i.e., $1 - 1.5 \times 10^{-23}$). The experiment parameters are listed in Table 3.1.

For any fiber length, we can solve Eqs. (5.12) and (5.13) to get N_s , N_E , N_{vac} , N_w and ν . Figure 5.2 shows how the optimal ν changes with transmission distance.

We have a few remarks on Figure 5.2, optimal ν versus transmission distance.

1. The optimal ν is small ($\sim 0.1 < \mu$) through the whole distance. In fact, it starts at a value $\nu \approx 0.04$ at zero distance and increases with the transmission distance.
2. There is small flat step at distance of 82 km. This is due to the fact that the vacuum decoy state becomes useful. From 0 km to 82 km transmission distance regime, the optimal pulse number for the vacuum decoy state N_{vac} is 0. That is, in this regime, one should use the one decoy state protocol instead of the Vacuum+Weak protocol⁶ protocol.
3. As the transmission distance increases, the optimal ν increases. This is reasonable because in a longer distance, the total transmittance η is low, thus Alice and Bob

⁶Actually, we did this simulation first and found this strange behavior at a distance of 82 km. Then we came up with the one decoy state protocol.

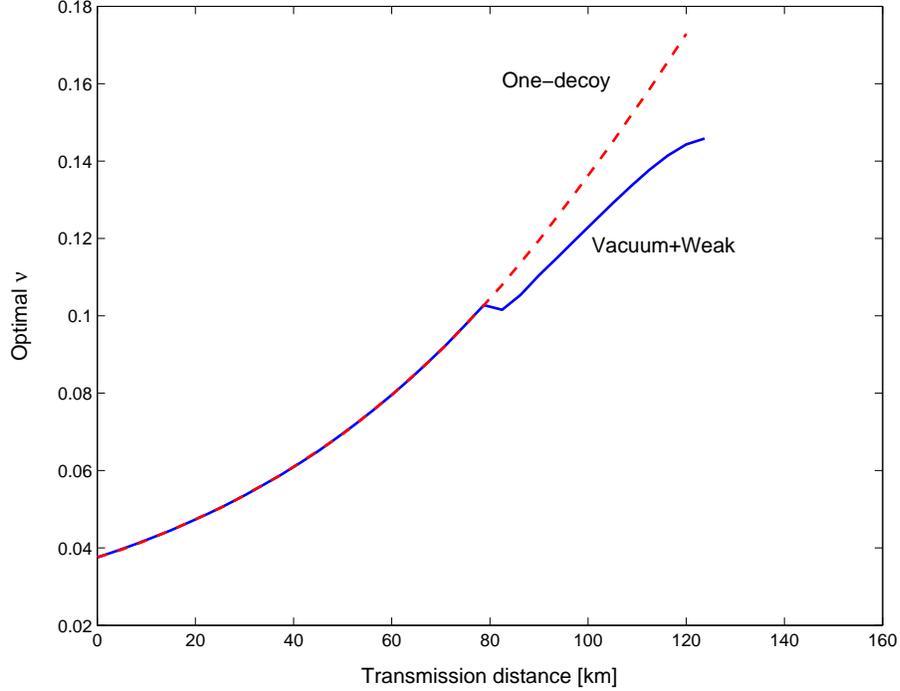


Figure 5.2: Plot of optimal ν versus transmission distance. The solid line shows the simulation result of the Vacuum+Weak protocol (Eqs. (5.4) and (5.5)) with statistical fluctuations. The dashed line shows the result for the one decoy state method (Eq. (5.8)). Here, we pick the data size (total number of pulses emitted by Alice) to be $N = 6 \times 10^9$. We find the optimal ν s for each fiber length by numerically solving Eqs. (5.10), (5.12) and (5.13). The confidence interval for statistical fluctuation is 10 standard deviations (i.e., $1 - 1.5 \times 10^{-23}$). The simulation parameters are listed in Table 3.1. The expected photon number of signal state $\mu = 0.48$ is calculated by Eq. (B.4).

need to put more pulses for decoy states and choose a larger ν to estimate Y_1 and e_1 accurately.

Now, we can put all these elements together to investigate the key generation rate R of Eq. (2.6). Figure 5.3 shows the key rate of the two practical decoy state protocols with statistical fluctuations in comparison to the infinite decoy state protocol (the asymptotic case). For each distance point, we optimize ν , N_s , N_{vac} and N_w numerically by considering Eqs. (5.12) and (5.13).

One can see that even taking into account the statistical fluctuations, both of the Vacuum+Weak and the one decoy state protocols can achieve close performance to the infinite decoy state protocol. Therefore, the following is noted:

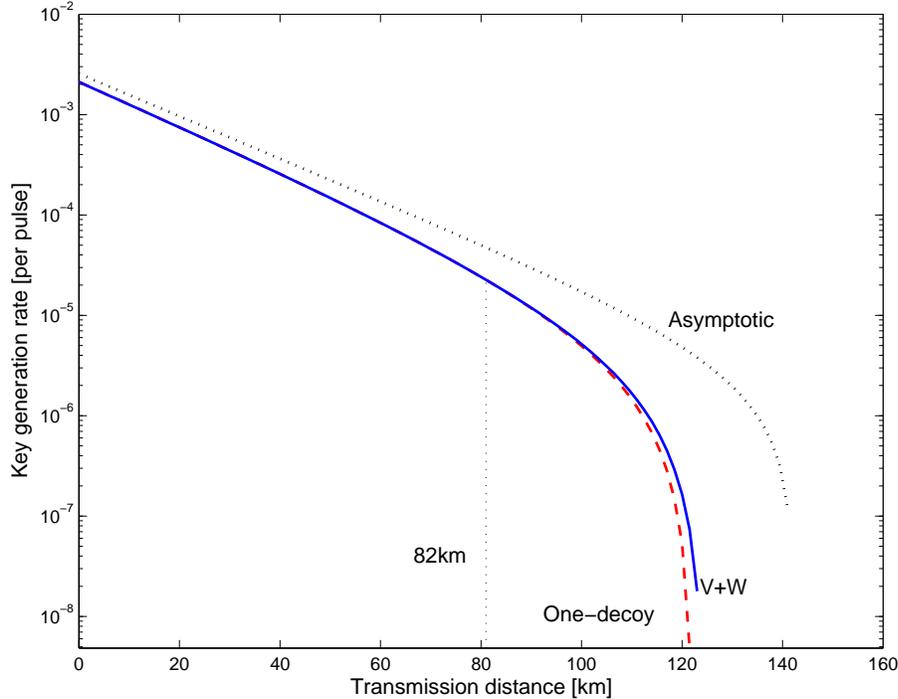


Figure 5.3: Plot of key generation rate in terms of channel transmission distance. The dotted line shows the key rate of the infinite decoy state method (the asymptotic case of the Vacuum+Weak decoy state protocol). The solid and dashed lines show the key rate of the Vacuum+Weak and one decoy state protocol with statistical fluctuations respectively. The data size is $N = 6 \times 10^9$. The simulation parameters are listed in Table 3.1. The expected photon number of signal state $\mu = 0.48$ is calculated by Eq. (B.4).

1. In a large regime of the distance (for instance, the distance between 0 km and 100 km), the two practical decoy state methods with statistical fluctuations achieve a close performance of the asymptotic limit of the infinite decoy state method. This is the case when the channel is not that lossy, the statistical fluctuations are easily controllable. This fact highlights the feasibility of the two practical decoy state protocols.
2. As shown in Figure 5.2, the vacuum decoy state becomes useful at 82 km.
3. The maximal secure distances of the three curves are 142 km, 125 km and 122 km. Note that with a larger data size, for instance, $N = 8.4 \times 10^{10}$, the maximal secure distance of the Vacuum+Weak decoy state method can achieve 132 km.

We have also simulated other experiment setups and all the results are consistent

with the simulation result of the GYS experiment setup shown above. For more details, one can refer to Refs. [77, 73].

5.4 Experimental demonstrations

The experimental demonstrations for the decoy state methods were first implemented by our group [131, 132] and followed by many other groups [99, 115, 88, 129, 128].

5.4.1 How to generate decoy states

The only difference of the decoy state QKD setup and the regular setup is that in the decoy state method, Alice needs to prepare decoy states, which have different intensities from the original signal states. Otherwise, the two setups are the same. The regular setup of the QKD without decoy states is discussed in Section 3.3.

There are several ways to generate decoy states. One way to do that is by using an attenuator to change the light intensity. There are two criteria for the attenuator.

- The attenuator can change attenuations fast enough⁷. Alice needs to prepare a decoy or signal state randomly in each pulse. Thus, the speed of changing attenuation should not be lower than the QKD repetition rate.
- The attenuator will not introduce differences in properties for change of signal and decoy states except for intensities. This is one precondition for the security of QKD with decoy states, as shown in Eq. (4.2). In a real experiment, one might need to apply some approximation. For example, an acousto-optic modulator (AOM) may shift the frequency of light. However, if we assume that both signal and decoy states will be shifted with the same amount of frequency, then we can still use AOM to prepare signal and decoy states.

For more discussions of using AOM to prepare decoy states, one can refer to Ref. [131].

Another way to prepare decoy states is by using different laser sources [88]. In this case, Alice can choose signal and decoy states by switching between different laser sources. Similarly, we require the switch to be fast enough and laser sources having the same properties except for intensities.

⁷Or it can switch on and off fast.

5.4.2 Experimental data post-processing

The processing of the decoy state QKD is as follows.

1. Alice prepares decoy and signal states and sends them to Bob. Bob measures all pulses in the two conjugate bases.
2. Bob announces the pulses that he obtains non-vacuum detections. Alice announces the pulses that are used for decoy states. Then they determine all the gains of signal and decoy states.
3. They perform basis reconciliation. Note that even these detection events that Alice and Bob use different bases, can be used to calculate the gains of signal and decoy states.
4. They compare all bit values decoy states to determine the QBER(s) of decoy states.
5. Alice and Bob perform error correction and error testing, after which they can determine the QBER of signal states.
6. They estimate the necessary amount of privacy amplification. Taking the Vacuum+Weak decoy state protocol for example, they estimate Y_1 and e_1 by values of Q_μ , E_μ , Q_ν , E_ν and Q_{vac} . In this step, they need to consider statistical fluctuations, for instance, by the procedures described in Section 5.2. Then they can plug all the values in Eq. (2.6) to calculate the amount of key that is needed to sacrifice for privacy amplification. Note that Eq. (2.6) is for the post-processing with one-way classical communication. In the next chapter, we will show that this result can be improved by introducing two-way classical communication.
7. They perform privacy amplification to get the final secure key.

Here, we describe the case where the QKD transmission is successful. In practice, Alice and Bob can keep tracking whether the final key is positive or not to determine whether they should continue the post-processing or not. For example, after step 2, they can estimate Y_1 . If the lower bound Y_1 is zero (or even negative), then they abort the post-processing and start QKD again.

5.5 Conclusion

The main conclusion of Chapters 4 and 5 is that the decoy state QKD takes a big step toward practical quantum cryptography. Recall that the motivation of this thesis is to encourage QKD into real-life applications.

Our result shows that we can have the best of both worlds: enjoy both unconditional security and record-breaking experimental performance. The decoy state method can increase key generation rate and extend the distance of QKD dramatically, all within the framework of unconditional security. The general principle of the decoy state QKD developed here can have widespread applications in other set-ups (e.g. open-air QKD or QKD with other photon sources). Later, we will come back to this point.

For practical implementations, we are able to show that with only one or two decoy states, one can achieve most of the benefits of the decoy state method. All the decoy state QKD experiment demonstrations, including our first realization, show that the decoy state idea is easy to implement in real system setups.

Recently, Yuan, Sharpe and Shields implemented an experimental decoy state QKD demonstration that can achieve a 5.51 kbits/s secure key rate through a 25.3 km fiber [129]. Let us compare this result to a couple of typical values in real-life communications. The state of the art digital speech coding [94] typically needs a bit rate around 4-10 kbits/sec. A typical city wide area network must cover an area with a radius of 5-25 km. As for other communications, such as video conversation, the bit rate may not be high enough. We want to point out that the bit rate might not be an essential problem. One can store a long secure key first and then use it for secure communications⁸.

Therefore, we conclude that the practical quantum cryptography is close to real-life applications.

Note that other than the decoy state method, there are other approaches to enhance the performance of the coherent state QKD, such as our dual detector scheme [93], QKD with strong reference pulses [48, 110] and differential-phase-shift QKD [42].

⁸One needs to consider the key management issue in this case.

Chapter 6

Decoy state QKD with 2-LOCC

As shown in the previous two chapters, the decoy state technique is an effective method for improving QKD performance. The data post-processing scheme of the decoy state QKD scheme that we proposed uses one-way classical communication. In this chapter, we develop two data post-processing schemes for the decoy state method using two-way classical communication. Our numerical simulation results show that the first scheme is able to extend the maximal secure distance from 142 km (by using only one-way classical communication with decoy states) to 181 km. The second scheme is able to achieve a 10% greater key generation rate in the whole regime of the distance. We conclude that the decoy state QKD protocol with two-way classical post-processing is of practical interest.

Here, we only consider a case without statistical fluctuations. For a statistical fluctuation analysis for the decoy state QKD with local operations and two-way classical communication (2-LOCC), one can refer to Ref. [74].

This work is published in Ref. [74]. In this project, I applied the Gottesman-Lo's 2-LOCC EDP and recurrence scheme to the decoy state QKD protocol and simulated a PDC experiment to show the improvement by using two-way classical communication in the decoy state QKD protocol.

6.1 2-LOCC EDP

First, let us review two EDPs based on 2-LOCC (Gottesman-Lo EDP and recurrence EDP) assuming that ideal single-photon (or perfect EPR) sources are used. Later, we will apply these two schemes to the decoy state QKD protocol.

6.1.1 Gottesman-Lo EDP

Gottesman and Lo [34] introduced an EDP based on 2-LOCC for use with QKD and showed that it can tolerate a higher bit error rate than 1-LOCC based EDPs. B and P steps are two primitives in the Gottesman-Lo EDP, and the EDP consists of executing a sequence of B and/or P steps, followed by a 1-LOCC EDP. The main objective for extra B and P steps is reducing the bit and/or phase error rates of qubits so that the following 1-LOCC EDP can work to extract secure keys. This is the reason why the Gottesman-Lo EDP is able to tolerate a higher initial bit error rate than 1-LOCC EDPs. The definitions of B and P steps are as follows:

Definition of B step [34]: (Figure 6.1) After randomly permuting all the EPR pairs, Alice and Bob perform a bilateral XOR (BXOR) between pairs of the shared EPR pairs and measure the target qubits in Z basis. This effectively measures the operator $Z \otimes Z$ by Alice and Bob locally, and detects the presence of a single bit flip error. If Alice and Bob's measurement outcomes disagree, they discard the remaining EPR pair. Otherwise, they keep the control qubit.

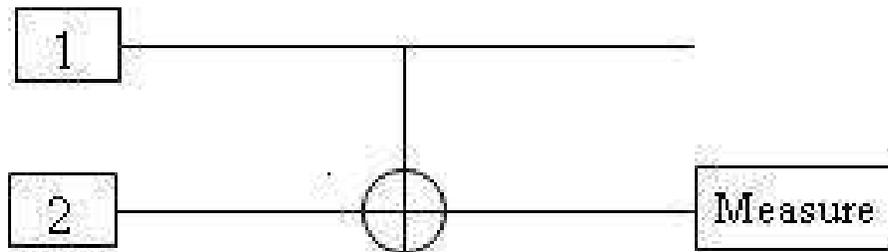


Figure 6.1: Alice and Bob each choose two qubits of two corresponding EPR pairs and input the quantum circuit as shown above. They discard both control and target qubits if they disagree on the outcomes of measurement on the target qubits. On the other hand, they keep the control qubits as surviving qubits if their measurement outcomes agree.

Since the B step only involves the measurement of $Z \otimes Z$, it can be used in the prepare-and-measure protocol, BB84. Classically, the B step simply involves random pairing of the key bits, for instance, x_1, x_2 on Alice's side and y_1, y_2 on Bob's side and the computation of the parity of each pair of bits, $x_1 \oplus x_2$ and $y_1 \oplus y_2$. Both Alice and Bob announce the parities. If their parities are the same, they keep x_1 and y_1 ; otherwise, they discard x_1, x_2, y_1 and y_2 . We can see that the B step is very simple to implement in data post-processing.

Suppose Alice and Bob input a control qubit $(q_{00}^C, q_{10}^C, q_{11}^C, q_{01}^C)$ ¹ and a target qubit $(q_{00}^T, q_{10}^T, q_{11}^T, q_{01}^T)$ with bit error rates δ_b^C and δ_p^C and phase error rates δ_b^T and δ_p^T , respectively. After one B step, the survival probability p_S is given by:

$$\begin{aligned} p_S &= (q_{00}^C + q_{01}^C)(q_{00}^T + q_{01}^T) + (q_{10}^C + q_{11}^C)(q_{10}^T + q_{11}^T) \\ &= (1 - \delta_b^C)(1 - \delta_b^T) + \delta_b^C \delta_b^T, \end{aligned} \quad (6.1)$$

and the density matrix $(q'_{00}, q'_{10}, q'_{11}, q'_{01})$ of output control qubit is given by:

$$\begin{aligned} q'_{00} &= \frac{q_{00}^C q_{00}^T + q_{01}^C q_{01}^T}{p_S} \\ q'_{10} &= \frac{q_{10}^C q_{10}^T + q_{11}^C q_{11}^T}{p_S} \\ q'_{11} &= \frac{q_{10}^C q_{11}^T + q_{11}^C q_{10}^T}{p_S} \\ q'_{01} &= \frac{q_{00}^C q_{01}^T + q_{01}^C q_{00}^T}{p_S}. \end{aligned} \quad (6.2)$$

Eqs. (6.2) can be derived from Table II of [13]. The corresponding bit error rate δ_b and phase error rate δ_p can be obtained from Eq. (6.2) by

$$\begin{aligned} \delta'_b &= q'_{10} + q'_{11} = \frac{\delta_b^C \delta_b^T}{p_S} \\ \delta'_p &= q'_{11} + q'_{01}. \end{aligned} \quad (6.3)$$

Definition of P step [34]: (Figure 6.2) Alice and Bob randomly permute all the EPR pairs. Afterwards, they group the EPR pairs into sets of three, and measure $X_1 X_2$ and $X_1 X_3$ on each set (for both Alice and Bob). This can be done (for instance) by performing a Hadamard transform, two bilateral XORs, measurement of the last two EPR pairs, and a final Hadamard transform. If Alice and Bob disagree on one measurement, Bob will conclude the phase error is probably on one of the EPR pairs which was measured, and do nothing; if both measurements disagree for Alice and Bob, Bob assumes the phase error is on the surviving EPR pair and corrects it by performing a Z operation.

Without a quantum computer, Alice and Bob are not able to perform P steps by the quantum circuit shown in the left hand side of Figure 6.2. In order to implement P steps classically, they can choose a post-processing scheme that does not rely on the measurement result from P steps. That is, they can implement the right hand side

¹The superscript C and T stand for the control and target qubits, respectively. The subscript 00, 10, 11 and 01 stand for the case with no error, with a bit error, with both a bit and a phase error, and with a phase error, respectively.

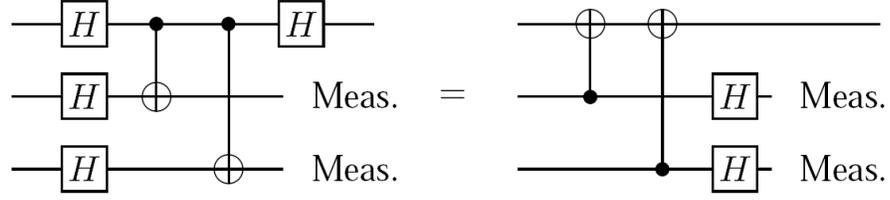


Figure 6.2: The two circuits are quantum mechanically equivalent. Alice and Bob each choose three qubits of three corresponding EPR pairs and input the quantum circuit as shown above. This figure is originally from Ref. [34].

quantum circuit of Figure 6.2 by simply omitting the measurement step. Thus, when a P step is implemented classically in BB84², the phase errors are not detected or corrected (i.e. the phase flip operation Z is not applied). Note that the measurement step in Figure 6.2 is not important because the phase errors do not need to be corrected in QKD [106]. The phase error correction is used in the security proof. One only needs to show that Alice and Bob could have done the phase error correction but not really need to do it. From this point of view, P steps are conceptually similar to the privacy amplification.

The P step then will be reduced to where Alice and Bob randomly form trios of the remaining qubits and compute the parity of each trio, for instance, $x_1 \oplus x_2 \oplus x_3$ by Alice and $y_1 \oplus y_2 \oplus y_3$ by Bob. They now regard those parities as their new bits for further processing.

Since before P steps, Alice and Bob will perform random permutation, for simplicity, we assume the input three qubits have the same density matrix: $(q_{00}, q_{10}, q_{11}, q_{01})$. After one P step, the density matrix $(q'_{00}, q'_{10}, q'_{11}, q'_{01})$ of the output qubit is given by:

$$\begin{aligned}
 q'_{00} &= q_{00}^3 + 3q_{00}^2q_{01} + 3q_{10}^2(q_{00} + q_{01}) + 6q_{00}q_{10}q_{11} \\
 q'_{10} &= q_{10}^3 + 3q_{10}^2q_{11} + 3q_{00}^2(q_{10} + q_{11}) + 6q_{00}q_{10}q_{01} \\
 q'_{11} &= q_{11}^3 + 3q_{10}q_{11}^2 + 3q_{01}^2(q_{10} + q_{11}) + 6q_{00}q_{11}q_{01} \\
 q'_{01} &= q_{01}^3 + 3q_{00}q_{01}^2 + 3q_{11}^2(q_{00} + q_{01}) + 6q_{10}q_{11}q_{01},
 \end{aligned} \tag{6.4}$$

which is given in Appendix C of [34]. Therefore, the bit error rate and phase error rate will be given by:

$$\begin{aligned}
 \delta'_b &= q'_{10} + q'_{11} = 3\delta_b(1 - \delta_b)^2 + \delta_b^3 \\
 \delta'_p &= q'_{11} + q'_{01} = 3\delta_p^2(1 - \delta_p) + \delta_p^3.
 \end{aligned} \tag{6.5}$$

²Strictly speaking, this procedure is different from the original P step we described. For simplicity, we use the same name for this simplified version of the P step.

Here, we emphasize that the B and P steps are important elements of the Gottesman-Lo EDP. After the B and P steps, the Gottesman-Lo EDP will be the same as the regular 1-LOCC EDP.

6.1.2 Recurrence EDP scheme

Here, we review another two-way EDP, the recurrence scheme [118]. Similar to the B step in the Gottesman-Lo EDP, the recurrence scheme reduces the bit error rate of the EPR pairs before passing them to the 1-LOCC based EDP for the distillation of maximally-entangled EPR pairs. However, there are two main differences between these two EDP schemes. The first is how the bit error syndrome of a target EPR pair in a bilateral XOR operation is learned. In the Gottesman-Lo EDP, Alice and Bob simply measure the target EPR pair in the Z basis and compare their results to learn about the bit error syndrome (see Figure 6.1). In the recurrence scheme, Alice and Bob group the bit error syndromes of all target EPR pairs together and learn about all the syndromes using random hashing. The second difference is that the recurrence scheme requires some extra maximally-entangled EPR pairs to begin with in order to learn about the bit error syndromes, whereas no such extra pairs are required in the Gottesman-Lo EDP. Note that the recurrence methods were studied in various papers, such as [22, 79, 3, 21].

The procedure of the recurrence protocol is described as follows:

1. Alice and Bob perform two BXOR operations on two noisy EPR pairs and one perfect maximally-entangled EPR pair. Specifically, the first BXOR is performed on one noisy EPR pair as the source and the perfect EPR pair as the target, and the second BXOR is performed using the other noisy EPR pair as the source and the same target.
2. They perform random hashing on the target EPR pairs to learn about the parities of the noisy EPR pairs. Note that only a portion of the target EPR pairs have to be measured in order to learn about all the parities. This is different from the B step approach.
3. They perform error correction and privacy amplification separately for even-parity and odd-parity EPR pairs.

In the prepare-and-measure scenario, the first two steps are as follows: Alice and Bob randomly pair up the key bits, and for each pair they compute the parity. They

each compress their own sequence of parities by using random hashing, encrypt the resulting hash values using the one-time pad with some pre-shared secret bits, and send the encrypted results to each other. Note that they use the same sequence of secret bits to encrypt their own sequence of hash values. They learn about the parities of the original noisy EPR pairs by adding the other party's encrypted sequence to their own encrypted sequence of hash values. Once they know the parities, they perform error correction and privacy amplification on the even-parity and odd-parity key bits separately. Note that the secret bits used up in the process should be returned to the secret bits pool by using the newly generated secret bits.

The key generation rate using the recurrence EDP with a single-photon source is given by:

$$R = q \left[-\frac{1}{2}H_2(p_S) - \frac{1}{2}p_S H_2\left(\frac{\delta_b^C \delta_b^T}{p_S}\right) + K \right] \quad (6.6)$$

where q is defined similarly as in Eq.(2.4), p_S is the probability of obtaining even parity given in Eq. (A.2), and $\delta_b^C(\delta_b^T)$ is the bit error rate of the control (target) EPR pair. Here, the first term in the bracket corresponds to the extra perfect EPR pairs borrowed, the second term corresponds to error correction, and the third term K corresponds to the privacy amplification given in Eq. (A.12). In Appendix A.2, we review the recurrence EDP in detail and develop a key rate formula.

6.1.3 Bounds of error rates

Here, we will consider the bounds of error rates (bit error rate δ_b and phase error rate δ_p), assuming a laser source that emits a basis-dependent single-photon source. The upper bounds can be derived by considering some simple attacks (such as intercept-resend attack) and determining the QBER caused by these attacks. The lower bounds can be determined by the unconditional security proof assuming that Eve is performing arbitrary attacks allowed by the law of quantum mechanics, and Alice and Bob employ a certain post-processing scheme (such as Gottesman-Lo EDP described in Subsection 6.1.1). One lower bound, obtained by considering Gottesman-Lo EDP, is 18.9% [34]. For BB84, an upper bound, obtained by considering an intercept-resend attack, is 25%.

Here, we consider the lower bound in a general setting where the error rates are characterized by (δ_b, δ_p) . In general, the bit error rate δ_b can be measured by error testing, but the phase error rate δ_p cannot be directly observed from the QKD experiment. In order to guarantee the security, Alice and Bob have to bound δ_p with the knowledge of

δ_b . For BB84 with an ideal single-photon source, due to the symmetry between the X and Z bases, one can show that the bit error rate and the phase error rate are the same, i.e.

$$\delta_b = \delta_p. \quad (6.7)$$

In general, for other protocols or with non-ideal sources (including coherent state sources), the bit and phase error rates might be different. For example, even for BB84, when a basis-dependent source is used, Eq. (6.7) may not hold. In this case, according to Eq. (9) of [50], due to the concavity of the right hand side of the equation, it is not difficult to show (see Appendix A.3) that δ_b and δ_p have the relation of

$$\sqrt{F} \leq \sqrt{(1 - \delta_b)(1 - \delta_p)} + \sqrt{\delta_b \delta_p}, \quad (6.8)$$

where F is the fidelity between the two states with two bases (X and Z) sent by Alice, and it is the single parameter that characterizes the basis dependency of the source. Thus, Alice and Bob can upper bound δ_p (denoted as δ_p^u) with this inequality given δ_b . Clearly, when $\delta_p = \delta_b$, the inequality will be always satisfied, i.e., $\delta_p = \delta_b$ is a particular solution of Eq. (6.8). Therefore, in general, we have $\delta_p^u \geq \delta_p$. In the following, we use δ_p to denote the upper bound δ_p^u for simplicity.

Given a QKD protocol and laser source, Alice and Bob can estimate the phase error rate δ_p from the bit error rate δ_b in accordance to the protocol and source. We investigate the highest error rates that a data post-processing scheme can tolerate. Figure 6.3 shows the tolerable error rates of the Gottesman-Lo EDP compared to the 1-LOCC EDP scheme, illustrating the superior performance of the Gottesman-Lo EDP over the 1-LOCC EDP. The boundaries of the error rates are found by searching through the regime of:

$$\begin{aligned} \delta_b &\leq \delta_p \\ \delta_b + \delta_p &< 1/2 \end{aligned} \quad (6.9)$$

such that positive key rates are obtained. The reason that we are interested in the region specified by the second inequality in Eq. (6.9) is as follows: We can assume that the error rates δ_b and δ_p are less than $1/2$, otherwise Alice and Bob can flip the qubits. Furthermore, if $\delta_b + \delta_p \geq 1/2$, the (worst scenario case) state shared by Alice and Bob is a separable state [13] and the Gottesman-Lo EDP cannot distill any pure EPR pairs [20].

The input to the Gottesman-Lo EDP is $(q_{00}, q_{10}, q_{11}, q_{01})$ with $q_{00} + q_{10} + q_{11} + q_{01} = 1$, see Subsection 6.1.1. However, Alice and Bob only know $\delta_b = q_{10} + q_{11}$ and $\delta_p = q_{11} + q_{01}$

from their error testing. There is one free parameter q_{11} . In Appendix C of [34], the authors proved that $q_{11} = 0$ is the worst case when $\delta_b = \delta_p$. Following that proof, we can show that $q_{11} = 0$ is the worst case when the condition of Eq. (6.9) is satisfied. That is, given (δ_b, δ_p) , if we check the input $(1 - \delta_b - \delta_p, \delta_b, 0, \delta_p)$ for the Gottesman-Lo EDP and obtain a positive key rate, then we can safely claim that the Gottesman-Lo EDP can tolerate the error rates of (δ_b, δ_p) .

To determine the tolerable bit error rate of a particular protocol, one should first obtain the relationship between the bit error rate and phase error rate, and plot it on Figure 6.3. The intersections between this curve and the boundary curves (the 1-LOCC curve and Gottesman-Lo curve) indicate the tolerable QBER for the corresponding EDPs. For example, for the BB84 protocol with a perfect single-photon source, we have $\delta_b = \delta_p$, which is the dashed line plotted in Figure 6.3. We can immediately read off from the figure that an initial bit error rate of 18.9% is tolerable using the Gottesman-Lo EDP [34], while an error rate of 11.0% is tolerable using the 1-LOCC EDP. In general, the Gottesman-Lo EDP gives rise to higher tolerable error rates than the 1-LOCC EDP.

We numerically optimize the B/P sequence up to 12 steps. The result is shown in Figure 6.3.

For protocols having constraints on q_{11} , such as the six-state protocol [17] and the SARG04 protocol with a single-photon source [101, 109, 28], the tolerable QBER can go beyond the boundary curves shown in Figure 6.3.

6.2 Decoy + GLLP + Gottesman-Lo EDP

In this section, we propose a 2-LOCC based data post-processing protocol in a form of a sequence of B steps, followed by 1-LOCC error correction and privacy amplification. This new scheme is a generalization of the Gottesman-Lo scheme to a case of imperfect devices. The reasons for skipping P steps here are as follows. First, from the simulation in Section 6.1.3, we found that P steps are not as useful as B steps. Secondly, only considering B steps can simplify the procedure of the data post-processing scheme.

The residual ratio of a post-processing scheme, r , is defined by:

$$R = qQ_\mu r \tag{6.10}$$

which characterizes the cost of the post-processing scheme.

The procedure of the data post-processing scheme, Decoy + GLLP + B steps, is as follows:

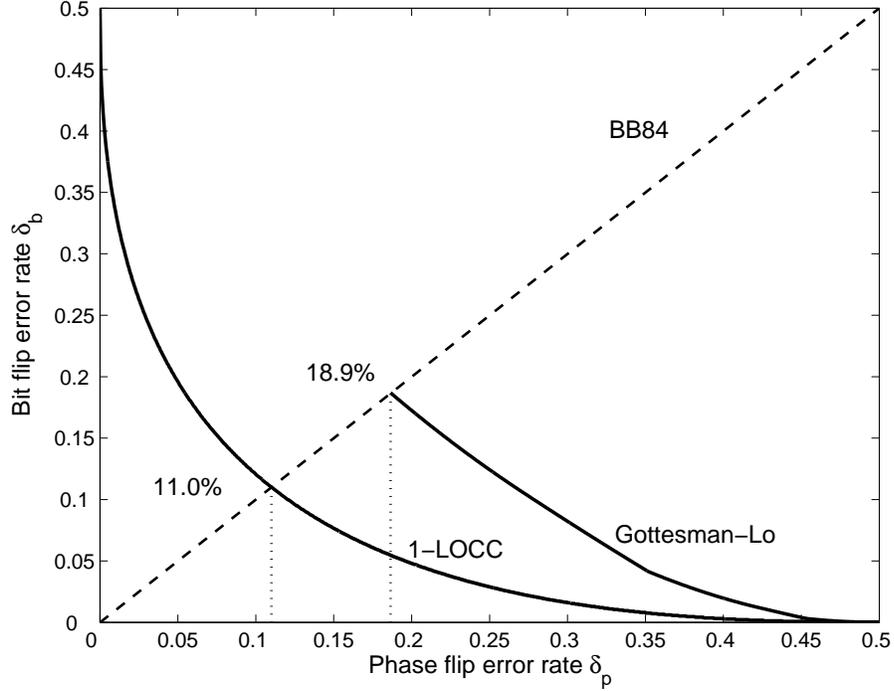


Figure 6.3: Plot of the secure regions in terms of error rates for the 1-LOCC EDP and Gottesman-Lo EDP. The regions under the solid lines are proven to be secure due to 1-LOCC EDP, and Gottesman-Lo EDP schemes (for the region under the solid line and dashed line), respectively. For 1-LOCC EDP, we use Eq. (2.4). For Gottesman-Lo EDP, we use Eqs. (6.2) and (6.4). In the Gottesman-Lo EDP, we numerically optimize the B/P sequence up to 12 steps.

1. Alice and Bob perform a sequence of B steps to the sifted key. During this procedure, they will discard a large ratio of the key. The survival key bit ratio is defined to be \tilde{r}_B .
2. They calculate the variables (such as QBER, untagged qubits ratio) after the B steps.
3. They perform an overall error correction, corresponding to the first term in Eq. (6.11).
4. They perform privacy amplification, corresponding to the second term in Eq. (6.11).

In the following, we will discuss how the residue of this post-processing scheme is calculated.

In the model described in Section 3.2, there are three kinds of qubits: vacuum, single photon and multi photon qubits. We emphasize again here that the final secure key can only be distilled from untagged qubits (single photon qubits) for the BB84 protocol.

Since either of the two inputs of a B step has three possibilities, the outcomes of a B step then have nine possibilities. Only the case where both inputs are untagged qubits will there be a positive contribution to the final secure key. That is, at the end of some B steps, bit error correction and privacy amplification can be only applied to the remaining qubits that come from the case where both inputs are untagged qubits. In other words, an output qubit after a subsequence of B steps is “untagged” if a) it passes all B steps and b) it is generated from a case where all initial input qubits are single photon qubits. Therefore, the residue ratio of data post processing can be expressed, according to Eq. (2.6), as:

$$r = \tilde{r}_B \{-f(\tilde{\delta})H_2(\tilde{\delta}) + \tilde{\Omega}[1 - H_2(\tilde{\delta}_p^{untagged})]\} \quad (6.11)$$

where $\tilde{\delta}$ is the remaining QBER, \tilde{r}_B is overall survival residue, $\tilde{\Omega}$ is the fraction of untagged states in the final survival states³ and $\tilde{\delta}_p^{untagged}$ is the phase error rate of the untagged states, after a sequence of B steps. In the following, we will show how these variables change with the performing of B steps.

An arbitrary B step: Let us consider how the various quantities (fraction of untagged states Ω , QBER of overall surviving states δ , bit error rate $\delta_{untagged}$ and phase error rates δ_p of the untagged states) are transformed under one step in a B step sequence.

Prior to a B step, the fraction of untagged states is Ω , the overall QBER is δ , the bit error rate of the untagged states is $\delta_{untagged}$, and the phase error rate of the untagged states is δ_p . According to Eq. (6.1), the overall survival probability p_S and the survival probability of the untagged states $p_S^{untagged}$ after one B step are given by:

$$\begin{aligned} p_S &= [\delta^2 + (1 - \delta)^2] \\ p_S^{untagged} &= [\delta_{untagged}^2 + (1 - \delta_{untagged})^2]. \end{aligned} \quad (6.12)$$

Then the residue after one B step is given by:

$$r_B = \frac{1}{2} p_S \quad (6.13)$$

where the factor 1/2 stems from the the fact that Alice and Bob only keep one qubit from a survival pair. Subsequently, after a B step, the fraction of untagged states Ω' is

³Without B steps, $\Omega \equiv Q_1/Q_\mu$.

given by:

$$\Omega' = \frac{\Omega^2 \cdot p_S^{untagged}}{p_S}. \quad (6.14)$$

Overall QBER: the change of the overall QBER δ' is given by:

$$\delta' = \frac{\delta^2}{\delta^2 + (1 - \delta)^2}. \quad (6.15)$$

Untagged states: before the first B step, the initial density matrix of the untagged state is $(1 - 2e_1 + q_{11}, e_1 - q_{11}, q_{11}, e_1 - q_{11})$, where e_1 is the error rate of single photon states. From Appendix C of [34], we know that $q_{11} = 0$ is the worst case for B steps. Thus we can conservatively choose $(1 - 2e_1, e_1, 0, e_1)$ as the initial input density matrix. If only B steps are performed, $q_{11} = 0$ will always be satisfied, according to Eq. (6.2). Therefore, the input untagged qubits for any round of B steps has the form of

$$(q_{00}, q_{10}, q_{11}, q_{01}) = (1 - \delta_{untagged} - \delta_p, \delta_{untagged}, 0, \delta_p). \quad (6.16)$$

The bit error rate of untagged state $\delta'_{untagged}$ only depends on the input $\delta_{untagged}$,

$$\delta'_{untagged} = \frac{\delta_{untagged}^2}{\delta_{untagged}^2 + (1 - \delta_{untagged})^2}. \quad (6.17)$$

According to Eqs. (6.2), (6.3) and (6.16), the phase error rate of untagged states is

$$\begin{aligned} \delta'_p &= q'_{11} + q'_{01} \\ &= \frac{2q_{10}q_{11} + 2q_{00}q_{01}}{(q_{10} + q_{11})^2 + (q_{00} + q_{01})^2} \\ &= \frac{2\delta_p \cdot (1 - \delta_{untagged} - \delta_p)}{\delta_{untagged}^2 + (1 - \delta_{untagged})^2}. \end{aligned} \quad (6.18)$$

Eqs. (6.12)-(6.18) are valid for a general B step. Alice and Bob can perform a sequence of B steps as described above and then perform the error correction and privacy amplification. Once all of these quantities are obtained, the key generation rate can be calculated from Eq. (6.11).

To illustrate the improvement made by introducing B steps, we simulate the GYS experiment [32], whose parameters are listed in Table 3.1. Similar to the simulations in previous chapters, we use $f(e) = 1.22$ for the error correction efficiency [16].

From Figure 6.4, we can see that there is a non-trivial extension of the maximal secure distance after introducing B steps. Note that the key rate of the decoy state protocol with 1 B step is higher than the one with 1-LOCC from a distance of around 132 km.

The maximal secure distance using 4 B steps is 181 km, which is not far from the upper bound of 208 km, given in Section 4.2.1. Even with only 1 B step, the maximal secure distance can be extended from 142 km to 162 km. Thus, B steps are useful in QKD data post-processing.

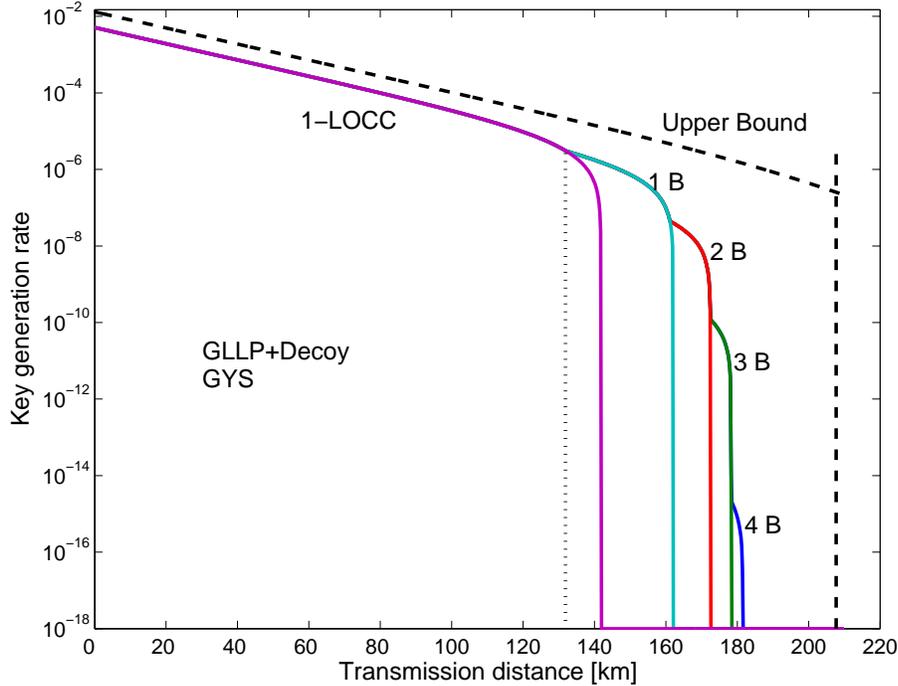


Figure 6.4: Plot of the key rate as a function of the transmission distance with the data post-processing scheme of GLLP+Decoy+B steps. The simulation parameters are from the GYS experiment [32] listed in Table 3.1. The GLLP+Decoy+B steps scheme suppresses the one with 1-LOCC at a distance of 132 km. The maximal secure distance using 4 B steps is 181 km, which is not far from the upper bound of 208 km. Note that B steps are useful only at rather long distances (over $132km$).

6.3 Decoy + GLLP + Recurrence EDP

In this section, we will present another data post-processing scheme based on the recurrence scheme [118], which is reviewed in Section 6.1.2. Our scheme is a generalization of the recurrence scheme to the case of imperfect sources.

Here, we will use the extended GLLP formula, Eq. (2.7), in Section 2.5.3. Again, we

use the definition of the residual, Eq. (6.10):

$$r = -\frac{1}{2}f(p_S)H_2(p_S) - \frac{1}{2}p_S f\left(\frac{\delta^2}{p_S}\right)H_2\left(\frac{\delta^2}{p_S}\right) + \sum_i \Omega_i K_i, \quad (6.19)$$

where p_S is the even parity possibility given in Eq. (A.2) with $\delta_b^C = \delta_b^T = \delta$, δ is the overall QBER before the recurrence, $f(\cdot)$ is error correction efficiency, Ω_i and K_i are the probability and the residue of the qubit groups with label i after privacy amplification, respectively.

In the post-processing, Alice and Bob first check the parity, corresponding to the first term of Eq. (6.19). Secondly, they apply an overall error correction to the qubits with even parity, corresponding to the second term of Eq. (6.19). Thirdly, they measure one of the qubits in the pairs with odd parity to obtain the error syndrome of another qubit. Afterwards, they can group the surviving qubits into several groups with labels i . Finally, they perform privacy amplification to each group with label i , corresponding to the last term of Eq. (6.19).

In the decoy state protocol, there are three kinds of input qubits: vacuum qubits (V), single-photon qubits (S) and multi-photon qubits (M). The input parameters for recurrence are listed in Table 6.1.

Qubit	Fraction	δ_b	δ_p	q_{11}
V	Ω_V	1/2	1/2	q_{11}^V
S	Ω	e_1	e_1	a
M	Ω_M	e_M	1/2	q_{11}^M

Table 6.1: List of the parameters of three kinds of input qubits for the recurrence scheme. Following Eqs. (3.7) and (3.8), the fractions of each group are given by $\Omega_V = Q_0/Q_\mu$, $\Omega = Q_1/Q_\mu$ and $\Omega_M = 1 - \Omega_V - \Omega$. $\Omega_V/2 + e_1\Omega + e_M\Omega_M = \delta$ is the overall QBER.

Thus, the outcome of one round of recurrence will have nine cases. Clearly, if neither input is a single photon qubits, the outcome will have no contribution to the final key. Alice and Bob need only apply Eq. (A.12) to calculate the residues, K_i , for the five cases: $V \oplus S$, $S \oplus V$, $S \oplus S$, $S \oplus M$, $M \oplus S$. The probabilities of occurrence, Ω_i , for the five cases are $\Omega_V\Omega$, $\Omega\Omega_V$, Ω^2 , $\Omega\Omega_M$, $\Omega_M\Omega$, respectively. Once we know K_i and Ω_i , we can then determine the overall residue, r , using Eq. (6.19) (details are shown in Appendix A.4):

$$r \geq -B + C - F_a \quad (6.20)$$

where

$$\begin{aligned}
B &= \frac{1}{2}f(p_S)H_2(p_S) + \frac{1}{2}p_S f\left(\frac{\delta^2}{p_S}\right)H_2\left(\frac{\delta^2}{p_S}\right) \\
C &= \frac{3}{4}\Omega_V\Omega + \Omega^2(1 - e_1 + e_1^2) + \frac{1}{2}\Omega\Omega_M(2 - e_1 - e_M + 2e_1e_M) \\
D_1 &= \frac{3}{4}\Omega_V\Omega + \frac{1}{2}\Omega^2(2 - e_1) + \frac{1}{2}\Omega\Omega_M(2 - e_M) \\
D_2 &= \frac{3}{4}\Omega_V\Omega + \frac{1}{2}\Omega^2(1 + e_1) + \frac{1}{2}\Omega\Omega_M(e_M + 1) \\
F_a &= D_1(1 - e_1)H_2\left(\frac{e_1 - a}{1 - e_1}\right) + D_2e_1H_2\left(\frac{a}{e_1}\right)
\end{aligned} \tag{6.21}$$

with equality when $q_{11}^V = 1/4$ and $q_{11}^M = e_M/2$. In order to get a lower bound of key generation rate R , we maximize F_a over a by using a bisection method as discussed in Appendix A.4.

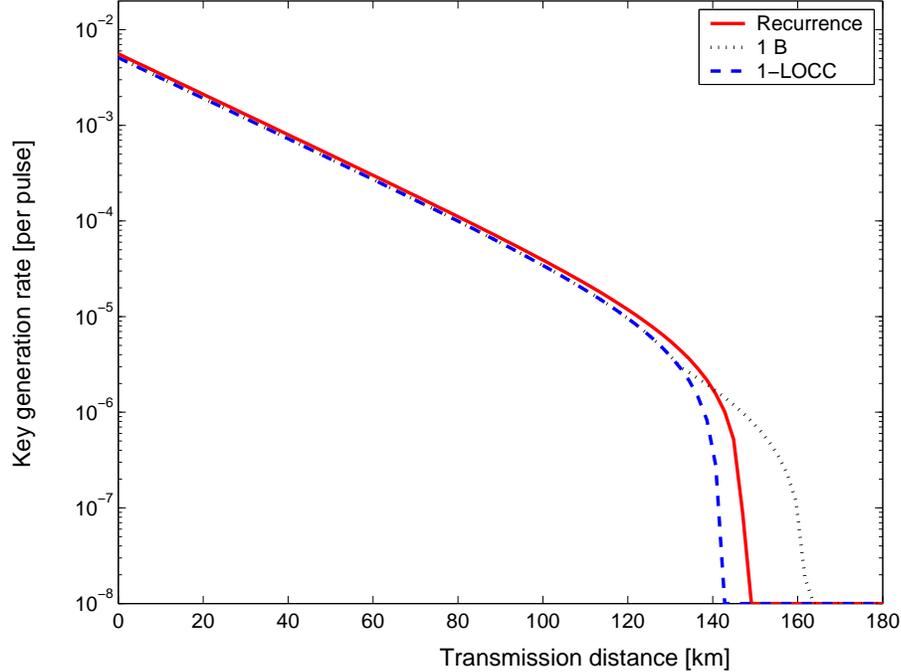


Figure 6.5: Plot of the key generation rate as a function of the transmission distance, GLLP+Decoy+Recurrence vs. GLLP+Decoy+1-LOCC. Recurrence improves the QKD performance over 1-LOCC in the whole regime of the distance. In particular, the recurrence method increases the key rate by more than 10% in our simulation. The maximal secure distance for each case is 142.8 km (1-LOCC), 149.1 km (Recurrence), 163.8 km (1 B), respectively. Here, we consider the asymptotic decoy state QKD with an infinitely long experiment. The parameters used are from the GYS experiment [32] listed in Table 3.1.

Figure 6.5 shows the key generation rate as a function of the transmission distance for GLLP+Decoy+1-LOCC, GLLP+Decoy+1 B step, and GLLP+Decoy+Recurrence. Recurrence has more than a 10% improvement of the key rate over 1-LOCC in the whole regime of the distance, and it also increases the maximal secure distance by 6 km.

6.4 Conclusion

We have developed two data post-processing schemes for the decoy state QKD using 2-LOCC, one based on B steps and the other based on the recurrence method. As discussed in Section 1.2.2, the maximal secure distance of QKD is crucial in practical applications, thus our Decoy+B steps post-processing protocol, which we have shown to be able to increase the maximal secure distance of QKD from 141 km to 182 km (using parameters from the GYS experiment [32]), proves to be useful in real-life applications. Moreover, our work shows that recurrence protocols are useful for increasing the key generation rate in a practical QKD system in the whole regime of the distance.

In Ref. [74], we also show that similar conclusions hold even with statistical fluctuations in the experimental variables for the Decoy+B step scheme. For the Decoy+Recurrence scheme, although we do not have a rigorous argument, physical intuition suggests that similar conclusions hold in the case of considering statistical fluctuations as well. We conclude that using two-way classical communication is superior to using one-way for our decoy state QKD schemes.

In addition, we provided a region of bit error rates and phase error rates that are tolerable by using the Gottesman-Lo EDP scheme.

Chapter 7

Triggering PDC QKD

Parametric down-conversion (PDC) sources can be used for QKD. One can use a PDC source as a triggered (heralded) single photon source. Recently, there are various practical proposals of the decoy state QKD with triggering PDC sources. In this chapter, we generalize the passive decoy state idea, originally proposed by Maurer and Silberhorn. The generalized passive decoy state idea can be applied to cases where either threshold detectors or photon number resolving detectors are used. The decoy state protocol proposed by Adachi, Yamamoto, Koashi and Imoto (AYKI) can be treated as a special case of the generalized passive decoy state method. By simulating a recent PDC experiment, we compare various practical decoy state protocols with the infinite decoy protocol and also compare the cases using threshold detectors and photon-number resolving detectors. Our simulation result shows that with the AYKI protocol, one can achieve a key generation rate that is close to the theoretical limit of the infinite decoy protocol. Furthermore, our simulation result shows that a photon-number resolving detector does not appear to be useful for improving the QKD performance in this case. Although our analysis is focused on the QKD with PDC sources, we emphasize that it can also be applied to QKD setups with other triggered single photon sources.

This work is presented in Ref. [76]. In this work, I modeled the QKD setup with triggered PDC source following the work of Lütkenhaus [70] and compare various decoy state proposals of triggering PDC QKD.

7.1 Background

The coherent state QKD suffers from photon-number splitting (PNS) attacks [39, 15, 71]. As discussed in Section 4.1, a main objective of the decoy state method is to close this loophole of multi photon components in QKD sources. Decoy states can help better estimate the channel properties (e.g., transmittance and error provability). To do that, Alice uses extra states with different light intensities during key transmission. Then Alice and Bob can consider detection statistics from signal and decoy states separately, from which they can better estimate the channel transmittance and error probability. The situation where Alice actively prepares decoy states is called the *active decoy state* method, which is differentiated from the *passive decoy state* method where Alice chooses decoy and signal states by passive measurements. A detailed discussion about the passive decoy state can be found in Section 7.4.4. Note that in the coherent state QKD, one can only use the active decoy state method.

Aside from a coherent state source, a PDC source can be used in a QKD experiment as well. There are two ways to use a PDC source. The first is to use it as a triggered (heralded) single photon source. Alice detects one of the two modes from a PDC source as a trigger¹ and actively encodes her qubit information into another mode. We call this implementation *triggering PDC QKD*. The second way is to use it as an entangled photon source for entanglement-based QKD protocols. See Chapter 8 for more discussion. We call this implementation *entanglement PDC QKD*.

The triggering PDC QKD, similar to the coherent state QKD, suffers from PNS attacks. By applying the GLLP security proof, one can find that the optimal average photon number μ is in the same order of the overall transmittance η . Then the key generation rate will be in the order of η^2 . For a rigorous derivation, one can refer to Appendix B.2. Thus, the performance of the triggering PDC QKD is very limited.

Since the decoy state idea can substantially enhance the performance of the coherent state QKD, a natural question will be: “Can the decoy state idea be applied to the triggering PDC QKD?” The answer is *yes*. One can apply the infinite decoy state idea [65], as discussed in Section 4.1, to the triggering PDC QKD. Not surprisingly, with decoy states, the key generation rate can be $O(\eta)$, which is the same as the order achieved by a single-photon source. Therefore, we expect that the decoy state QKD will become a standard technique not only in the coherent state QKD, but also in QKD with triggering

¹See Section 7.2 for the definition of a trigger.

PDC sources. Recently, a few practical decoy proposals for triggering PDC requiring a finite number of decoy states have been proposed [82, 2, 122, 121]. Note that an experimental demonstration of the decoy state QKD with a triggering PDC source was implemented recently [120].

We are interested in comparing various protocols for the triggering PDC QKD. Among the practical decoy protocols for triggering PDC QKD, we find that the one proposed by Adachi, Yamamoto, Koashi and Imoto (AYKI) [2] is simple to implement. The AYKI protocol is conceptually similar to the one-decoy state scheme [77], as discussed in Section 5.1.2. In the AYKI protocol, Alice and Bob only need to consider the statistics of triggered and non-triggered detection events² separately, instead of preparing new signals for the decoy states. We emphasize that the AYKI protocol is easy to implement since there is no need for a hardware change.

Other decoy state proposals for the triggering PDC QKD require hardware modifications. For example, the one proposed by Maurer and Silberhorn [82] requires photon-number resolving detectors, and the one proposed by Wang, Wang and Guo [122] requires Alice to pump the laser source at various intensities.

The following is a generalization of the passive decoy state idea proposed by Maurer and Silberhorn [82]. The main idea is that Bob can group his detection events in accordance to the public announcement of Alice's detection events. For example, when Alice uses a threshold detector, Bob can group his detection results in accordance to whether Alice gets a detection or not. The generalized passive decoy state idea can be applied to both cases that use threshold detectors and photon-number resolving detectors. The AYKI protocol can be treated as a special case of the generalized passive decoy state protocol.

By simulating a recent PDC experiment [115], we compare one case with a perfect photon-number resolving detector and four cases with threshold detectors: no decoy, infinite decoy, weak decoy and AYKI. Our simulation result shows that in a large regime (for instance, the optical link loss between 0 dB and 25 dB), the performance of AYKI protocol is close to that of the infinite decoy protocol and thus, there is not much room left for improvement after the AYKI protocol has been implemented. Moreover, the QKD performance of the case with the infinite decoy protocol using threshold detectors is close to the case using a perfect photon-number resolving detector. Thus, a photon-number resolving detector does not appear to be useful for triggering PDC QKD.

²In a non-triggered detection event, Bob gets a detection, but Alice does not get a trigger.

We emphasize that an advantage of the passive decoy state method is that by passively choosing decoy and signal states, the possibility that Eve can distinguish decoy and signal states is reduced. On the other hand, in active (regular) decoy state experiments, it is more difficult to verify the assumption that Eve cannot distinguish decoy and signal states.

Note that the passive decoy state idea can be combined with the active decoy state idea. In Ref. [121], the authors provide a special case where passive and active decoy state ideas are combined. Again, we emphasize that for the coherent state QKD, one can only use active decoy state methods.

Although our analysis is focussed on a QKD with a triggered PDC source, we emphasize that it can also be applied to QKD setups with other triggered single photon sources.

In Section 7.2, we will review the experiment setup of the triggering PDC QKD. In Section 7.3, we provide a model for the triggering PDC QKD. In Section 7.4, we will study various post-processing schemes for the triggering PDC QKD. In Section 7.5, we will compare various schemes of the triggering PDC QKD: non-decoy+threshold detectors, infinite decoy+threshold detectors, AYKI and a case with a perfect photon-number resolving detector, by simulating a real PDC experiment.

7.2 Experiment setup

In triggering PDC QKD, a PDC source is used as a triggered single photon source³. The schematic diagram is shown in Figure 7.1.

As shown in Figure 7.1, a PDC source generates two modes of photons, which can be separated by a polarization beam splitter (PBS). One mode goes to Alice’s own detector (DA in Figure 7.1) as the triggering signal and the other mode is used as a triggered single photon state for the QKD. When Alice’s detector (DA) clicks, we call it a *trigger*. We divide the detection events on Bob’s side into two groups depending on whether Alice gets a trigger or not: triggering detection events and non-triggering detection events.

Note that Alice can use either a threshold detector or a photon-number resolving detector (DA in Figure 7.1). She only needs to know the number of photons in the trigger mode. Therefore, only one detector is sufficient on Alice’s side. Due to the high channel losses, without Eve’s interference, Bob is highly likely to receive a vacuum or

³Sometimes it is called heralded single photon source.

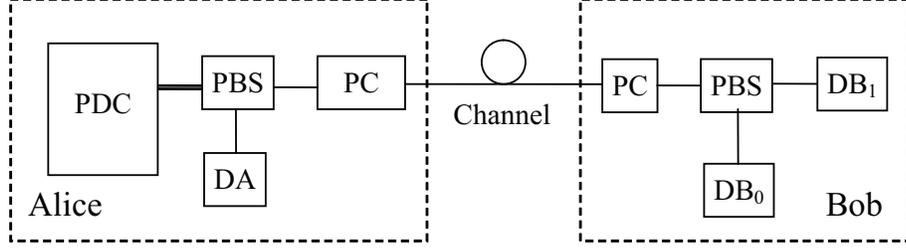


Figure 7.1: A schematic diagram for the triggering PDC QKD. Alice collects photon pairs emitted from a PDC source and uses a polarization beam splitter (PBS) to separate two polarization modes. She detects one of the two modes with her detector (DA) as a trigger, modulates the polarization of the other mode by a polarization controller (PC) and sends it to Bob. On Bob's side, he chooses his basis by a PC and performs a measurement by his detectors (DB_0 and DB_1).

single photon state. Thus it is sufficient for Bob to use threshold detectors. Threshold single photon detectors can only tell whether there is a click or not, but not the photon numbers. Bob needs to identify polarizations of incoming photons. Here, we assume Alice encodes qubit information in photon polarizations.

In real experiments, there are two types of PDC sources, both of which can be used in a triggering PDC QKD setup. Here, we assume Alice uses a type-II PDC source. The Hamiltonian of the type-II PDC process in the triggering setup shown in Figure 7.1 can be written as [119]:

$$H = i\chi a^\dagger b^\dagger + h.c. \quad (7.1)$$

where $h.c.$ means Hermitian conjugate and χ is a coupling constant which depends on the crystal nonlinearity and the amplitude of the pump beam. The operators a^\dagger , b^\dagger and a , b are the creation and annihilation operators of two modes with different polarizations.

The state coming from a triggering PDC source, with a Hamiltonian of Eq. (7.1), can be written as [119]:

$$|\Psi\rangle = (\cosh \chi)^{-1} \sum_{n=0}^{\infty} (\tanh \chi)^n |n, n\rangle. \quad (7.2)$$

Here, we assume that the state is single-mode. The expected photon pair number is given by $\mu = \sinh^2 \chi$. The probability to get an n -photon-pair is:

$$P(n) = \frac{\mu^n}{(1 + \mu)^{n+1}}. \quad (7.3)$$

Here, we assume that the PDC source always sends out photon pairs. That is, the photon number of mode a and b is always the same.

There is a nonzero probability for the PDC source to emit more than one photon pair in a pulse. Thus, Alice may send out multi photon states after she encodes basis and key information by her polarization controller (PC). This is the reason why the triggering PDC QKD suffers from PNS attacks. Later in the next chapter, we will show that when Alice uses the PDC source as an entangled photon source to implement an entanglement based QKD, it will be immune from PNS attacks.

Let us compare triggering PDC QKD and entanglement PDC QKD implementations. For the setup of entanglement PDC QKD, one can refer to Section 8.2. In the triggering PDC QKD, Alice actively encodes the key information, while in the entanglement PDC QKD, Alice measures the polarization of one mode of PDC source directly. The advantage of the triggering PDC QKD here is that it does not rely on the polarization correlations between two modes of the PDC source. It only requires the photon-pair generation of the source, which means entanglement between photon pairs are not important for the triggering PDC QKD. However, in an entanglement PDC QKD implementation, the entanglement between two modes has to be well maintained for QKD transmission. We notice that maintaining entanglement in real experiments is a highly non-trivial task⁴.

7.3 Model

Lütkenhaus studied the model of triggering PDC QKD [70] with threshold detectors. His model is similar to the one of the coherent state QKD, except for a different photon number distribution.

The channel model of triggering PDC QKD is exactly the same as the coherent state QKD. Thus, one can use Eqs. (3.6) and (3.9).

7.3.1 On Alice's side

In the triggering PDC QKD, Alice may use either a threshold detector or a photon-number resolving detector. A *N-photon-resolving* detector is defined to be a detector that can tell $0, 1, \dots, N$ photons of an incoming signal. For a threshold detector, we have $N = 1$, which can only tell the presence of photons, but not the photon numbers. Given an incoming i -photon state, the probability for Alice's detector to indicate a j -photon state is $\eta_{j|i}$, with $\sum_{j=0}^{j=N} \eta_{j|i} = 1$ for all $i = 0, 1, \dots$. In general, $\eta_{j|i}$ s are real

⁴A. M. Steinberg, private communication.

numbers in $[0,1]$. We define a j -photon trigger for a case where Alice's detector indicates a j -photon state.

For a triggered PDC photon source, as given in Eq. (7.2), the probability for Alice's detector to indicate a j -photon detection is:

$$P_{Aj} = \sum_{i=0}^{\infty} \frac{\mu^i}{(1+\mu)^{i+1}} \eta_{j|i}. \quad (7.4)$$

With the assumption that the PDC source always emits photon pairs, the probability (gain) for Alice getting a j -photon detection and Bob getting a detection is:

$$\begin{aligned} Q_{\mu,j} &= \sum_{i=0}^{\infty} Q_{i,j} \\ &= \sum_{i=0}^{\infty} \frac{\mu^i}{(1+\mu)^{i+1}} \eta_{j|i} Y_i, \end{aligned} \quad (7.5)$$

where the yield Y_i is given in Eq. (3.6). The quantum bit error rate (QBER) conditioned on Alice's j -photon detection, similar to Eq. (7.5), is given by:

$$\begin{aligned} E_{\mu,j} Q_{\mu,j} &= \sum_{i=0}^{\infty} Q_{i,j} e_i \\ &= \sum_{i=0}^{\infty} \frac{\mu^i}{(1+\mu)^{i+1}} \eta_{j|i} Y_i e_i. \end{aligned} \quad (7.6)$$

where the error rate e_i is given in Eq. (3.9).

It is observed that in the triggering PDC QKD setup, shown in Figure 7.1, the quantities Y_i and e_i are independent of Alice's measurement outcome j . This is based on the single-mode PDC source assumption described in Eq. (7.1) in Section 7.2. Therefore, in Section 7.4, we can apply the decoy state idea.

7.3.2 Threshold detector

Here, we will discuss a special case where Alice uses a threshold detector. That is,

$$\begin{aligned} \eta_{0|i} &= (1 - Y_{0A})(1 - \eta_A)^i \\ &\simeq (1 - \eta_A)^i \\ \eta_{1|i} &= 1 - \eta_{0|i} \\ \eta_{j|i} &= 0, \quad \forall j \geq 2, \end{aligned} \quad (7.7)$$

where Y_{0A} and η_A are the background count rate and the detector efficiency on Alice's side. The approximation is due to the fact that normally, we have $\eta_A \gg Y_{0A}$. That is, we neglect the background contributions on Alice's side.

According to Eqs. (7.5) and (7.6), without Eve's interference, the gains and QBER's of triggered ($j = 1$) and non-triggered ($j = 0$) detections are given by:

$$\begin{aligned}
Q_{\mu,0} &= \frac{1}{1 + \eta_A \mu} - \frac{1 - Y_{0B}}{1 + (\eta_A + \eta - \eta_A \eta) \mu} \\
Q_{\mu,1} &= 1 - \frac{1}{1 + \eta_A \mu} - \frac{1 - Y_{0B}}{1 + \eta \mu} + \frac{1 - Y_{0B}}{1 + (\eta_A + \eta - \eta_A \eta) \mu} \\
E_{\mu,0} Q_{\mu,0} &= e_d Q_{\mu|0} + \frac{(e_0 - e_d) Y_{0B}}{1 + \eta_A \mu} \\
E_{\mu,1} Q_{\mu,1} &= e_d Q_{\mu|1} + \frac{(e_0 - e_d) \eta_A \mu Y_{0B}}{1 + \eta_A \mu}.
\end{aligned} \tag{7.8}$$

Without Eve's interference, the gains and error rates of the single photon state in two detections are given by:

$$\begin{aligned}
Q_{1,0} &= \frac{\mu(1 - \eta_A)}{(1 + \mu)^2} Y_1 \\
Q_{1,1} &= \frac{\mu \eta_A}{(1 + \mu)^2} Y_1 \\
e_1 Y_1 &= e_d Y_1 + (e_0 - e_d) Y_{0B}
\end{aligned} \tag{7.9}$$

where Y_1 and e_1 are given in Eqs. (3.6) and (3.9), respectively.

7.3.3 Perfect photon-number resolving detector

Here, we will discuss the case where Alice uses a perfect photon-number resolving detector, which can faithfully tell the number of photons in the incoming signal. That is, $\eta_{j|i} = \delta_{ij}$. Thus, from Eqs. (7.5) and (7.6), the gains and QBERs are given by:

$$\begin{aligned}
Q_{\mu,i} &= Q_{i,i} = \frac{\mu^i}{(1 + \mu)^{i+1}} Y_i \\
E_{\mu,i} Q_{\mu,i} &= e_i Q_{i,i} = \frac{\mu^i}{(1 + \mu)^{i+1}} e_i Y_i,
\end{aligned} \tag{7.10}$$

from where one can directly infer the gains and error rates of the i -photon state, $Q_{i,j} = Q_{i,i} \delta_{i,j}$.

7.4 Post-processing

Here, we will apply the standard GLLP analysis, as shown in Eq. (2.6). All the classical data measured can be grouped according to Alice's detection events, $j = 0, 1, \dots, N$. Subsequently, we can apply the GLLP idea [35, 74] to each group. The final key generation rate will be given by summing over contributions from all groups:

$$R = \sum_{j=0}^N R_j. \quad (7.11)$$

In each case j , one can apply Eq.(7.19):

$$R_j \geq q\{-f(E_{\mu,j})Q_{\mu,j}H_2(E_{\mu,j}) + Q_{1,j}[1 - H_2(e_1)]\}, \quad (7.12)$$

where $Q_{0,j}$ and $Q_{1,j}$ are the first and second terms on the right hand side of Eq. (7.5). Here, the error rate of the single photon state e_1 is independent of j , see the observation in the end of Section 7.3.1. Note that the key generation rate from all j -photon trigger detections should be non-negative. If any of them contributes a negative key generation rate, we should assign 0 to it. In this case, Alice and Bob can just discard that type of detection. Based on this observation, we can further simplify Eq. (7.11). Given that Alice detects more than one photon, the probability of emitting a single photon state in Bob's arm is small⁵. As we mentioned in the beginning of this section, only a single photon state can contribute positively to the final key rate. Thus we can focus on the case $j = 0, 1$.

$$R = R_0 + R_1, \quad (7.13)$$

where R_0 and R_1 are given in Eq. (7.12). Again, both R_0 and R_1 should be non-negative, otherwise they should be assigned 0.

In Eq. (7.12), the gain $Q_{\mu,j}$ and the QBER $E_{\mu,j}$, given in Eqs. (7.5) and (7.6), can be measured or tested from QKD experiments directly. In this section, we will discuss various ways to estimate $Q_{0,j}$, $Q_{1,j}$, and e_1 . We assume that the PDC photon source and detector characteristics are fixed and known to Alice. That is, μ , the photon number distribution in Eq. (7.3) and η_A are fixed and known.

⁵In Section 7.2, we assume that Alice's PDC source always sends out photon pairs. Given that Alice detects more than one photon on the triggering arm, a single photon state is present on the other arm only when there is a dark count in Alice's detector. Normally, we can assume that the detector efficiency is much higher than the dark count probability on Alice's side. Thus, we neglect the probability of a single photon state with a multi photon trigger.

7.4.1 Non-decoy states with threshold detectors

Here, we assume that Alice uses a threshold detector. Thus, Alice only has two measurement outcomes, $j = 0, 1$. A simple way to estimate $Q_{0,j}$, $Q_{1,j}$, and e_1 is by assuming that all losses and errors come from the single photon states. This is because Eve can in principle, perform PNS attacks on the multi-photon states. The gain and error rate of the single photon states in triggered ($j = 1$) and non-triggered ($j = 0$) detections can be bounded by:

$$\begin{aligned}
Q_{1,0} &\geq Q_{\mu,0} - \sum_{i=2}^{\infty} \frac{\mu^i}{(1+\mu)^{i+1}} \eta_{0|i} \\
&= Q_{\mu,0} - \frac{(1-\eta_A)^2 \mu^2}{(1+\eta_A \mu)(1+\mu)^2} \\
Q_{1,1} &\geq Q_{\mu,1} - \frac{\eta_A(2-\eta_A+\mu)\mu^2}{(1+\eta_A \mu)(1+\mu)^2} \\
e_{1,0} &\geq \frac{E_{\mu,0} Q_{\mu,0}}{Q_{1,0}} \\
e_{1,1} &\geq \frac{E_{\mu,1} Q_{\mu,1}}{Q_{1,1}}
\end{aligned} \tag{7.14}$$

where η_A is the efficiency of Alice's detector. The gain Q_μ and the QBER E_μ , given in Eqs. (7.5) and (7.6), can be measured or tested from QKD experiments directly. In the following simulations, we will use Eq. (7.8). Since we assume all errors come from single photon states, one should take the lower bound of the vacuum contribution to be $Q_{0,j} = 0$.

7.4.2 Infinite active decoy state with threshold detectors

To perform a privacy amplification process, Alice and Bob need to bound $Q_{0,j}$, $Q_{1,j}$, and e_1 for Eq. (7.12). From Eq. (7.5), we know that to bound $Q_{0,j}$ and $Q_{1,j}$, Alice and Bob need to estimate Y_1 .

The decoy state method provides a good way to estimate Y_1 and e_1 [40, 65]. The essential idea is that instead of considering each linear equation of Y_1 and e_1 in the form of Eqs. (7.5) and (7.6) separately, Alice and Bob consider all the linear equations simultaneously.

Let us imagine that Alice and Bob obtain an infinite number of linear equations in the form of Eqs. (7.5) and (7.6), e.g., they use an infinite number of intensities μ . In principle, Alice and Bob can solve the equations to get Y_1 and e_1 accurately. Mathematically, the problem is solvable. The intuition is that the contributions from higher order terms of Y_i

and e_i decrease exponentially in Eqs. (7.5) and (7.6). For the case coherent state QKD, one or two decoy states are proven to be sufficient [77]. Shortly, we will see that one decoy state is sufficient for triggering PDC QKD.

The key underlying assumption of the decoy state method is shown in Eq. (4.2). In other words, Eve sets the same values of Y_i and e_i for the decoy and signal states. This can be guaranteed by the assumption that Eve cannot distinguish decoy and signal states.

In Appendix B.2, we will show that the optimal μ for the infinite decoy state case is in the order of 1, $\mu = O(1)$, which yields final a key rate $R = O(\eta)$. On the other hand, the optimal μ for the non-decoy case is $\mu = O(\eta)$, which yields a final key rate $R = O(\eta^2)$. Therefore, we expect the decoy state QKD to become a standard technique not only in the coherent state QKD, but also in QKD with triggering PDC sources.

There are various ways to apply the decoy state idea to the triggering PDC QKD [82, 2, 122]. Here, we consider the upper bound (infinite decoy state case) of all possible decoy protocols of triggering PDC QKD with threshold detectors: triggering PDC+infinite decoy method [65]. In the infinite decoy state method, Alice and Bob perform an infinite number of decoy states by choosing different intensities of the PDC source, μ . They can then solve the linear equations in the form of Eqs. (7.5) and (7.6) to estimate Y_1 and e_1 accurately. Hence, they can calculate each $Q_{0,j}$, $Q_{1,j}$, and e_1 accurately. In the simulation, we will use Eqs. (7.8) and (7.9) directly.

7.4.3 Weak active decoy state with threshold detectors

Here, we assume that Alice and Bob use threshold detectors and focus on triggered detection events. Alice uses another intensity ν , for instance, by attenuating the pumping laser, for the weak decoy state. Wang, Wang and Guo proposed a practical decoy method for triggering PDC QKD [122], which is essentially applying the Vacuum+Weak decoy state method [77] described in Section 5.1.1. Note that for triggered detection events, the vacuum contribution can be negligible since $\eta_A \gg Y_{0A}$. Thus there is no need to estimate the vacuum contribution here. Therefore, Alice and Bob only need to perform a weak decoy state instead of the Vacuum+Weak decoy states. In this case, only one weak decoy state is sufficient.

Bounds of Y_1 and e_1 are given by $\mu^2(1 + \nu)^3 \times Q_{\nu,1} - \nu^2(1 + \mu)^3 \times Q_{\mu,1}$ in Eqs. (7.5)

and (7.6):

$$\begin{aligned} Y_1 &\geq \frac{1}{\eta_A(\mu - \nu)} \left[\frac{\mu}{\nu} (1 + \nu)^3 Q_{\nu|1} - \frac{\nu}{\mu} (1 + \mu)^3 Q_{\mu|1} \right] \\ e_1 &\leq \min \left\{ \frac{(1 + \mu)^2}{\mu} \frac{E_{\mu,1} Q_{\mu,1}}{\eta_A Y_1}, \frac{(1 + \nu)^2}{\nu} \frac{E_{\nu,1} Q_{\nu,1}}{\eta_A Y_1} \right\} \end{aligned} \quad (7.15)$$

where ν is the expected photon pair number of the weak decoy state and η_A is the efficiency of Alice's threshold detector.

It is not difficult to show that when $\nu \rightarrow 0$, Eq. (7.15) approaches the infinite case, Eqs. (7.8) and (7.9), described in the previous subsection.

7.4.4 Passive decoy state

Recently, Maurer and Silberhorn proposed a passive decoy state scheme, in which photon-number resolving detectors are required [82]. Let us recap the heuristic idea of the original passive decoy state scheme briefly here. As discussed in Section 7.3, Alice and Bob eventually get different detection events grouped by triggers on Alice's side. The key idea proposed by Maurer and Silberhorn is that Alice and Bob manually combine the $\{j\}$ -trigger detection events to get the decoy states with different photon number statistics and then follow the regular decoy state scheme.

Here, we want to point out that the ‘‘combination’’ step is unnecessary. In general, each detection event group with a j -trigger has a different photon number statistic on the photon source arm. Thus, Alice and Bob need to treat all $\{j\}$ -trigger detection events statistics separately. Furthermore, photon-number resolving detectors are not necessary in passive decoy state schemes. Our new generalized passive decoy state scheme is as follows.

1. Alice uses a PDC source as her triggered photon source. She detects one of the modes from her PDC source as the trigger and encodes key information into another mode. Due to the detector Alice uses, she will get different trigger events: $j = 0, 1, \dots$. When she uses a threshold detector, she will only get $j = 0, 1$.
2. As the usual BB84 protocol, Bob measures signals in two different bases. Alice and Bob perform basis reconciliation.
3. Alice announces her trigger detection results for each pulse: j . Bob groups his detection events by the information j . For each j , they calculate the gain $Q_{\mu,j}$ and test the QBER $E_{\mu,j}$.

Mathematically, they will obtain a set of linear equations in the form of Eqs. (7.5) and (7.6). Notice that the setup parameters, μ and $\eta_{j|i}$ s, are known to Alice and Bob. Thus, they can estimate Y_1 and e_1 by considering Eqs. (7.5) and (7.6).

4. The post-processing is applied accordance to Eq. (7.13).

Note that the scheme is called *passive* because Alice does not actively select decoy states. Instead, she determines the decoy states by measuring the trigger mode. Later, we will show that this is one advantage of using the triggering PDC source for QKD. Actually, in this case, there are no strict definitions of decoy states and signal states. In the original decoy state method [77], decoy states are only used to estimate Y_1 and e_1 and the key is always generated from signal states⁶. In a triggering PDC QKD case, both the triggered $j = 0$ and non-triggered $j = 1$ detection events may have positive contributions to the final key generation.

7.4.5 Passive decoy state with threshold detectors

Here, we will review the decoy protocol proposed by Adachi, Yamamoto, Koashi and Imoto [2] as a special case of the passive decoy state protocol. The AYKI protocol is interesting in practice since it does not involve any hardware change to implement the decoy state idea.

Both Alice and Bob use threshold detectors, thus they have two types of detection events, triggered ($j = 1$) and non-triggered ($j = 0$). Secure keys can be generated from both types of detection events. Following the passive decoy state method procedure described in the previous subsection, Alice and Bob can estimate Y_1 and e_1 by considering the statistics of triggered and non-triggered detection events together. This is conceptually similar to the one decoy state idea [77] described in Section 5.1.2.

By solving two linear equations of Eq. (7.5) with $j = 0, 1$, $[1 - (1 - \eta_A)^2] \times Q_{\mu,0} - (1 - \eta_A)^2 \times Q_{\mu,1}$, one can get:

$$Y_1 \geq Y_1^L \equiv \frac{(1 + \mu)^2}{\mu} \left[\frac{2 - \eta_A}{1 - \eta_A} (Q_{\mu,0} - Q_{0,0}) - \frac{1 - \eta_A}{\eta_A} Q_{\mu,1} \right] \quad (7.16)$$

where $Q_{0,0}$ is the vacuum state contribution in non-triggered detection events. One needs to minimize the key rate of Eq. (7.13) for $Q_{0,0}$ with the constraint of Eq. (7.6). Note that this result is essentially Eq. (14) given in Ref. [2]. We can see that when η_A is close to

⁶In the coherent state QKD, there is an optimal μ for a setup. To maximize the final key rate, Alice and Bob should publicly compare all detection results from decoy states.

1 or μ is small, after neglecting $Q_{\mu,0}$ (background counts), the lower bound Y_1^L is tight (approaches the real value of Y_1 , see Eq. (3.6)):

$$\lim_{\eta_A \rightarrow 1} Y_1^L = \lim_{\mu \rightarrow 0} Y_1^L = \eta. \quad (7.17)$$

By neglecting the vacuum state contribution for triggered detection events, $Q_{0,1} = 0$, e_1 can be simply estimated by:

$$e_1 \leq \frac{E_{\mu,1}Q_{\mu,1}}{Q_{1,1}}. \quad (7.18)$$

To get the lower bound of Y_1 in Eq. (7.16), one has to estimate the background contribution $Q_{0,0}$ as well. A simple bound of $Q_{0,0}$ is $0 \leq Q_{0,0}e_0 \leq E_{\mu,0}Q_{\mu,0}$ from Eq. (7.6), where $e_0 = 1/2$.

Note that the key rate calculated by substituting Eqs. (7.16) and (7.18) into Eq. (7.13) is not optimal. To get a tighter key rate bound, one can numerically calculate the lower bound of Eq. (7.13) directly, given the measurement results, Eq. (7.9).

7.4.6 With a perfect photon-number resolving detector

Here, we discuss a special case where Alice uses a perfect photon-number resolving detector, discussed in Section 7.3.3. Now that Alice knows the exact photon number of the source, Alice and Bob only need to focus the post-processing on single photon state detection events. In this case, the BB84 protocol is implemented by single photon states only. Thus, they can directly apply Shor and Preskill's formula [106, 75]:

$$R \geq qQ_1[1 - f(e_1)H_2(e_1) - H_2(e_1)]. \quad (7.19)$$

Later from the simulation that is shown in Figure 7.2, we can see that a perfect photon-number resolving detector does not improve the QKD performance dramatically in comparison to the threshold detector case.

7.4.7 A few remarks

From the analysis of optimal μ in Appendix B.2, one can see that the key rate for a case without decoy states quadratically depends on the channel loss, $R = O(\eta^2)$, while for the case with decoy states, $R = O(\eta)$. This result is consistent with prior work that compared the cases of a coherent state QKD with and without decoy states [65].

In the decoy state security proof [65], the key assumption is that the decoy state and signal state should satisfy Eq. (4.2). This is guaranteed by the assumption that Eve

cannot distinguish decoy and signal states. However, in the active decoy state method, Alice may introduce side information that can distinguish decoy and signal states when she actively prepares decoy and signal states. For example, an attenuator on Alice’s side, used to prepare different intensities for signal and decoy states, may introduce different frequency shifts for signal and decoy states [131]. In general, it is difficult to verify the assumption that Eve cannot distinguish decoy and signal states in real active decoy state experiments.

In the passive decoy state scheme, decoy and signal states are passively determined by Alice’s measurement outcome. Alice does not use an extra component (such as in the active decoy state method) to prepare decoy states. This reduces the possibility of side information leakage. By passively choosing decoy states, Alice prepares same states on Bob’s arm⁷. In fact, Alice can measure trigger signals after Bob finishes his measurements. Thus, from Eve’s point of view, the states transmitted through the channel is independent of Alice’s measurement results (j). Therefore, in principle, Eve cannot distinguish the decoy and signal states in the passive decoy state QKD.

This is the main advantage in using the passive decoy state methods. Note that for a coherent state QKD, one can only use the active decoy state idea.

7.5 Simulation

In this section, we will compare the passive decoy state with a perfect number resolving detector and four QKD implementations with threshold detectors: non-decoy, infinite decoy, weak active decoy and AYKI (passive decoy state).

We deduce experimental parameters from a recent PDC experiment [115], which are listed in Table 7.1. In the following simulations, we will use $q = 1/2$ and $f(E_\mu) = 1.22$ in Eq. (7.12). We notice that with the slightly modified experiment setup, a coherent state QKD with decoy states is implemented [115]. Thus, it is reasonable to use this experiment setup to simulate the five QKD implementations.

In the simulation, for fair comparison, we always assume Bob uses the same detection setup (with threshold detectors).

⁷Strictly speaking, there is one underlying assumption: the PDC source is single-mode.

Repetition rate	Wavelength	η_{Alice}	η_{Bob}	e_d	Y_{0B}
249MHz	710 nm	14.5%	14.5%	1.5%	6.024×10^{-6}

Table 7.1: List of parameters from the 144 km PDC experiment [115]. Here, η_{Alice} and η_{Bob} are the detection efficiencies in Alice and Bob’s detection system, not including the optical channel loss. e_d is the intrinsic detector error rate. Y_{0B} is the background count rate of Bob’s detection system (for example, if Bob has two detectors, then Y_{0B} will be the sum of the background count rates of the two detectors). The transmission efficiency η in Eq. (3.6) is given by η_{Bob} plus the channel loss. Since Alice owns the PDC source, $\eta_A = \eta_{Alice}$.

7.5.1 Without statistical fluctuations

In the first simulation, we will consider a case where Alice and Bob perform an infinitely long QKD (no statistical fluctuations). In this case, the weak active decoy state protocol will approach the infinite decoy case, similar to the discussion in Section 5.1.1. We assume that Alice is able to adjust μ (the brightness of the PDC source) in the regime of $[0, 1]$ arbitrarily. In the simulation, we numerically optimize μ for each of the four implementation protocols: non-decoy, infinite decoy, AYKI and a case with a perfect number resolving detector. The simulation result is shown in Figure 7.2⁸.

From Figure 7.2, we have the following remarks.

1. In Appendix B.2, instead of numerically optimizing μ as the case was for Figure (7.2), we qualitatively investigate the optimal μ for triggering PDC QKD with and without decoy states. The simulation result is consistent with the qualitative conclusion $R = O(\eta)$ for the case with with decoy states and $R = O(\eta^2)$ for the case without decoy states.
2. The space between the solid and dashed line in Figure 7.2 indicates room left for improvement by other decoy protocols with threshold detectors after the AYKI protocol is implemented. We can see that, in a large regime of the optical link loss (for instance, between 0 dB and 25 dB), the performances of AYKI and the infinite decoy are close. For instance, the AYKI protocol yields around 50% of the key rate of the infinite decoy state protocol when the channel loss is within 20 dB.

⁸Here we simulate a free space QKD setup [115]. Since in a free space QKD system, the channel transmittance will depend on not only the distance but also other components, such as the size of the telescope, it is more appropriate to use the optical loss rather than the distance for x-axis of Figure 7.2.

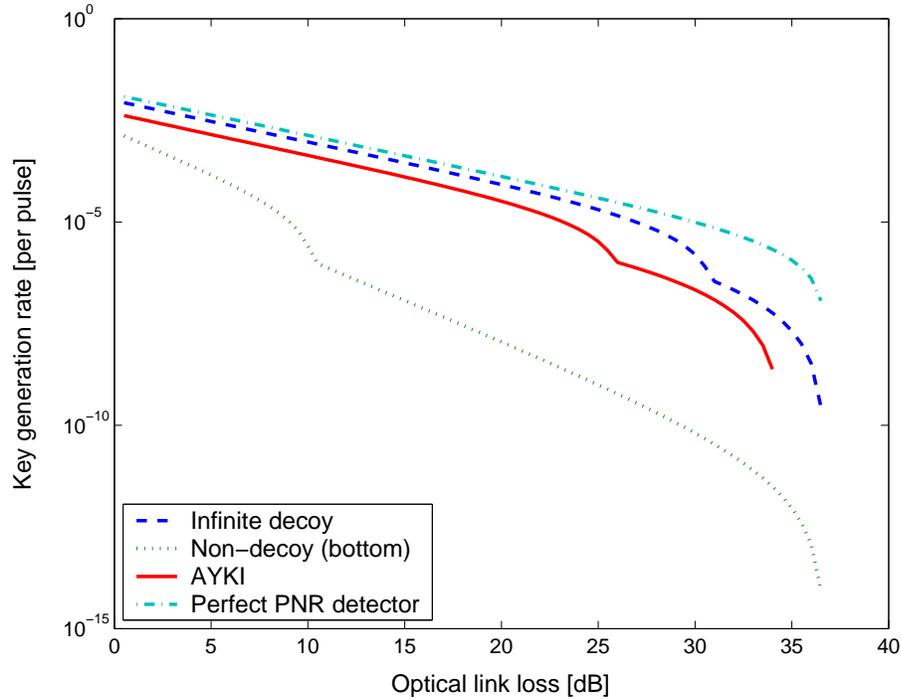


Figure 7.2: Plot of the key generation rate in terms of the optical loss, comparing four schemes without considering statistical fluctuations: non-decoy, infinite decoy, AYKI and a case with a perfect number resolving detector. Here, we use $q = 1/2$ and $f(E_\mu) = 1.22$. We numerically optimize μ for each curve, see Appendix B.2 for more discussions. Simulation parameters are listed in Table 7.1.

3. By comparing AYKI and a case with a perfect photon-number resolving detector, we can see that even with a perfect photon-number resolving detector on Alice's side, the key rate has not improved dramatically in a large regime of the optical link loss.
4. The non-decoy protocol is better than the AYKI in the regime close to maximal secure distances. This is because we use the bounds of Eqs. (7.16) and (7.18) for the AYKI curve. In reality, Alice and Bob can use the bound of Eq. (7.14) directly in this regime.
5. There is a bump in each curve. This is due to the fact that in the key generation rate formula Eq. (7.13), the non-triggered detection events have no contribution to the final secure key after the bump.
6. At the point of loss=0 dB, the key rates of four cases (from top to bottom) are

1.21×10^{-2} , 8.6×10^{-3} , 4.2×10^{-3} and 1.3×10^{-3} .

7. At the point of loss=0 dB, the numerical results for optimal μ for four cases (from top to bottom) are: 1, 0.52, 0.194, 0.0589. The optimal μ for the case with a perfect threshold detector is always 1, which is reasonable since $\mu = 1$ maximizes the single photon state probability. In Appendix B.2, we show that the optimal μ s for the infinite decoy and AYKI case are relatively stable in a large regime of the optical link loss (for instance, between 0 dB and 25 dB). The optimal μ for the no decoy state case decreases with channel loss.
8. Note that the real μ used in the experiment [115] is $\mu = 0.0265$. In general, it is experimentally difficult to increase the brightness (μ) of a PDC source.
9. All of the four cases can tolerate similar optical losses.

7.5.2 With statistical fluctuations

In a real experiment, the key length is always finite. Alice and Bob should consider statistical fluctuations. As pointed out in Section 5.2, the statistical fluctuation analysis is a complicated problem in the decoy state QKD scheme.

Similar to the analysis in Section 5.2, we assume a few conditions:

1. Alice knows the exact value of the average photon pair number μ , which is a fixed number during key transmission.
2. The distribution of the photon number, Eq. (7.3), does not fluctuate.
3. The QKD transmission is assumed to be part of an infinite length experiment.

Here, we focus on three cases with threshold detectors: infinite decoy, weak decoy and AYKI. We assume that the data size is 6×10^9 pulses of Alice's pumping laser. The simulation result is shown in Figure 8.5. From the simulation result, we have the following observations.

1. Similar to a case without the fluctuation analysis, in a large regime of the optical link loss, the performances of AYKI and the infinite decoy are close.
2. At the point of loss=0 dB, the key rates of the three cases from top to bottom are 8.6×10^{-3} (infinite), 5.0×10^{-3} (weak) and 4.7×10^{-3} (AYKI).

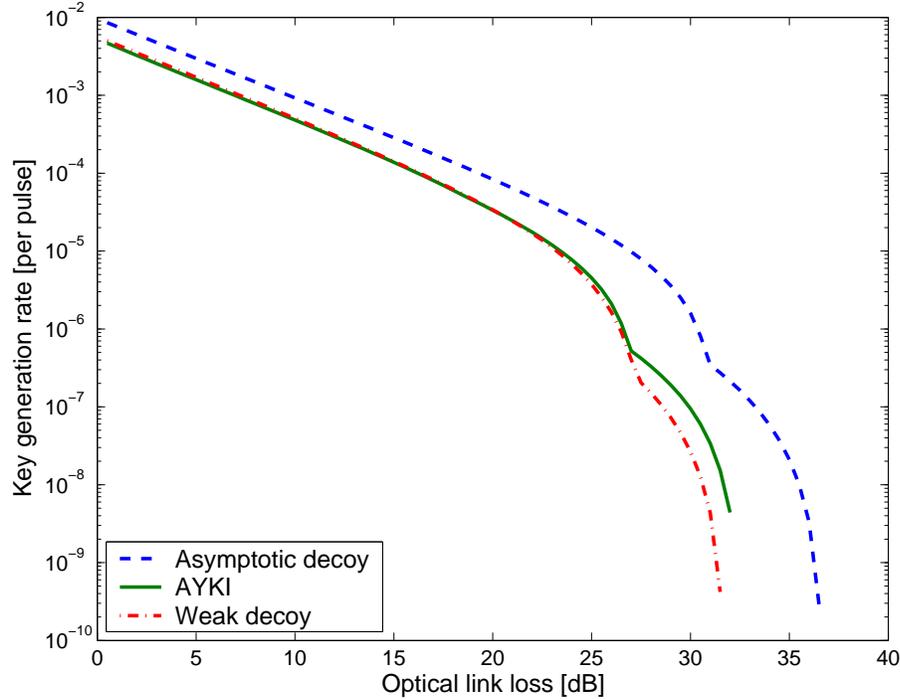


Figure 7.3: Plot of the key generation rate in terms of the optical loss, comparing three cases with threshold detectors after considering statistical fluctuations: infinite decoy, weak active decoy and AYKI. We numerically optimize μ for each curve. Here, we use $q = 1/2$ and $f(E_\mu) = 1.22$. In the weak decoy state case, we assume Alice can randomly attenuate her PDC source intensity. Simulation parameters are listed in Table 7.1. The data size is 6×10^9 pumping laser pulses on Alice’s side.

3. The maximal tolerable secure optical losses for the three cases are rather similar: 37 dB (infinite), 32.5 dB (AYKI), 32 dB (weak).
4. The AYKI protocol yields a higher key rate than the weak decoy state protocol when the loss is greater than 16 dB. AYKI is less affected by statistical fluctuations than the weak decoy state because in AYKI, Alice does not need to sacrifice extra pulses for decoy states.

In Section 7.4.7, we pointed out that from a practical security point of view, the passive decoy state method has an advantage over active decoy state methods. Moreover, the AYKI method does not require any additional hardware changes to implement the decoy state, while in the weak decoy state case, Alice needs to add an attenuator to create decoy states. Now, from the simulation result, we can see that the AYKI and

weak active decoy state method yield a similar QKD performance. Thus, our conclusion is that one should just use the AYKI method instead of the weak decoy state method.

7.6 Conclusion

By investigating the optimal photon source intensity, we find that the triggering PDC QKD setup with decoy states is able to achieve a key rate that linearly depends on the channel transmittance, in comparison to the quadratic dependence for the case without decoy states. Therefore, we expect the decoy state QKD to become a standard technique not only in the coherent state QKD, but also in QKD with triggering PDC sources.

On the practical side, we generalize the passive decoy state idea. The generalized passive decoy state idea can be applied to cases where either threshold detectors or photon number resolving detectors are used. The decoy protocol proposed by Adachi, Yamamoto, Koashi and Imoto (AYKI) can be treated as a special case of the generalized passive decoy state method. In comparison to the active (regular) decoy state methods, the passive one opens less possibility for Eve to distinguish decoy and signal states, which is a key underlying assumption in the security proof of the decoy state QKD scheme. From this sense, the passive decoy state method is more secure than the active decoy state methods in practice.

By simulating a recent PDC experiment, we compared various practical decoy state protocols with the infinite decoy protocol. We also compared cases using threshold detectors and photon-number resolving detectors. Our simulation result shows that with the AYKI protocol, one can achieve a key generation rate that is close to the theoretical limit of infinite decoy protocol. Furthermore, our simulation result suggests that a photon-number resolving detector has little room to improve the QKD performance, in comparison to the case using threshold detectors.

We also considered the statistical fluctuations. We compared infinite decoy protocol, weak active decoy state method and AYKI protocol. The simulation result shows that the weak active decoy state method and AYKI protocol yield a very close QKD performance. In a large regime of the optical link loss, the AYKI protocol can achieve a performance that is close to the infinite decoy case. Since the AYKI protocol requires no hardware changes for triggering PDC QKD, we conclude that AYKI method is a good protocol for triggering PDC QKD experiments.

Although our analysis is focused on QKD with PDC sources, we emphasize that it

can also be applied to other QKD setups with triggered single photon sources.

Chapter 8

Entanglement-based QKD

A parametric down-conversion (PDC) source can be used as either a triggered single photon source or an entangled photon source in QKD. The triggering PDC QKD was already studied in the previous chapter. However, a model and a post-processing protocol for the entanglement PDC QKD are still missing. Here, we fill in this important gap by proposing such a model and a post-processing protocol for the entanglement PDC QKD. Although the PDC model is proposed for studying the entanglement-based QKD, we emphasize that our generic model may also be useful for other non-QKD experiments involving a PDC source. Since an entangled PDC source is a basis independent source, we apply Koashi-Preskill's security analysis to the entanglement PDC QKD. We will also investigate the entanglement PDC QKD with two-way classical communication. Our results indicate that the recurrence scheme increases the key rate and Gottesman-Lo protocol helps tolerate higher channel losses. By simulating a recent 144 km open-air PDC experiment, we will compare three implementations: entanglement PDC QKD, triggering PDC QKD and coherent state QKD. The simulation result suggests that the entanglement PDC QKD can tolerate higher channel losses than the coherent state QKD. The coherent state QKD with decoy states is able to achieve the highest key rate in the low and medium-loss regions. By applying Gottesman-Lo two-way post-processing protocol, the entanglement PDC QKD can tolerate up to 70 dB of combined channel losses (35 dB for each channel) provided that the PDC source is placed in between Alice and Bob. After considering statistical fluctuations, the PDC setup can tolerate up to a 53 dB channel loss.

This work is published in Ref. [75]. In this work, I build an entangled PDC source model, apply Koashi-Preskill's security analysis and simulate a PDC experiment to show

the performance of the entanglement-based QKD in comparison with the triggering PDC QKD and coherent state QKD.

8.1 Introduction

As we discussed in Chapter 2, there are mainly two types of QKD schemes. One is the prepare-and-measure scheme, such as BB84 [11] and the other is the entanglement based QKD, such as Ekert91 [24] and BBM92 [12].

With a PDC source, one can realize either prepare-and-measure or entanglement-based QKD protocols [44]. To implement a prepare-and-measure QKD protocol, one can use a PDC source as a triggered single photon source. On the other hand, to implement an entanglement-based QKD protocol, one can use the polarization entanglement between two modes of light emitted from a PDC source. We call these two implementations the triggering PDC QKD and entanglement PDC QKD. With an entangled source, one can also implement QKD protocols based on causality [81] and Bell's inequality [1]. We notice that the PDC QKD based on the time-energy entanglement has been exploited [112].

Here, we present a model for the entanglement PDC QKD. From the model, we find that an entangled PDC source is a basis independent source for QKD. Based on this observation, we propose a post-processing scheme by applying Koashi-Preskill's security analysis [54].

Recently, a free-space distribution of entangled photons over 144 km was demonstrated [115]. We will simulate this experiment setup and compare three QKD implementations: entanglement PDC QKD, triggering PDC QKD and coherent state QKD. In the simulation, we will also apply Gottesman-Lo two-way post-processing protocol [34] and a recurrence scheme [118], see also [74].

The main contributions of this chapter are as follows.

- We present a model for the entanglement PDC QKD. Although the model is proposed to study the entanglement-based QKD, this generic model may also be useful for other non-QKD experiments involving a PDC source.
- From the model, we find that an entangled PDC source is a basis independent source for QKD. Based on this observation, we propose a post-processing scheme for the entanglement PDC QKD. Essentially, we apply Koashi-Preskill's security analysis [54].

- By simulating a PDC experiment [115], we compare three QKD implementations: entanglement PDC QKD, triggering PDC QKD and coherent state QKD. In the entanglement PDC QKD, we consider two cases: the source in the middle and source on Alice's side.
- In the case where the PDC source is placed in between Alice and Bob, we find that the entanglement PDC QKD can tolerate the highest channel losses, up to 70 dB by applying Gottesman-Lo two-way classical communication post-processing protocol [34]. Note that a 35 dB channel loss is comparable to the estimated loss in a satellite to ground transmission in the literature [6, 95, 45, 117, 4].
- We consider statistical fluctuations for the entanglement PDC QKD. In this case, the PDC setup can tolerate up to a 53 dB channel loss.
- The coherent state QKD with decoy states is able to achieve the highest key rate in the low and medium-loss regions.

In Section 8.2, we will review two experiment setups of the entanglement PDC QKD. In Section 8.3, the entanglement PDC QKD will be modeled. In Appendix A.5, we calculate the quantum bit error rate in the entanglement PDC QKD. In Section 8.4, a post-processing scheme for the entanglement PDC QKD will be proposed. In Section 8.5, we will compare the entanglement PDC QKD, the triggering PDC QKD and the coherent state QKD by simulating a real PDC experiment. We also apply protocols based on two-way classical communication and consider statistical fluctuations. In Appendix B.3, the optimal μ for the entanglement PDC QKD is investigated.

8.2 Implementation

In general, the entangled PDC source does not necessarily belong to one of the two legitimate QKD users, Alice or Bob. One can even assume that an eavesdropper, Eve, owns the PDC source. In this section, we will compare two experimental setups of the entanglement PDC QKD due to the position of the PDC source; in between Alice and Bob or on Alice's side.

Let us start with a general discussion about an entangled PDC source. With the rotating-wave approximation, the Hamiltonian of the PDC process can be written as [55]:

$$H = i\chi(a_H^\dagger b_V^\dagger - a_V^\dagger b_H^\dagger) + h.c. \quad (8.1)$$

where $h.c.$ means Hermitian conjugate and χ is a coupling constant depending on the crystal nonlinearity and the amplitude of the pump beam. The operators a_i and b_i are the annihilation operators for rectilinear polarizations $i \in \{H, V\}$ in modes a and b respectively. Modes a and b are the modes sent to Alice and Bob, respectively. Notice that the difference between this Hamiltonian and Eq. (7.1) is that in this case, one should consider two freedoms: polarization (H and V) and space (a and b).

In Section 8.3, we will focus on modeling the measurement of the rectilinear polarization (Z) basis. Due to symmetry, all the calculations can be applied to X basis too.

8.2.1 Source in the middle

First, we consider a case where the PDC source sits in between Alice and Bob. The schematic diagram is shown in Figure 8.1.

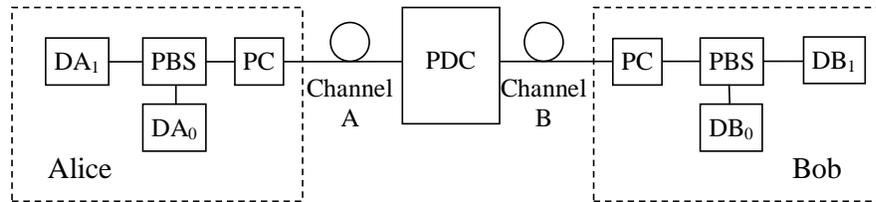


Figure 8.1: A schematic diagram for the entanglement PDC QKD. Alice and Bob connect to an entangled PDC source by optical links. They each receive one of two entangled modes coming out from the PDC source. Both Alice and Bob randomly choose basis (by polarization controllers) to measure the arrived signals (by single photon detectors). PC: polarization controller; PBS: polarization beam splitter; DA_0 , DA_1 , DB_0 , DB_1 : threshold detectors.

As shown in Figure 8.1, a PDC source provides two entangled modes, a and b , which are sent to Alice and Bob, respectively. After receiving the signals, Alice and Bob each randomly choose a basis (X or Z) to perform a measurement. A key observation of this setup is that the state emitted from the PDC source is independent of the bases Alice and Bob that choose for the measurements.

8.2.2 Source on Alice's side

Another case is where Alice owns the PDC source. The schematic diagram is shown in Figure 8.2.

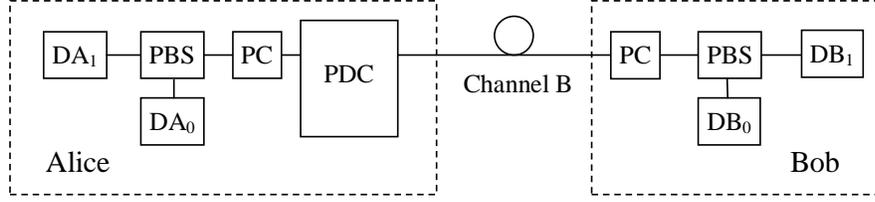


Figure 8.2: A schematic diagram for the entanglement PDC QKD. Alice measures one of entangled modes coming out from the PDC source and sends Bob the other mode.

In comparing Figures 8.1 and 8.2, we can see that the only difference is the position of the PDC source. As we will see Section 8.4, the post-processing of these two setups are similar.

Note that in the second setup, Alice's measurement commutes with Bob's measurement. Thus, we have the same observation as before where the PDC source state is independent of the measurement bases.

Therefore, for both setups, the entangled PDC source is a basis-independent source. It follows that the entanglement PDC QKD is a basis independent QKD.

8.3 Model

In this section, we will model an entangled PDC source, channel and detectors for the entanglement PDC QKD. We emphasize that this model is applicable for both experiment setups described in Section 8.2.

8.3.1 An entangled PDC source

From Eq. (8.1), the state emitted from a type-II PDC source can be written as [55]:

$$|\Psi\rangle = (\cosh \chi)^{-2} \sum_{n=0}^{\infty} \sqrt{n+1} \tanh^n \chi |\Phi_n\rangle, \quad (8.2)$$

where $|\Phi_n\rangle$ is the state of an n -photon-pair, given by:

$$|\Phi_n\rangle = \frac{1}{\sqrt{n+1}} \sum_{m=0}^n (-1)^m |n-m, m\rangle_a |m, n-m\rangle_b. \quad (8.3)$$

For example, when $n = 1$, Eq. (8.3) will give a Bell state:

$$\begin{aligned} |\Phi_1\rangle &= \frac{1}{\sqrt{2}}(|1, 0\rangle_a |0, 1\rangle_b - |0, 1\rangle_a |1, 0\rangle_b) \\ &= \frac{1}{\sqrt{2}}(|\leftrightarrow\rangle_a |\uparrow\rangle_b - |\uparrow\rangle_a |\leftrightarrow\rangle_b), \end{aligned} \quad (8.4)$$

Here, we use the polarizations $|1, 0\rangle = |\leftrightarrow\rangle$ and $|0, 1\rangle = |\uparrow\rangle$ as a qubit basis (Z basis) for QKD. From Eq. (8.2), the probability of getting an n -photon-pair is:

$$P(n) = \frac{(n+1)\lambda^n}{(1+\lambda)^{n+2}} \quad (8.5)$$

where we define $\lambda \equiv \sinh^2 \chi$. The expected photon pair number is $\mu = 2\lambda$, which is the average number of photon pairs generated by one pump pulse, characterizing the brightness of a PDC source.

8.3.2 Detection

Now we need to consider two channels: one for Alice and the other for Bob. We can apply the photon number channel model, described in Section 3.2.3, to each arm. The yield of an n -photon-pair Y_n mainly comes from two parts, the background and the true signal. Assuming that the background counts are independent of the signal photon detection, then Y_n is given by:

$$Y_n = [1 - (1 - Y_{0A})(1 - \eta_A)^n][1 - (1 - Y_{0B})(1 - \eta_B)^n] \quad (8.6)$$

where Y_{0A} and Y_{0B} are the background count rates on the sides of Alice and Bob, respectively. The vacuum state contribution is $Y_0 = Y_{0A}Y_{0B}$. The *gain* of the n -photon-pair Q_n , which is the product of Eqs. (8.5) and (8.6), is given by:

$$\begin{aligned} Q_n &= Y_n P(n) \\ &= [1 - (1 - Y_{0A})(1 - \eta_A)^n][1 - (1 - Y_{0B})(1 - \eta_B)^n] \frac{(n+1)\lambda^n}{(1+\lambda)^{n+2}}. \end{aligned} \quad (8.7)$$

The overall gain is given by:

$$\begin{aligned} Q_\lambda &= \sum_{n=0}^{\infty} Q_n \\ &= 1 - \frac{1 - Y_{0A}}{(1 + \eta_A \lambda)^2} - \frac{1 - Y_{0B}}{(1 + \eta_B \lambda)^2} + \frac{(1 - Y_{0A})(1 - Y_{0B})}{(1 + \eta_A \lambda + \eta_B \lambda - \eta_A \eta_B \lambda)^2}. \end{aligned} \quad (8.8)$$

Here, the overall gain Q_λ is the probability of a coincident detection event given a pump pulse. Note that the parameter λ is one half of the expected photon pair number μ .

The overall quantum bit error rate (QBER, E_λ) is given by:

$$E_\lambda Q_\lambda = e_0 Q_\lambda - \frac{2(e_0 - e_d)\eta_A\eta_B\lambda(1 + \lambda)}{(1 + \eta_A\lambda)(1 + \eta_B\lambda)(1 + \eta_A\lambda + \eta_B\lambda - \eta_A\eta_B\lambda)} \quad (8.9)$$

where Q_λ is the gain given in Eq. (8.8). The calculation of the E_λ is shown in Appendix A.5.

8.4 Post-processing

As mentioned in Section 8.2, the entanglement PDC QKD is a basis-independent QKD. Thus, we can apply Koashi and Preskill's security proof [54]. The key generation rate is given by:

$$R \geq q\{Q_\lambda[1 - f(\delta_b)H_2(\delta_b) - H_2(\delta_p)]\}. \quad (8.10)$$

where the subscript λ denotes for one half of the expected photon number μ , Q_λ is the overall gain, δ_b (δ_p) is the bit (phase) error rate, $f(x)$ is the bi-direction error correction efficiency.

Due to the symmetry of X and Z bases measurements, as shown in Section 8.2, δ_b and δ_p are given by:

$$\delta_b = \delta_p = E_\lambda, \quad (8.11)$$

where E_λ is the overall QBER. This equation is true for the asymptotic limit of an infinitely long key distribution. Later, in Section 8.5.3, we will see that Eq. (8.11) may not be true when statistical fluctuations are taken into account.

Note that in Koashi and Preskill's security proof, the squash model [35] is applied. In the squash model, Alice and Bob project the state onto the qubit Hilbert space before X or Z measurements. For more details of the squash model, one can refer to [35]. In the case where Alice owns the PDC source, as discussed in Subsection 8.2.2, the key rate formula of Eq. (8.10) has been proven [51] to be valid for the QKD with threshold detectors without the squash model, see also [67]. We also notice that this post-processing scheme, Eqs. (8.10) and (8.11), can be derived from the security analysis based on the uncertainty principle [52].

In Eq. (8.10), Q_λ can be directly measured from a QKD experiment and E_λ can be estimated by error testing. In the simulation shown in Section 8.5, we will use Eqs. (8.8) and (8.9).

Note that the post-processing for the entanglement PDC QKD is simpler than the coherent state QKD and triggering PDC QKD. In the entanglement PDC QKD, all the parameters needed for the post-processing (Q_λ and E_λ) can be directly calculated or tested from the measured classical data. On the other hand, in the coherent PDC QKD and the triggering PDC QKD, Alice and Bob need to know the value of some experimental parameters ahead of time, such as the expected photon number μ . They also need to estimate the gain and error rate of the single photon states Q_1 and e_1 , which make the statistical fluctuation analysis difficult [77], as investigated in Section 5.2.

The post-processing can be further improved by introducing two-way classical communication between Alice and Bob [34, 74]. Moreover, the adding noise technique may enhance the performance [56].

8.5 Simulation

In this section, we will first compare three QKD implementations: entanglement PDC QKD, triggering PDC QKD and coherent state QKD. Then we will apply post-processing protocols with two-way classical communication to the entanglement PDC QKD. Finally, we will consider the statistical fluctuations.

We deduce parameters from a recent PDC experiment [115] with respect to the model given in Section 8.3, which are listed in Table 7.1. For the coherent state QKD, we use $\eta_A = 1$ since Alice prepares the states in this case. In the following simulations, we will use $q = 1/2$ and $f(E_\mu) = 1.22$ [16].

The optimal expected photon number μ of the coherent state QKD is discussed in Ref. [70, 77]. In Appendix B.3, we investigate the optimal μ (2λ) for the entanglement PDC QKD. Not surprisingly, we find that the optimal μ for the entanglement PDC QKD is in the order of 1, $\mu = 2\lambda = O(1)$. Thus, the key generation rate given in Eq. (8.10) depends linearly on the channel transmittance.

8.5.1 Comparison of three QKD implementations

In the first simulation, we assumed that Alice was able to adjust the expected photon pair number μ (2λ , the brightness of the PDC source) in the region of $[0, 1]$. Thus, we can optimize μ for the entanglement PDC QKD and the triggering PDC QKD. The simulation results are shown in Figure 8.3. For the simulation of triggering PDC QKD with decoy states, one can refer to Section 7.5.

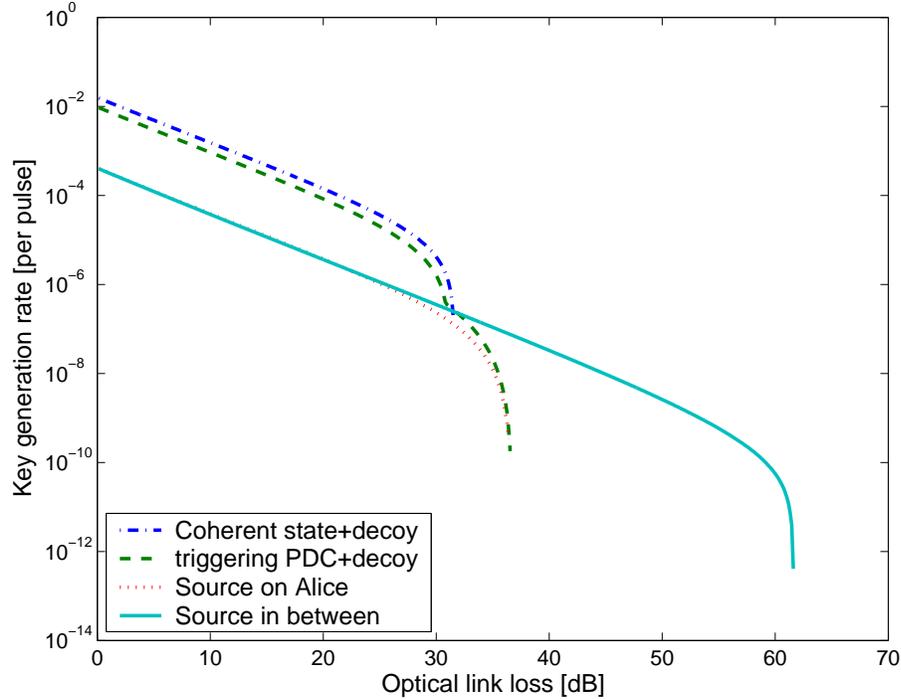


Figure 8.3: Plot of the key generation rate in terms of the optical loss, comparing four cases: coherent state QKD+asymptotic decoy, triggering PDC+asymptotic decoy, and entanglement PDC QKD (source in the middle and source on Alice’s side). For the coherent state QKD+decoy, we use $\eta_A = 1$. We numerically optimize μ (2λ) for each curve. The simulation of triggering PDC QKD with decoy states can be found in Section 7.5.

From Figure 8.3, we have the following remarks.

1. The entanglement PDC QKD can tolerate the highest channel losses in the case where the source is placed in the middle between Alice and Bob.
2. The coherent state QKD with decoy states is able to achieve the highest key rate in the low and medium-loss region. This is because in the coherent state QKD implementation, Alice does not need to detect any photons, which will effectively give $\eta_A = 1$ in the PDC QKD implementations.
3. In comparing two cases of the entanglement PDC QKD with a source in the middle and source on Alice’s side, they yield a similar key rate in the low and media- region. However, the source in the middle case can tolerate higher channel losses.

In the following simulations, we will focus on the case where the entangled PDC

source sits in the middle between Alice and Bob.

8.5.2 With two-way classical communication

We can also apply the idea of post-processing with two-way classical communication. Similar to the argument in Chapter 6, we can apply the recurrence idea [118] and the B steps described in Section 6.1.1. The simulation results are shown in Figure 8.4.

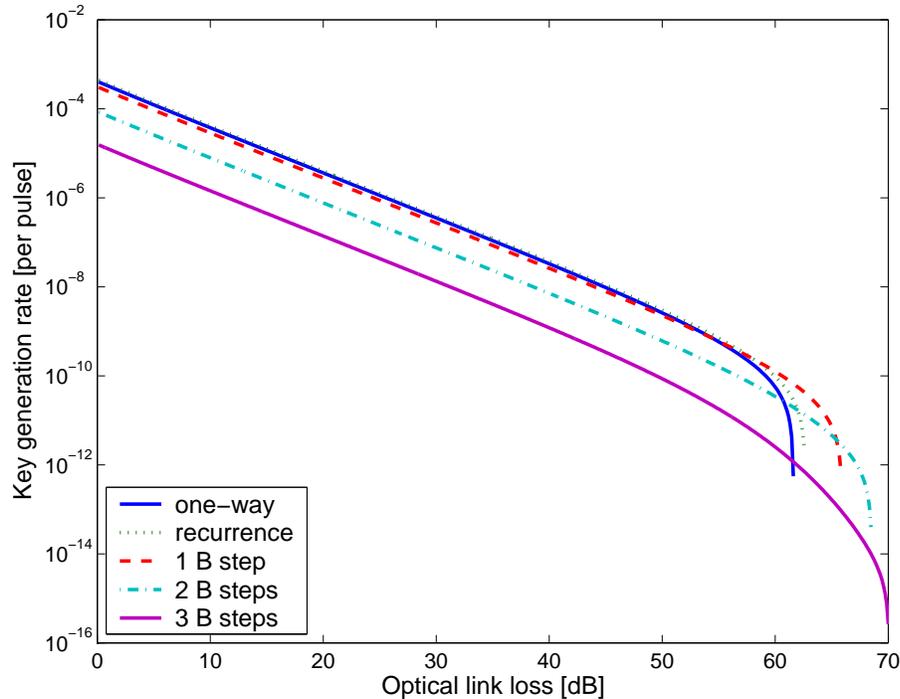


Figure 8.4: Plot of the key generation rate in terms of the optical loss. We apply the recurrence idea and up to 3 B steps. μ is numerically optimized for each curve.

From Figure 8.4, we can see that the recurrence scheme can increase the key rate by around 10% and extend the maximal tolerable loss by around 1 dB. The PDC experiment setup can tolerate up to a 70 dB channel loss with 3 B steps. Note that 70 dB (35 dB in each channel) is comparable to the estimated loss in a satellite to ground transmission [117]. This result suggests that satellite-ground QKD may be possible. However, this simulation assumes an ideal situation where an infinite number of signals are transmitted. Moreover, we assume that μ (the brightness of the PDC source) is a freely adjustable parameter in the PDC experiment. In a more realistic case where a finite number of signals are transmitted and μ is a fixed parameter, the tolerable channel loss becomes smaller, which will be shown next.

8.5.3 Statistical fluctuations

In Eq. (8.11), we assume that δ_b and δ_p are the same due to the symmetry between X and Z measurements. Alice and Bob randomly choose to measure in X or Z basis. Then asymptotically, δ_b is good estimate of δ_p . However, in a realistic QKD experiment, only a finite number of signals are transmitted. Thus δ_p may slightly differ from δ_b . We assume that Alice and Bob do not perform error testing explicitly. Instead, they obtain the bit error rate directly from an error correction protocol (e.g., the Cascade protocol [16]). In such a case, there is no fluctuation in the bit error rate $\delta_b = E_\lambda$. On the other hand, the phase error rate may fluctuate to a certain value of $\delta_p = \delta_b + \epsilon$. Following the fluctuation analysis of Ref. [106], we know that the probability of getting an ϵ bias is

$$P_\epsilon \leq \exp\left[-\frac{\epsilon^2 n}{4\delta_b(1 - \delta_b)}\right], \quad (8.12)$$

where $n = NQ_\lambda$ the number of detection events, the product of total number of pulses N and the overall gain Q_λ .

In the 144 km PDC experiment [115], the repetition rate of the pump pulse is 249MHz as given in Table 7.1. As discussed in Ref. [117], the typical time of a ground-satellite QKD allowed by satellite visibility is 40 minutes. Here, we assume the experiment runs 10 minutes, which means the data size (the number of the pumping pulses) is $N = 1.5 \times 10^{11}$. By taking this data size, we considered the fluctuations for the entanglement PDC QKD.

In a realistic case, the brightness of the PDC source μ cannot be set freely. In the 144 km PDC experiment [115], the expected photon pair number is $\mu = 2\lambda = 0.053$. After taking $\mu = 0.053$ and the data size of $N = 1.5 \times 10^{11}$ for the fluctuation analysis, the simulation result is shown in Figure 8.5.

We have a couple remarks about Figure 8.5.

1. In Figure 8.5, if we use the key rate of 10^{-10} as the cut-off point¹, the entanglement PDC QKD with one B step can tolerate up to a 53 dB transmission loss.
2. We have tried simulations with various μ s. We find that the key rate is stable with moderate changes of μ . With the above fluctuation analysis, if we numerically optimize μ for each curve, the maximal tolerable channel loss (with cut off key rate of 10^{-10}) is only 1 dB larger than the one given by $\mu = 0.053$. Thus, one cannot

¹Then the final key length is 15 bits. One should also consider the cost in the authentication procedure. Thus this is a reasonable cut off point.

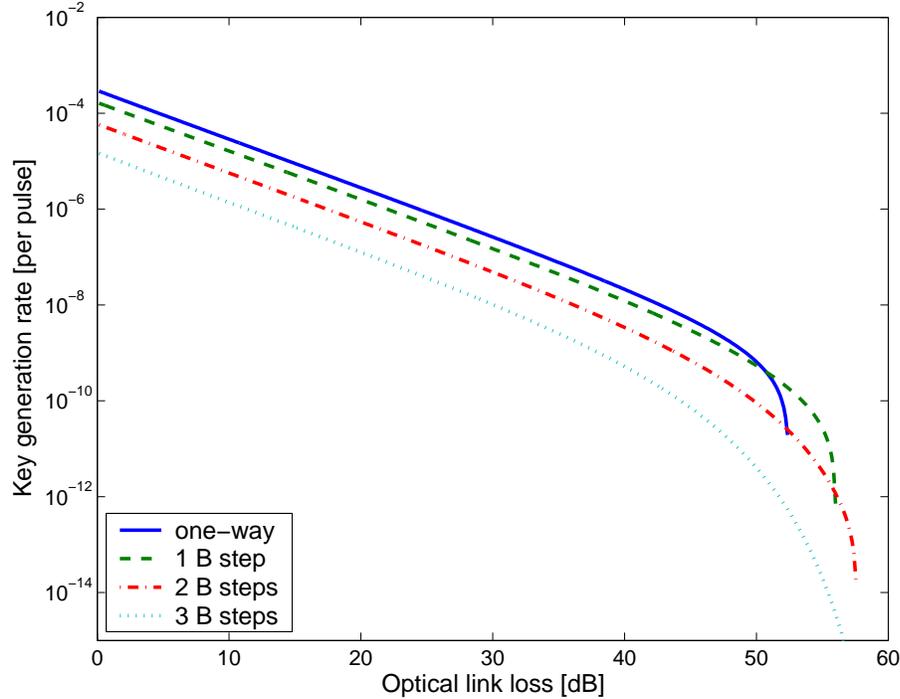


Figure 8.5: Plot of the key generation rate in terms of the optical loss. We take a realistic $\mu = 2\lambda = 0.053$, and consider a fluctuation with a data size (the number of the pumping pulses) of $N = 1.5 \times 10^{11}$ and a confident interval of $1 - P_\epsilon \geq 1 - e^{-50}$.

significantly improve the maximal tolerable channel loss by just using a better PDC source in the 144 km PDC experiment setup [115].

8.6 Conclusion

We proposed a model and post-processing protocol for the entanglement PDC QKD. We find that the post-processing is simple by applying Koashi-Preiskill's security proof due to the fact that the entanglement PDC QKD is a basis independent QKD. Specifically, only directly measured data (the overall gain and the overall QBER) are needed to perform the post-processing. By simulating a recent experiment, we compare three QKD schemes: coherent state QKD+asymptotic decoy, triggering PDC+asymptotic decoy, and entanglement PDC QKD (source in the middle and on Alice's side). We find that a) the entanglement PDC (with source in the middle) can tolerate the highest channel loss; b) the coherent state QKD with decoy states can achieve the highest key rate in the medium- and low-loss regions; c) asymptotically, with a realistic PDC experiment

setup, the entanglement PDC QKD can tolerate up to a 70 dB channel loss by applying post-processing schemes with two-way classical communication; d) the PDC setup can tolerate up to a 53 dB channel loss when statistical fluctuations are taken into account.

Chapter 9

Quantum cryptanalysis

In this chapter, we will discuss existing security loopholes in current QKD setups. We propose a technologically feasible attack and present possible solutions. Note that although the attack is proposed for the BB84 coherent state QKD implementation, the attack works for many other protocols as well.

The theoretical work of the time-shift attack is published in Ref. [90]. The security proof of efficiency mismatch is presented in Ref. [29]. Aside from the decoy state method, we also studied other methods to improve the QKD performance, such as dual detector scheme [93, 92]. Note that I am not the main contributor of these projects. I joined in discussions and helped work out the details.

9.1 Side information

In Chapter 2, we discussed various security analyses of QKD. In many cases, we assumed that Eve cannot learn about bit values or basis information directly from Alice and Bob's systems, e.g., by breaking into Alice or Bob's box. As we pointed out in Section 2.2, in the security proofs, many rely on the assumption of the squash model. In reality, the bit value or basis information might be revealed to Eve through some side channels. For example, two detectors used in QKD systems may have different properties, which might reveal to Eve partial information about the bit values.

9.1.1 Detector inefficiency loophole

Before examining the details of possible side information channels in current QKD setups, let us take a look at a fundamental reason for existence of these loopholes.

An important piece of evidence that indicates the validity of quantum mechanics is shown by the violation of the Bell inequality [8] and its descendant experiment verifications (see for example, Ref. [5]). The experiments show that the concept of traditional local realism is inconsistent with quantum mechanics and then, with the real world. However, this verification has not been completely conclusive, since there exists certain loopholes in these experiments. See for example, [87, 19, 30].

Since entanglement is the precondition of QKD security [20] and the concept of entanglement is closely related to Bell's inequality¹, a natural question is “Does this detector inefficiency loophole affect the security of QKD?” As we will show shortly, the answer is *yes*.

9.1.2 Timing information

In many QKD systems, detectors are operated in a gated mode in order to reduce the dark count rate. In general, the width of SPD's open window (a few ns) is often substantially larger than the laser pulse duration (a few hundreds ps). Here, we treat the signal pulse as a delta function in time-domain.

Typically, Bob uses two separate single photon detectors, which are labeled as SPD0 and SPD1, to detect bit “0” and bit “1”, respectively. In real life, due to device imperfections, the time-dependent efficiencies of the two detectors are not identical in general as shown in Figure 9.1.

Ideally, Alice and Bob can synchronize the laser pulse with the center of the time window (T_0 in Figure 9.1). This ensures that a small detector efficiency mismatch will not affect the normal operation of the QKD system. In reality, the timing may be shifted by a small amount due to fluctuations or device imperfections². Thus, the pulse timing contains information about the detector efficiencies, which may reveal the detection bit values.

Note that other freedoms of the signal may also introduce similar problems. For example, two detectors may respond differently in the frequency domain [91]. In the following discussions, we will focus on the efficiency mismatch due to signal timing.

¹Although entanglement does not promise violation of the Bell's inequality.

²Shortly, we will see that Eve may shift the pulse large for her attack.

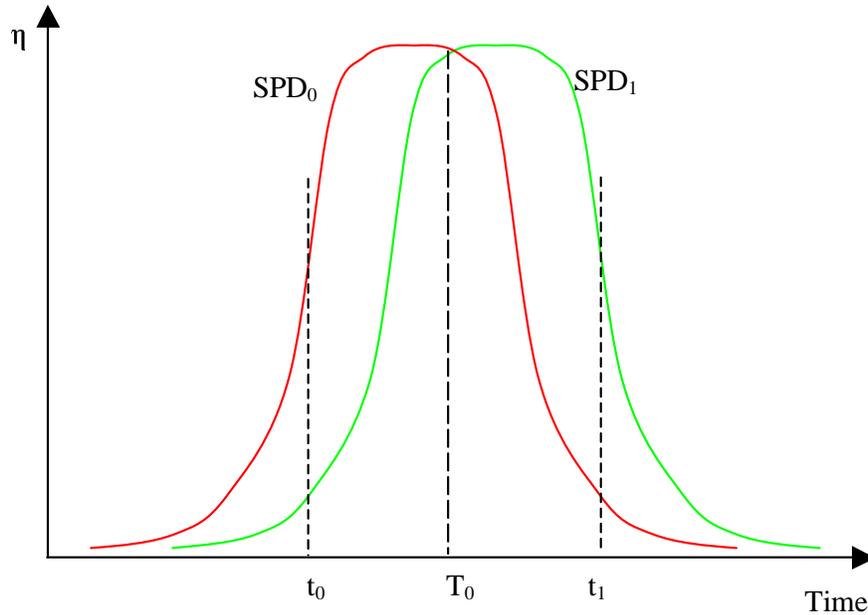


Figure 9.1: The time-dependence efficiencies of single photon detectors (SPDs).

9.2 Time-shift attack

Recently, an eavesdropping attack that exploits this efficiency mismatch of detectors in the QKD system has been proposed [78]. In this attack, Eve intercepts and performs a complete von Neumann measurement on each quantum state sent out by Alice. She then generates a new time-shifted signal based on her measurement result and sends it to Bob.

Note that to implement this attack in Ref. [78], Eve will need a complicated detection (similar to Bob’s system) and resend (similar to Alice’s system) system. If we assume that Eve builds her “practical” eavesdropping device based on today’s technology, she will also experience the problem of low detection efficiency and will introduce additional errors due to imperfections in her setup.

Based on this work, we propose a simple practical attack: time-shift attack [90]. In our attack, Eve does not measure the quantum state that is sent to Alice. Instead, Eve simply shifts the arrival time of either the signal pulse or the synchronization (reference) pulse or both between Alice and Bob. Consequently, Eve has control of the arriving time of the pulse. For example, she shifts the pulse to t_0 in Figure 9.1 and then Bob claims a detection event of that pulse. Now, Eve knows with a high probability that SPD0 clicks. Hence, she can guess Bob’s measurement result 0. In an extreme case where there is a

complete detector efficiency mismatch³, Eve can acquire full information on the final key without introducing any error. In other words, a naïve application of standard security proofs, for instance, the GLLP [35] security analysis, without taking into account the detector efficiency mismatch is invalid.

Figure 9.2 shows a schematic diagram for the experimental realization of the time-shift attack. Instead of measuring Alice’s quantum state, Eve just randomly shifts the time of Alice’s quantum state to make sure that it arrives at Bob’s detector at either time t_0 or t_1 . When Eve chooses time t_0 and Bob detects a signal, with the probability of $\eta_0/(\eta_0 + \eta_1)$, the bit value will be “0”. Here, we assume that the detector efficiencies of SPD0 and SPD1 are η_0 and η_1 at time t_0 and Alice chooses bit “0” and “1” with an equal prior probability. Because the probability that Eve incorrectly guesses Bob’s bit value is $\eta_1/(\eta_0 + \eta_1)$, therefore, Eve’s knowledge about the final key is given by:

$$I(B : E) = 1 - H_2\left(\frac{\eta_1}{\eta_0 + \eta_1}\right). \quad (9.1)$$

Note in this attack, Eve does not measure Alice’s state. Therefore, Eve will not introduce extra errors. Due to the symmetry, the same analysis can also be applied to the case when Eve chooses t_1 .

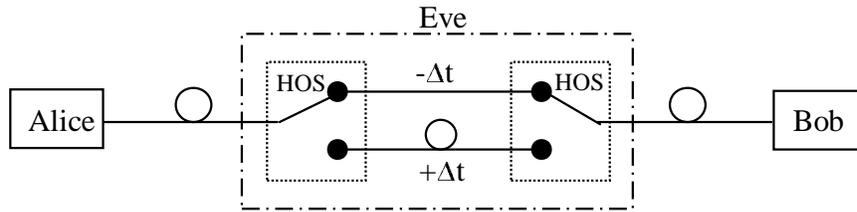


Figure 9.2: A schematic diagram of Eve’s attack. HOS: high-speed optical switch.

In comparison with the attack in Ref. [78], our attack is simpler and can be easily realized with today’s technology: Eve can use high speed optical switches to re-route Alice’s signal through either a long or short optical path to achieve the desired time shift. Another advantage of our attack is that Eve will never introduce errors. Therefore, it is difficult for Alice and Bob to detect Eve’s presence.

For details of the time-shift attack, one can refer to Ref. [90]. Note that our time-shift attack was experimentally realized in our lab [130].

³That is to say, there is a time window where SPD0 (or SPD1) is active while SPD1 (or SPD0) is completely inactive.

9.3 Security against time-shift attack

Now that we know about the time-shift attack, we can provide a secure QKD against the attack. There are two approaches: hardware based and software based. In the hardware based approach, we perform some counter measurements or improve the system setups. In the software based approach, we provide a security analysis with detector efficiency mismatch.

9.3.1 A simple solution

To counter Eve’s attack, Alice and Bob could develop various countermeasures, such as those discussed in Ref. [78]. Note that a recently proposed single SPD QKD system is also immune to this attack [58]. In a phase encoding BB84 version of this design, instead of randomly selecting from a set of two values, Bob’s phase modulation is randomly selected from a set of four values, which is identical to the set for Alice’s phase modulation. In this case, Bob not only randomly chooses his measuring basis for each incoming pulse, he also randomly determines which SPD is used for detecting bit “0” or bit “1”. Bob broadcasts his basis choice, but keeps his choice of detector (for the bit “0” or “1”) secretly. In such a set-up, even if Eve has information about which detector clicks, Eve still cannot work out Bob’s bit value because she does not know which detector corresponds to the bit “0”. Bob’s random choice of detectors to detect the bit “0” or “1” will even out the efficiency mismatch.

9.3.2 Security proof for a QKD system with detector efficiency mismatch

Here, we will only discuss the security proof for a simple scenario: single photon source, noiseless channel and the efficiencies of two detectors, which are η_0 and η_1 , to detect the bit “0” and “1”⁴. For a full discussion of the security proof for a QKD system with efficiency mismatch detectors, one can refer to Ref. [29].

In this simple QKD picture, Eve does not introduce any bit or phase errors, but only intervenes in the auxiliary dimension to gain side information. As discussed in Section 2.4, the state shared by Alice and Bob after transmission (Eve’s intervention) and basis

⁴In real time-shift attack, Eve might shift the pulse in various positions. Here, we only consider one point that will cause a detector efficiency mismatch. In general, η_0 and η_1 can be characterized by a tensor in the auxiliary dimension (for instance, time domain).

reconciliation is

$$(|00\rangle + |11\rangle)_{AB} \mapsto (\sqrt{\eta_0}|00\rangle + \sqrt{\eta_1}|11\rangle)_{AB} \quad (9.2)$$

Eve does not introduce any bit errors and she simply attaches an extra system T , by shifting the timing of the signals that represents her intervention in the auxiliary dimension.

With a hashing based EDP [13], the amount of EPR pairs that Alice and Bob can distill from the final state is $H_2(\eta_0/(\eta_0 + \eta_1))$, which is consistent with the result of Eq. (9.1). Note that when $\eta_0 \neq \eta_1$, the key rate is less than 1 in comparison to the perfect case of $R = 1$.

9.4 Discussion

From this cryptanalysis exercise, we learn that a security proof is only as good as its underlying assumptions. Once a security loophole has been discovered, it is often not very difficult to develop countermeasures that will plug the loophole and regain unconditional proofs of security of the QKD system. One example is the time-shift attack that we mentioned above. However, the difficult part is how to identify such security loopholes in the first place. A QKD system is a complicated system with many intrinsic imperfections. It is, thus, very important to conduct extensive research on such imperfections carefully to determine if they are innocent or fatal for security. We need more quantum hackers in the field. The investigation of loopholes and countermeasures in practical QKD systems plays a complementary role to security proofs.

Given that a practical QKD system will always have imperfections, one might wonder if QKD systems offer any real advantages over conventional systems. Our answer is three-fold. First of all, implementation loopholes are a fact of life. Even conventional security systems, such as smart cards, suffer implementation loopholes. For instance, Eve may attempt to read off a private key from a smart card by using various techniques (including X-ray) to reverse-engineer the circuit embedded in a smart card. Secondly, QKD can be used in concatenation with a conventional system to ensure security. By defending in depth, QKD can only increase security, not reduce it. Thirdly, QKD has an important advantage of being future-proof: The signals are quantum. Once the transmission is done, there is no transcript for the transmission. For an eavesdropper to launch a quantum attack, she has to possess much of the quantum technology during the quantum transmission. In contrast, in a standard Diffie-Hellman public-key key exchange

scheme, Eve has a complete transcript of the transmission and can save such a transcript for decades to wait for unexpected future advances in hardware and algorithms. Given that public key crypto-systems are an unexpected discovery made only three decades ago, our view is that it will be complacent to believe that our standard public key crypto-systems will be safe forever. Therefore, it pays to reduce one's risk by defending in depth with a QKD system in concatenation with a conventional cryptosystem.

Chapter 10

Conclusions and outlook

In this chapter, I will conclude my thesis by summarizing the results of my Ph.D. study and stating some interesting topics for future research.

10.1 Decoy state QKD

The major topic in my Ph.D. study is decoy state quantum key distribution (QKD). The main results are presented in Chapters 4, 5, 6 and 7.

Recall that the motivation of this thesis is to bridge the gap between theory and practice of QKD. One of the major problems in a practical QKD system is that a single photon source is difficult to obtain with current technology. Now, with the decoy state method, the key rate is linearly dependent on the channel transmission. Note that this is the highest order that the key rate can reach even with a perfect single photon source. Hence, with decoy states, one can treat weak coherent state sources and triggering parametric down-conversion (PDC) sources as good single photon sources for QKD setups.

For practical implementations, we showed that with only one or two decoy states, one can achieve most of the benefits of the decoy state method. Further improvement for the decoy state QKD was studied by considering two-way classical communication in the post-processing step. With our two-way classical communication based schemes, one can obtain a performance that is close to the theoretical limit. We also investigated the decoy state method for other photon sources, triggering PDC source. With similar results concluded, we expected the decoy state QKD to become a standard technique not only in the coherent state QKD, but also in QKD with triggering PDC sources.

All the decoy state QKD experiment demonstrations, including our first realization, showed that the decoy state idea is easy to implement in real system setups. Therefore, we conclude that the practical quantum cryptography is close to real-life applications.

10.2 Other topics

As an extension of the decoy state QKD work, we searched for other techniques to improve the QKD performance of practical systems. We proposed a dual detector scheme to improve the case when fast and noisy detectors are in use.

We also investigated other QKD protocols, such as the entanglement based QKD protocols. By simulating a recent experiment, we showed that a) with an entangled PDC source in the middle, the QKD setup can tolerate highest channel loss comparing to decoy state QKD protocols; b) the coherent state QKD with decoy states can achieve the highest key rate in the medium- and low-loss regions.

Security is the most important issue in QKD. We studied various eavesdropping attack schemes in quantum cryptography. We proposed a technologically feasible attack scheme and presented possible solutions. Note that although the attack is proposed for the BB84 coherent state QKD implementation, the attack works for many other protocols as well. We also studied the countermeasures against this attack. We provided a security proof for a QKD system with detector efficiency mismatch.

10.3 Future work outlook

In the future, one interesting topic is a natural extension of my previous work: enhancing the performance of practical QKD systems. Further improvements, both in key rate and secure transmission distance, are required for some applications. Another crucial point is that, in real life, one needs to consider some extra disturbances (e.g., quantum signals may share the channel with regular classical signals). The final goal is to achieve a customer friendly QKD system that can be easily integrated with the Internet.

To achieve an intercontinental transmission distance, ground-satellite QKD is a promising proposal. One interesting project is to test the feasibility of ground-satellite QKD. In Chapter 8, we have preliminarily studied the feasibility of ground-satellite QKD with the current entangled photon source. Previously, we used a beam splitter as a channel model for ground-satellite QKD. A study of the disturbance of atmosphere is needed

to develop a more realistic model for the ground-satellite channel. By modeling and simulating, one can investigate the requirement for QKD components. For example, what efficiency and noise level of single photon detectors are required and how large the telescope is needed. Meanwhile, it is interesting to explore good QKD schemes for ground-satellite QKD.

To achieve a higher QKD key rate, one can consider other QKD protocols. Continuous variable QKD is proposed to achieve a higher key rate in the short and medium transmission distance. One open question is the security of continuous variable QKD. This is an appealing topic in the field. Modeling and simulations for continuous variable QKD are also interesting.

Statistical fluctuations need to be considered in QKD with a finite key length. There is some work on this topic recently (e.g., by Renner [96]). One interesting topic is to apply Koashi's complementary idea [53] to finite key QKD and compare it with prior results.

It has already been known that one can realize quantum gates by quantum teleportation [33]. There are some proposals for the experimental quantum computation with linear optics [47]. However, the scalability is a huge challenge. As yet, no one knows how to build a large scale quantum computer. A long-term challenge in the field is to find a practical proposal for a quantum factoring machine with current technology. Here a interesting topic is that whether those techniques developed in QKD could be useful to quantum computing. For instance, can the restrictions in single photon source be loosened by applying decoy idea?

Appendix A

Abbreviations and mathematical derivations

A.1 Abbreviations

The following abbreviations are used in this thesis.

- QKD: quantum key distribution
- BB84: the QKD protocol presented by Bennett and Brassard in 1984 [11]
- EPR pair: a maximally entangled photon pair that originated from the Einstein-Podolsky-Rosen paradox [89]
- EDP: entanglement distillation protocol
- LOCC: local operations and classical communication; 1-LOCC: local operations and one-way classical communication; 2-LOCC: local operations and two-way classical communication
- PDC: parametric down-conversion
- GLLP: the security proof of QKD with imperfect devices proposed by Gottesman, Lo, Lütkenhaus, and Preskill [35]

A.2 Key rate of the recurrence scheme with an ideal single photon source

In this section, we will review the recurrence EDP and develop the key generation rate formula given by:

$$R = q \cdot r, \quad (\text{A.1})$$

where q is the basis reconciliation factor and r is the residue of post-processing which we will find in the sequel. In the following, we use the same notation as in Section 2.4 and consider a Bell diagonal state $(q_{00}, q_{10}, q_{11}, q_{01})$.

A.2.1 Parity check

As the first step of recurrence, Alice and Bob check the parity of two pairs (labeled by control qubit C and target qubit T). They will get an even parity if the two pairs are in one of the following states:

$$0000, 0001, 0100, 0101, 1010, 1011, 1110, 1111,$$

and will get odd parity if they are in one of the following states:

$$0010, 0011, 0110, 0111, 1000, 1001, 1100, 1101,$$

where the first two bits represent the control qubit, and the last two bits represent the target qubit. That is, ij represents the Bell state $|\psi_{ij}\rangle$ as given in Eq. (2.2) with $i, j = 0, 1$. For example, 1110 means that there is a bit error and a phase error in the control qubit ($|\psi_{11}\rangle$), and a bit error and no phase error in the target qubit ($|\psi_{10}\rangle$). Thus, the probability to get an even parity is given by:

$$\begin{aligned} p_S &= (q_{00}^C + q_{01}^C)(q_{00}^T + q_{01}^T) + (q_{10}^C + q_{11}^C)(q_{10}^T + q_{11}^T) \\ &= (1 - \delta_b^C)(1 - \delta_b^T) + \delta_b^C \delta_b^T, \end{aligned} \quad (\text{A.2})$$

where $\delta_b^C = q_{10}^C + q_{11}^C$ and $\delta_b^T = q_{10}^T + q_{11}^T$ are the bit error rates of the input control and target qubits, respectively. During the parity check, the number of pure EPR pairs (or secret bits) that Alice and Bob need to sacrifice is given by:

$$\frac{1}{2} H_2(p_S), \quad (\text{A.3})$$

where the factor $1/2$ is for the reason that Alice and Bob compute the parity of two-qubit pairs at one time.

After the parity check, the qubits are divided into two groups, qubits with even parity and odd parity. In the following, we will discuss the error correction and privacy amplification on these two groups separately. The recurrence protocol appearing in Ref. [118] only performs error correction on qubits with even parity.

A.2.2 Error correction

For even parity qubits, we can see that the bit error syndrome of control qubits will be the same as that of target qubits. Thus, Alice and Bob only need to do error correction on the control (or target) qubits. Similar to Eq. (6.3), the bit error rate of control qubits after recurrence is given by:

$$\tilde{\delta}_b^C = \frac{(q_{10}^C + q_{11}^C)(q_{10}^T + q_{11}^T)}{p_S} = \frac{\delta_b^C \delta_b^T}{p_S} \quad (\text{A.4})$$

where p_S is the probability of even parity in the recurrence given by Eq. (A.2). Therefore, Alice and Bob need to sacrifice a fraction:

$$\frac{1}{2}p_S H_2(\tilde{\delta}_b^C) = \frac{1}{2}p_S H_2\left(\frac{\delta_b^C \delta_b^T}{p_S}\right) \quad (\text{A.5})$$

to do the overall error correction. The factor $1/2$ is due to the fact that control qubits have the same error syndrome as target qubits.

Therefore, the residue of data post-processing can be expressed as:

$$r = -\frac{1}{2}H_2(p_S) - \frac{1}{2}p_S H_2\left(\frac{\delta_b^C \delta_b^T}{p_S}\right) + K \quad (\text{A.6})$$

where p_S is given in Eq. (A.2), δ_b^C and δ_b^T are the QBER of control and target qubits respectively, and K is the residue of privacy amplification, which we will focus on in the following discussion.

A.2.3 Privacy amplification

Alice and Bob perform privacy amplification to the qubits with even and odd parities separately.

Even parity: Now, Alice and Bob already know the bit error syndrome. The control and target qubits have the same bit error syndromes, but may have different phase error syndromes. Thus, Alice and Bob can divide the even parity qubits into four groups: control qubits with bit error syndrome 0 and 1, and target qubits with bit error syndrome

0 and 1, and treat these groups separately in the privacy amplification step. The probability of each group (summing together the even parity probabilities given in Eq. (A.2)) is given by:

$$\frac{(q_{00}^C + q_{01}^C)(q_{00}^T + q_{01}^T)}{2}, \frac{(q_{10}^C + q_{11}^C)(q_{10}^T + q_{11}^T)}{2}, \frac{(q_{00}^C + q_{01}^C)(q_{00}^T + q_{01}^T)}{2}, \frac{(q_{10}^C + q_{11}^C)(q_{10}^T + q_{11}^T)}{2}$$

with phase error rate:

$$\frac{q_{01}^C}{q_{00}^C + q_{01}^C}, \frac{q_{11}^C}{q_{10}^C + q_{11}^C}, \frac{q_{01}^T}{q_{00}^T + q_{01}^T}, \frac{q_{11}^T}{q_{10}^T + q_{11}^T}.$$

Since the error syndrome of each group of qubits is known to Alice and Bob, privacy amplification can be applied to the different groups separately. Then, Alice and Bob should sacrifice a fraction:

$$\begin{aligned} & \frac{(q_{00}^C + q_{01}^C)(q_{00}^T + q_{01}^T)}{2} H_2\left(\frac{q_{01}^C}{q_{00}^C + q_{01}^C}\right) + \frac{(q_{10}^C + q_{11}^C)(q_{10}^T + q_{11}^T)}{2} H_2\left(\frac{q_{11}^C}{q_{10}^C + q_{11}^C}\right) + \\ & \frac{(q_{00}^C + q_{01}^C)(q_{00}^T + q_{01}^T)}{2} H_2\left(\frac{q_{01}^T}{q_{00}^T + q_{01}^T}\right) + \frac{(q_{10}^C + q_{11}^C)(q_{10}^T + q_{11}^T)}{2} H_2\left(\frac{q_{11}^T}{q_{10}^T + q_{11}^T}\right) \end{aligned} \quad (\text{A.7})$$

to do the privacy amplification. Given the bit and phase error rates of input control and target qubits $\delta_p^C = q_{11}^C + q_{01}^C$ and $\delta_p^T = q_{11}^T + q_{01}^T$, Eq. (A.7) can be written as:

$$\frac{1}{2}(1 - \delta_b^C)(1 - \delta_b^T) \left[H_2\left(\frac{\delta_p^C - q_{11}^C}{1 - \delta_b^C}\right) + H_2\left(\frac{\delta_p^T - q_{11}^T}{1 - \delta_b^T}\right) \right] + \frac{1}{2} \delta_b^C \delta_b^T \left[H_2\left(\frac{q_{11}^C}{\delta_b^C}\right) + H_2\left(\frac{q_{11}^T}{\delta_b^T}\right) \right]. \quad (\text{A.8})$$

Thus, the privacy amplification residue of even parity qubits is given by:

$$K_{\text{even}} = p_S - \frac{1}{2}(1 - \delta_b^C)(1 - \delta_b^T) \left[H_2\left(\frac{\delta_p^C - q_{11}^C}{1 - \delta_b^C}\right) + H_2\left(\frac{\delta_p^T - q_{11}^T}{1 - \delta_b^T}\right) \right] - \frac{1}{2} \delta_b^C \delta_b^T \left[H_2\left(\frac{q_{11}^C}{\delta_b^C}\right) + H_2\left(\frac{q_{11}^T}{\delta_b^T}\right) \right]. \quad (\text{A.9})$$

Odd parity: It turns out that pairs with odd parity during the recurrence can also contribute to the final key [118]. Instead of including them in the error correction, Alice and Bob measure one of the two qubits and hence, they know the bit error syndrome of the remaining qubit. They can then proceed with privacy amplification on these qubits.

Suppose Alice and Bob always choose to measure the target qubits and obtain the error syndrome of the control qubits. Similar to the even parity case, now, Alice and Bob can divide the control qubits with odd parity into two parts in accordance to the bit error syndrome. The probability of each part is given by:

$$\frac{(q_{00}^C + q_{01}^C)(q_{10}^T + q_{11}^T)}{2}, \frac{(q_{10}^C + q_{11}^C)(q_{00}^T + q_{01}^T)}{2},$$

with a phase error rate:

$$\frac{q_{01}^C}{q_{00}^C + q_{01}^C}, \frac{q_{11}^C}{q_{10}^C + q_{11}^C}.$$

With the same argument as Eq. (A.7), the number of qubits that need to be sacrificed to privacy amplification is given by:

$$\begin{aligned} & \frac{(q_{00}^C + q_{01}^C)(q_{10}^T + q_{11}^T)}{2} H_2\left(\frac{q_{01}^C}{q_{00}^C + q_{01}^C}\right) + \frac{(q_{10}^C + q_{11}^C)(q_{00}^T + q_{01}^T)}{2} H_2\left(\frac{q_{11}^C}{q_{10}^C + q_{11}^C}\right) \\ &= \frac{1}{2} \left[(1 - \delta_b^C) \delta_b^T H_2\left(\frac{\delta_p^C - q_{11}^C}{1 - \delta_b^C}\right) + \delta_b^C (1 - \delta_b^T) H_2\left(\frac{q_{11}^C}{\delta_b^C}\right) \right] \end{aligned} \quad (\text{A.10})$$

Hence, the privacy amplification residue of odd parity qubits is given by:

$$K_{\text{odd}} = \frac{1}{2} (1 - \delta_b^C) \delta_b^T \left[1 - H_2\left(\frac{\delta_p^C - q_{11}^C}{1 - \delta_b^C}\right) \right] + \frac{1}{2} \delta_b^C (1 - \delta_b^T) \left[1 - H_2\left(\frac{q_{11}^C}{\delta_b^C}\right) \right] \quad (\text{A.11})$$

Therefore, the privacy amplification residue, K in Eq. (A.6), by adding Eqs. (A.9) and (A.11) and substituting Eq. (A.2), is given by:

$$\begin{aligned} K &= K_{\text{even}} + K_{\text{odd}} \\ &= 1 - \frac{1}{2} (1 - \delta_b^C) \delta_b^T - \frac{1}{2} \delta_b^C (1 - \delta_b^T) - \frac{1}{2} (1 - \delta_b^C) H_2\left(\frac{\delta_p^C - q_{11}^C}{1 - \delta_b^C}\right) - \frac{1}{2} \delta_b^C H_2\left(\frac{q_{11}^C}{\delta_b^C}\right) \\ &\quad - \frac{1}{2} (1 - \delta_b^C) (1 - \delta_b^T) H_2\left(\frac{\delta_p^T - q_{11}^T}{1 - \delta_b^T}\right) - \frac{1}{2} \delta_b^C \delta_b^T H_2\left(\frac{q_{11}^T}{\delta_b^T}\right). \end{aligned} \quad (\text{A.12})$$

Note that there are two free parameters q_{11}^C and q_{11}^T in Eq. (A.12), which should be minimized over to lower-bound the key rate.

A.3 Security against basis dependent source

Here, we derive Eq. (6.8) in Section 6.1.3. Rewriting Eq. (9) of [50] gives:

$$\sqrt{F} \leq \sqrt{(1 - \delta_{bx})(1 - \delta_{pz})} + \sqrt{\delta_{bx} \delta_{pz}}, \quad (\text{A.13})$$

where F is the fidelity between the two states with two bases (X and Z) sent by Alice, δ_{bx} is the QBER of X -basis states from error testing, and δ_{pz} is the phase error rate of the Z -basis states¹. Similarly, we have another inequality between the QBER of Z -basis states δ_{bz} , and the phase error rate of X -basis states δ_{px} :

$$\sqrt{F} \leq \sqrt{(1 - \delta_{bz})(1 - \delta_{px})} + \sqrt{\delta_{bz} \delta_{px}}. \quad (\text{A.14})$$

¹Note that we have used different notations from those in Ref. [50]. By letting $\delta_1 = \delta_{bx}$ and $\delta_{ph} = \delta_{pz}$, and substituting Eq. (3) of [50], we can recover Eq. (9) of [50] from Eq. (A.13).

Adding Eqs. (A.13) and (A.14) gives:

$$\begin{aligned}
\sqrt{F} &\leq \frac{1}{2} \left(\sqrt{(1 - \delta_{bx})(1 - \delta_{pz})} + \sqrt{\delta_{bx}\delta_{pz}} + \sqrt{(1 - \delta_{bz})(1 - \delta_{px})} + \sqrt{\delta_{bz}\delta_{px}} \right) \\
&\leq \sqrt{(1 - (\delta_{bx} + \delta_{bz})/2)(1 - (\delta_{pz} + \delta_{px})/2)} + \sqrt{(\delta_{bx} + \delta_{bz})/2(\delta_{pz} + \delta_{px})/2} \quad (\text{A.15}) \\
&= \sqrt{(1 - \delta_b)(1 - \delta_p)} + \sqrt{\delta_b\delta_p},
\end{aligned}$$

where the second inequality is due to the concavity of the function $\sqrt{(1-x)(1-y)} + \sqrt{xy}$ in $[0, 1] \times [0, 1]$ and we have used the definitions $\delta_b \equiv (\delta_{bx} + \delta_{bz})/2$ and $\delta_p \equiv (\delta_{pz} + \delta_{px})/2$. Here, we assume the number of received qubits with Z basis and X basis is the same.

A.4 Residue for the Decoy+GLLP+Recurrence scheme

We calculate the residues, K_i , in Eq. (6.19) for the five cases: $V \oplus S$, $S \oplus V$, $S \oplus S$, $S \oplus M$, $M \oplus S$. Here, we apply each case, with parameters shown in Table 6.1 into Eq. (A.12) to calculate each K_i .

$V \oplus S$: the probability of this case is $\Omega_{VS} = \Omega_V \Omega$.

$$\begin{aligned}
K_{VS} &= 1 - \frac{1}{4} - \frac{1}{4}H_2(1 - 2q_{11}^V) - \frac{1}{4}H_2(2q_{11}^V) - \frac{1}{4}(1 - e_1)H_2\left(\frac{e_1 - a}{1 - e_1}\right) - \frac{1}{4}e_1H_2\left(\frac{a}{e_1}\right) \\
&\geq \frac{1}{4} - \frac{1}{4}(1 - e_1)H_2\left(\frac{e_1 - a}{1 - e_1}\right) - \frac{1}{4}e_1H_2\left(\frac{a}{e_1}\right)
\end{aligned} \quad (\text{A.16})$$

with equality when $q_{11}^V = 1/4$. This is due to the concavity of function $H_2(\cdot)$.

$S \oplus V$: the probability of this case is $\Omega_{VS} = \Omega_V \Omega$.

$$\begin{aligned}
K_{SV} &\geq 1 - \frac{1}{4} - \frac{1}{2}(1 - e_1)H_2\left(\frac{e_1 - a}{1 - e_1}\right) - \frac{1}{2}e_1H_2\left(\frac{a}{e_1}\right) - \frac{1}{4}(1 - e_1)H_2(1 - 2q_{11}^V) - \frac{1}{4}e_1H_2(2q_{11}^V) \\
&\geq \frac{1}{2} - \frac{1}{2}(1 - e_1)H_2\left(\frac{e_1 - a}{1 - e_1}\right) - \frac{1}{2}e_1H_2\left(\frac{a}{e_1}\right)
\end{aligned} \quad (\text{A.17})$$

with equality when $q_{11}^V = 1/4$.

$S \oplus S$: the probability of this case is $\Omega_{VS} = \Omega^2$.

$$\begin{aligned}
K_{SS} &= 1 - e_1(1 - e_1) - \frac{1}{2}(1 - e_1)H_2\left(\frac{e_1 - a}{1 - e_1}\right) - \frac{1}{2}e_1H_2\left(\frac{a}{e_1}\right) \\
&\quad - \frac{1}{2}(1 - e_1)^2H_2\left(\frac{e_1 - a}{1 - e_1}\right) - \frac{1}{2}e_1^2H_2\left(\frac{a}{e_1}\right).
\end{aligned} \quad (\text{A.18})$$

$S \oplus M$: the probability of this case is $\Omega_{SM} = \Omega\Omega_M$.

$$\begin{aligned}
K_{SM} &= 1 - \frac{1}{2}e_1(1 - e_M) - \frac{1}{2}e_M(1 - e_1) - \frac{1}{2}(1 - e_1)H_2\left(\frac{e_1 - a}{1 - e_1}\right) - \frac{1}{2}e_1H_2\left(\frac{a}{e_1}\right) \\
&\quad - \frac{1}{2}(1 - e_1)(1 - e_M)H_2\left(\frac{1 - 2q_{11}^M}{2 - 2e_M}\right) - \frac{1}{2}e_1e_MH_2\left(\frac{q_{11}^M}{e_M}\right) \\
&\geq \frac{1}{2} - \frac{1}{2}(1 - e_1)H_2\left(\frac{e_1 - a}{1 - e_1}\right) - \frac{1}{2}e_1H_2\left(\frac{a}{e_1}\right),
\end{aligned} \tag{A.19}$$

with equality when $q_{11}^M = e_M/2$.

$M \oplus S$: the probability of this case is $\Omega_{MS} = \Omega_M\Omega$.

$$\begin{aligned}
K_{MS} &= 1 - \frac{1}{2}e_M(1 - e_1) - \frac{1}{2}e_1(1 - e_M) - \frac{1}{2}(1 - e_M)H_2\left(\frac{1 - 2q_{11}^M}{2 - 2e_M}\right) - \frac{1}{2}e_MH_2\left(\frac{q_{11}^M}{e_M}\right) \\
&\quad - \frac{1}{2}(1 - e_1)(1 - e_M)H_2\left(\frac{e_1 - a}{1 - e_1}\right) - \frac{1}{2}e_1e_MH_2\left(\frac{a}{e_1}\right) \\
&\geq \frac{1}{2} - \frac{1}{2}e_M(1 - e_1) - \frac{1}{2}e_1(1 - e_M) \\
&\quad - \frac{1}{2}(1 - e_1)(1 - e_M)H_2\left(\frac{e_1 - a}{1 - e_1}\right) - \frac{1}{2}e_1e_MH_2\left(\frac{a}{e_1}\right),
\end{aligned} \tag{A.20}$$

with equality when $q_{11}^M = e_M/2$.

Therefore, the data post-processing residue of the Decoy+GLLP+Recurrence scheme will be given by substituting Eqs. (A.16), (A.17), (A.18), (A.19) and (A.20) into

Eq. (6.19):

$$\begin{aligned}
r &= -\frac{1}{2}f(p_S)H_2(p_S) - \frac{1}{2}p_S f\left(\frac{\delta^2}{p_S}\right)H_2\left(\frac{\delta^2}{p_S}\right) + K_{VS} + K_{SV} + K_{SS} + K_{SM} + K_{MS} \\
&\geq -\frac{1}{2}f(p_S)H_2(p_S) - \frac{1}{2}p_S f\left(\frac{\delta^2}{p_S}\right)H_2\left(\frac{\delta^2}{p_S}\right) \\
&\quad + \Omega_V \Omega \left[\frac{1}{4} - \frac{1}{4}(1 - e_1)H_2\left(\frac{e_1 - a}{1 - e_1}\right) - \frac{1}{4}e_1 H_2\left(\frac{a}{e_1}\right) \right] \\
&\quad + \Omega_V \Omega \left[\frac{1}{2} - \frac{1}{2}(1 - e_1)H_2\left(\frac{e_1 - a}{1 - e_1}\right) - \frac{1}{2}e_1 H_2\left(\frac{a}{e_1}\right) \right] \\
&\quad + \Omega^2 \left[1 - e_1(1 - e_1) - \frac{1}{2}(1 - e_1)H_2\left(\frac{e_1 - a}{1 - e_1}\right) - \frac{1}{2}e_1 H_2\left(\frac{a}{e_1}\right) \right. \\
&\quad \left. - \frac{1}{2}(1 - e_1)^2 H_2\left(\frac{e_1 - a}{1 - e_1}\right) - \frac{1}{2}e_1^2 H_2\left(\frac{a}{e_1}\right) \right] \\
&\quad + \Omega \Omega_M \left[\frac{1}{2} - \frac{1}{2}(1 - e_1)H_2\left(\frac{e_1 - a}{1 - e_1}\right) - \frac{1}{2}e_1 H_2\left(\frac{a}{e_1}\right) \right] \\
&\quad + \Omega \Omega_M \left[\frac{1}{2} - \frac{1}{2}e_M(1 - e_1) - \frac{1}{2}e_1(1 - e_M) \right. \\
&\quad \left. - \frac{1}{2}(1 - e_1)(1 - e_M)H_2\left(\frac{e_1 - a}{1 - e_1}\right) - \frac{1}{2}e_1 e_M H_2\left(\frac{a}{e_1}\right) \right]
\end{aligned} \tag{A.21}$$

with equality when $q_{11}^V = 1/4$ and $q_{11}^M = e_M/2$. In order to simplify this formula, we define some variables:

$$\begin{aligned}
B &= \frac{1}{2}f(p_S)H_2(p_S) + \frac{1}{2}p_S f\left(\frac{\delta^2}{p_S}\right)H_2\left(\frac{\delta^2}{p_S}\right) \\
C &= \frac{3}{4}\Omega_V \Omega + \Omega^2(1 - e_1 + e_1^2) + \frac{1}{2}\Omega \Omega_M(2 - e_1 - e_M + 2e_1 e_M) \\
D_1 &= \frac{3}{4}\Omega_V \Omega + \frac{1}{2}\Omega^2(2 - e_1) + \frac{1}{2}\Omega \Omega_M(2 - e_M) \\
D_2 &= \frac{3}{4}\Omega_V \Omega + \frac{1}{2}\Omega^2(1 + e_1) + \frac{1}{2}\Omega \Omega_M(e_M + 1)
\end{aligned} \tag{A.22}$$

Thus, Eq. (6.20) can be expressed as:

$$\begin{aligned}
r &= -B + K_{VS} + K_{SV} + K_{SS} + K_{SM} + K_{MS} \\
&\geq -B + C - F_a
\end{aligned} \tag{A.23}$$

where

$$F_a = D_1(1 - e_1)H_2\left(\frac{e_1 - a}{1 - e_1}\right) + D_2 e_1 H_2\left(\frac{a}{e_1}\right) \tag{A.24}$$

with equality when $q_{11}^V = 1/4$ and $q_{11}^M = e_M/2$.

To obtain the lower bound r in Eq. (A.23), we need to find the maximum value of F_a over the free variable a . We are interested in the range of $a \in [0, e_1]$ with $e_1 \leq 1/2$.

Note that F_a is a concave function of a in the valid range, since a sum of two concave functions is also a concave function, and reflecting and shifting a concave function is also a concave function. Thus, we can take the derivative of F_a with respect to a and set it to zero to find the maximum of F_a . Differentiating F_a with respect to a gives:

$$\frac{dF_a}{da} = D_1 \left[\log_2 \left(\frac{e_1 - a}{1 - e_1} \right) - \log_2 \left(1 - \frac{e_1 - a}{1 - e_1} \right) \right] + D_2 \left[\log_2 \left(1 - \frac{a}{e_1} \right) - \log_2 \left(\frac{a}{e_1} \right) \right]$$

Setting $2 \frac{dF_a}{da} = 1$ gives

$$\left(\frac{1 - e_1}{e_1 - a} - 1 \right)^{-D_1} \left(\frac{e_1}{a} - 1 \right)^{D_2} = 1.$$

Denoting the left-hand side to be $f(a)$, $f(a)$ is a decreasing function of a since $\frac{dF_a}{da}$ is a decreasing function of a . Therefore, we can use the bisection method to find a such that $f(a) = 1$. The initial range for the bisection method is $[0, e_1]$.

A.5 QBER for entanglement PDC QKD

Here, we will study the quantum bit error rate (QBER) of the entanglement PDC QKD. Our objective is to derive the QBER formula given in Eq. (8.9) used in the simulation. The QBER has three main contributions:

1. background counts, which are random noises $e_0 = 1/2$;
2. intrinsic detector errors, e_d , which is the probability that a photon hits the erroneous detector. e_d characterizes the alignment and stability of the optical system between the detection systems of Alice and Bob;
3. errors introduced by multi-photon-pair states: a) Alice and Bob may detect different photon pairs; b) double clicks. Due to the strong pulsing attack [69], we assume that Alice and Bob will assign a random bit when they get a double click. In either case, the error rate will be $e_0 = 1/2$.

Let us start with the single-photon-pair case, a Bell state given in Eq. (8.4). The error rate of single-photon-pair e_1 has two sources: background counts and intrinsic detector errors:

$$e_1 = e_0 - \frac{(e_0 - e_d)\eta_A\eta_B}{Y_1} \tag{A.25}$$

If we neglect the case where both background and true signal cause clicks, then e_1 can be written as:

$$e_1 \approx \frac{e_0(Y_{0A}Y_{0B} + Y_{0A}\eta_B + \eta_A Y_{0B}) + e_d\eta_A\eta_B}{Y_1}. \quad (\text{A.26})$$

where $e_0 = 1/2$ is the error rate of background counts. The first term of the numerator is the background contribution and the second term comes from the errors of true signals.

In the following, we will discuss the errors introduced by multi-photon pair states, e_n with $n \geq 2$. Here, we assume that Alice and Bob use threshold detectors. One can imagine the detection of an n -photon-pair state as follows.

1. Alice and Bob project the n -photon-pair state, Eq. (8.3), into $Z^{\otimes n}$ basis.
2. Afterwards, they detect each photon with certain probabilities (η_A for Alice and η_B for Bob).
3. If either Alice or Bob detects vacuum, then we regard it as a *loss*. If Alice and Bob both detect non-vacuum only in one polarization (\leftrightarrow or \uparrow), we regard it as a *single click* event. Otherwise, we regard it as a *double click* event.

The state of a 2-photon-pair state, according to Eq. (8.3), can be written as:

$$\begin{aligned} |\Phi_2\rangle &= \frac{1}{\sqrt{3}}(|2, 0\rangle_a |0, 2\rangle_b - |1, 1\rangle_a |1, 1\rangle_b + |0, 2\rangle_a |2, 0\rangle_b) \\ &= \frac{1}{\sqrt{3}}[| \leftrightarrow \leftrightarrow \rangle_a | \uparrow \uparrow \rangle_b - \frac{1}{2}(| \leftrightarrow \uparrow \rangle + | \uparrow \leftrightarrow \rangle)_a \otimes (| \uparrow \leftrightarrow \rangle + | \leftrightarrow \uparrow \rangle)_b + | \uparrow \uparrow \rangle_a | \leftrightarrow \leftrightarrow \rangle_b]. \end{aligned} \quad (\text{A.27})$$

As discussed above, Alice and Bob project the state into $Z \otimes Z$ basis. If they end up with the first or the third state in the bracket of Eq. (A.27), they will get perfect anti-correlation, which will not contribute to errors. If they get the second state in the bracket of Eq. (A.27), their results are totally independent, which will cause an error with a probability $e_0 = 1/2$. Thus, the error probability introduced by a 2-photon-pair state is $1/6$. Here, we have only considered the errors introduced by multi photon states, which is item 3 discussed in the beginning of this Appendix. We should also take into account the effects of background counts and intrinsic detector errors. With these modifications, the error rate of 2-photon-pair state is given by:

$$e_2 = e_0 - \frac{2(e_0 - e_d)[1 - (1 - \eta_A)^2][1 - (1 - \eta_B)^2]}{3Y_2} \quad (\text{A.28})$$

where Y_2 is given in Eq. (8.6). Eq. (A.28) can be understood as follows. Only when Alice and Bob project Eq. (A.27) into $| \leftrightarrow \leftrightarrow \rangle_a | \uparrow \uparrow \rangle_b$ or $| \uparrow \uparrow \rangle_a | \leftrightarrow \leftrightarrow \rangle_b$ and no background

count occurs, they have a probability of e_d to get the wrong answer. Given a coincident detection, the conditional probability for this case is $2[1 - (1 - \eta_A)^2][1 - (1 - \eta_B)^2]/3Y_2$. All other cases, a background count, a double click and measuring different photon pairs, will contribute to an error probability $e_0 = 1/2$.

Next, let us study the errors coming from the state $|n - m, m\rangle_a |m, n - m\rangle_b$. When Alice detects at least one of $n - m$ $|\uparrow\rangle$ photons, but none of m $|\leftrightarrow\rangle$ photons, and Bob detects at least one of $n - m$ $|\leftrightarrow\rangle$ photons, but none of m $|\uparrow\rangle$ photons, or both Alice and Bob have bit flips of this case, they will end up with an error probability of e_d . Given a coincident detection, the conditional probability for these two cases is:

$$\frac{1}{Y_n} \{ [1 - (1 - \eta_A)^{n-m}] (1 - \eta_A)^m [1 - (1 - \eta_B)^{n-m}] (1 - \eta_B)^m \\ + [1 - (1 - \eta_A)^m] (1 - \eta_A)^{n-m} [1 - (1 - \eta_B)^m] (1 - \eta_B)^{n-m} \}.$$

When Alice detects at least one of $n - m$ $|\uparrow\rangle$ polarizations, but none of m $|\leftrightarrow\rangle$ polarizations, and Bob detects at least one of m $|\uparrow\rangle$ polarizations, but none of $n - m$ $|\leftrightarrow\rangle$ polarizations, or both Alice and Bob have bit flips of this case, they will end up with an error probability of $1 - e_d$. Given a coincident detection, the conditional probability for these two cases is:

$$\frac{1}{Y_n} \{ [1 - (1 - \eta_A)^m] (1 - \eta_A)^{n-m} [1 - (1 - \eta_B)^{n-m}] (1 - \eta_B)^m \\ + [1 - (1 - \eta_A)^{n-m}] (1 - \eta_A)^m [1 - (1 - \eta_B)^m] (1 - \eta_B)^{n-m} \}.$$

For all other cases, the error probability is e_0 . Thus, the error probability for the state $|n - m, m\rangle_a |m, n - m\rangle_b$ is:

$$\begin{aligned} e_{nm} &= e_0 - \frac{e_0 - e_d}{Y_n} \{ (1 - \eta_A)^{n-m} (1 - \eta_B)^{n-m} [1 - (1 - \eta_A)^m] [1 - (1 - \eta_B)^m] \\ &\quad + (1 - \eta_A)^m (1 - \eta_B)^m [1 - (1 - \eta_A)^{n-m}] [1 - (1 - \eta_B)^{n-m}] \\ &\quad - (1 - \eta_A)^{n-m} (1 - \eta_B)^m [1 - (1 - \eta_A)^m] [1 - (1 - \eta_B)^{n-m}] \\ &\quad - (1 - \eta_A)^m (1 - \eta_B)^{n-m} [1 - (1 - \eta_A)^{n-m}] [1 - (1 - \eta_B)^m] \} \\ &= e_0 - \frac{e_0 - e_d}{Y_n} [(1 - \eta_A)^{n-m} - (1 - \eta_A)^m] [(1 - \eta_B)^{n-m} - (1 - \eta_B)^m] \end{aligned} \quad (\text{A.29})$$

In general, for an n -photon-pair state described by Eq. (8.3), the error rate is given by:

$$\begin{aligned}
e_n &= \frac{1}{n+1} \sum_{m=0}^n e_{nm} \\
&= \frac{1}{n+1} \sum_{m=0}^n e_0 - \frac{e_0 - e_d}{Y_n} [(1 - \eta_A)^{n-m} - (1 - \eta_A)^m] [(1 - \eta_B)^{n-m} - (1 - \eta_B)^m] \\
&= e_0 - \frac{e_0 - e_d}{(n+1)Y_n} \sum_{m=0}^n [(1 - \eta_A)^{n-m} - (1 - \eta_A)^m] [(1 - \eta_B)^{n-m} - (1 - \eta_B)^m] \\
&= e_0 - \frac{2(e_0 - e_d)}{(n+1)Y_n} \left[\frac{1 - (1 - \eta_A)^{n+1}(1 - \eta_B)^{n+1}}{1 - (1 - \eta_A)(1 - \eta_B)} - \frac{(1 - \eta_A)^{n+1} - (1 - \eta_B)^{n+1}}{\eta_B - \eta_A} \right]
\end{aligned} \tag{A.30}$$

The overall QBER is given by:

$$\begin{aligned}
E_\lambda Q_\lambda &= \sum_{n=0}^{\infty} e_n Y_n P(n) \\
&= e_0 Q_\lambda - \sum_{n=0}^{\infty} \frac{2(e_0 - e_d) \lambda^n}{(1 + \lambda)^{n+2}} \left[\frac{1 - (1 - \eta_A)^{n+1}(1 - \eta_B)^{n+1}}{1 - (1 - \eta_A)(1 - \eta_B)} - \frac{(1 - \eta_A)^{n+1} - (1 - \eta_B)^{n+1}}{\eta_B - \eta_A} \right] \\
&= e_0 Q_\lambda - \frac{2(e_0 - e_d) \eta_A \eta_B \lambda (1 + \lambda)}{(1 + \eta_A \lambda)(1 + \eta_B \lambda)(1 + \eta_A \lambda + \eta_B \lambda - \eta_A \eta_B \lambda)}
\end{aligned} \tag{A.31}$$

where Q_λ is the gain given in Eq. (8.8).

Appendix B

Optimal μ

In this appendix, we will discuss the optimal expected photon number μ for various protocols.

B.1 Coherent state QKD

Here, we will discuss the optimal choice of the expected photon number μ of the coherent state QKD with and without decoy states.

Let us start with a generic discussion. On the one hand, we need to maximize the probability of a single photon detection, which is the only source of the final secure key (for BB84). To achieve this point, we should maximize the single photon sources. Considering a weak coherent state photon sources in accordance to the Poisson distribution of the photon number as shown in Eq. (3.3), the single photon source reaches its maximum when $\mu = 1$. On the other hand, we have to control the probability of the multi photon detection to ensure the security of the system. Thus, we should keep the untagged states (single photon states) ratio large, which requires μ to be not too large. Therefore, intuitively we have:

$$\mu \in (0, 1].$$

B.1.1 Without decoy states

Here, we will consider the case of the coherent state QKD without decoy states, following the discussion in Ref. [70]. Assume that Alice and Bob apply the GLLP security analysis as discussed in Section 2.5. We desire to get an optimal value of μ that maximizes the key generation rate R in Eq. (2.6) with other parameters fixed. The key parameters here

are the overall transmittance η given in Eq. (3.4), background rate Y_0 , and the intrinsic detection error rate e_d .

Let us make an approximation first: if the background contribution is negligible, that is, $Y_0 \ll \eta$, then from Eqs. (3.11):

$$\begin{aligned} Q_\mu &\cong 1 - e^{-\eta\mu} \\ E_\mu &\cong e_d \end{aligned} \tag{B.1}$$

Then according to Eq. (4.1), the estimation of Q_1 and e_1 is:

$$\begin{aligned} Q_1 &\geq Q_\mu - \sum_{i=2}^{\infty} \frac{\mu^i}{i!} e^{-\mu} \\ &\cong (1 + \mu)e^{-\mu} - e^{-\eta\mu} \\ e_1 &\leq \frac{e_d(1 - e^{-\eta\mu})}{(1 + \mu)e^{-\mu} - e^{-\eta\mu}} \end{aligned} \tag{B.2}$$

Then we can substitute these approximations into the key rate formula Eq. (2.6) and take the derivative of μ to get the optimal μ .

$$\begin{aligned} R &\leq \frac{1}{2}(Q_\mu - p_M) \\ &= \frac{1}{2}[(1 + \mu) \exp(-\mu) - \exp(-\eta\mu)] \end{aligned}$$

with the pessimistic assumption Eq. (4.1). This expression is optimized if we choose $\mu = \mu_{Optimal}$, which fulfills:

$$-\mu \exp(-\mu) + \eta \exp(-\eta\mu) = 0.$$

Since for a realistic setup, we expect that $\eta\mu \ll 1$, we find:

$$\eta_{Optimal} \approx \eta. \tag{B.3}$$

We use the numerical analysis to verify Eq. (B.3). When we keep all parameters fixed and vary the expected photon number μ of the signal, we can determine the $\mu_{Optimal}$ to maximize the key generation rate by Eq. (2.6). If we fix the background rate Y_0 and the probability of erroneous detection e_d , and vary the transmittance η , we can draw the relationship between the optimal $\mu_{Optimal}$ and η . The result is shown in Figure B.1, from which we can see that Eq. (B.3) is a good approximation.

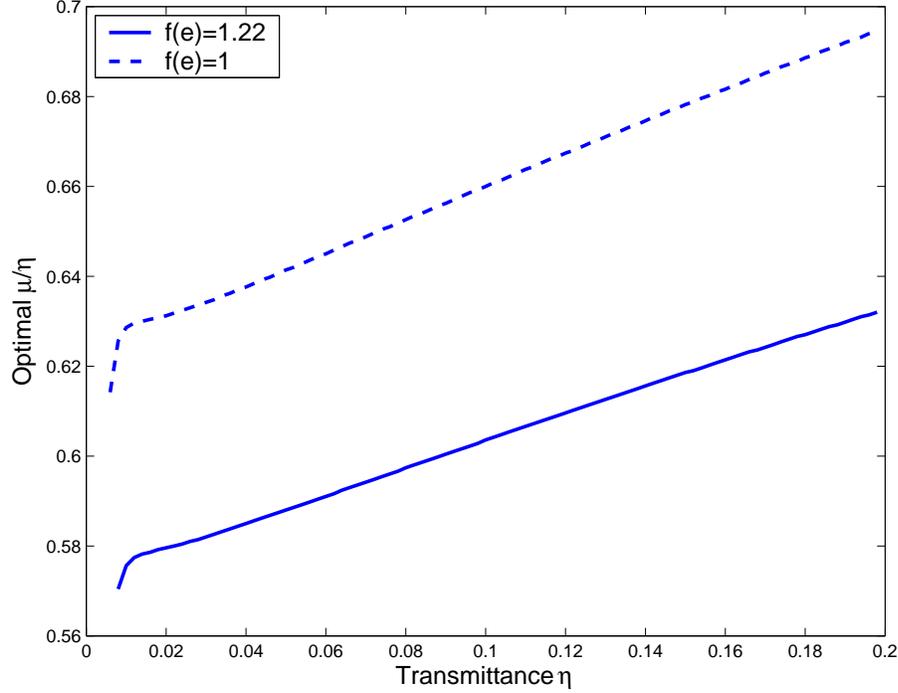


Figure B.1: Plot of the optimal expected photon number μ as a function of transmittance η for the coherent state QKD+non decoy. The parameters used in the simulation are listed in Table 3.1. Here, we numerically calculate the optimal μ that maximizes the key generation rate by Eqs. (2.6) and (4.1). In the regime around $\eta \approx 0$, the key rate is 0. Thus, there is no point to talk about optimal μ in that regime.

B.1.2 With decoy state

In principle, Alice and Bob can estimate Q_1 and e_1 accurately with the decoy state. Hence, $\mu_{Optimal}$ should maximize the untagged states ratio $\Omega = Q_1/Q_\mu$. Thus, we can expect that $\mu_{Optimal}$ should be greater than (B.3).

Let us start with a numerical analysis on Eq. (2.6) directly. For each distance, we determine the optimal μ that maximizes the key generation rate. The result is shown in Figure B.2. We can see that the optimal μ for GYS is around 0.48 when $f(\delta) = 1.22$.

Now, we would like to do an analytical discussion under some approximations. We take the approximations $Y_0 \ll \eta \ll 1$. Then Eqs. (3.7), (3.9), (3.8) and (3.10) are reduced

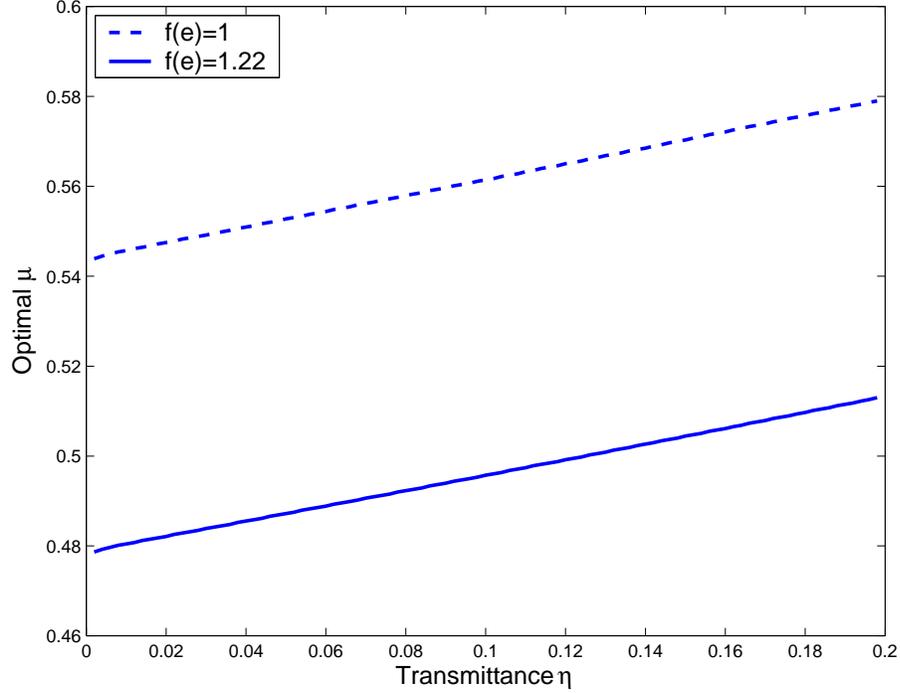


Figure B.2: Plot of the optimal expected photon number μ as a function of transmittance η for the coherent state QKD+infinite decoy. The parameters used in the simulation are listed in Table 3.1.

to:

$$Q_1 \cong \eta\mu e^{-\mu}$$

$$e_1 \cong e_d$$

$$Q_\mu \cong \eta\mu$$

$$E_\mu \cong e_d$$

Substituting these formulas into Eq. (2.6), the key generation rate is given by:

$$R \approx \frac{1}{2} \{-\eta\mu f(e_d) H_2(e_d) + \eta\mu e^{-\mu} [1 - H_2(e_d)]\}$$

The expression is optimized if we choose $\mu = \mu_{Optimal}$ which fulfills:

$$(1 - \mu) \exp(-\mu) = \frac{f(e_d) H_2(e_d)}{1 - H_2(e_d)}. \quad (\text{B.4})$$

Then we can solve this equation and obtain, by using $f(\delta) = 1.22$:

$$\mu_{Optimal}^{GYS} \approx 0.48$$

where for the GYS experiment, $e_d = 3.3\%$, as listed in Table 3.1. In comparison of this result to Figure B.2, we can see that Eq. (B.4) is a good approximation.

B.2 Triggering PDC QKD

Here, instead of numerically optimizing μ as implemented for Figure (7.2), we qualitatively investigate the optimal μ for the triggering PDC QKD with and without decoy states. We are interested in the case where Alice uses a threshold detector.

B.2.1 Without decoy states

Let us begin with the optimal μ of the case without decoy states. Here, we will apply the GLLP [35] security analysis. As shown in Ref. [73], GLLP and Lütkenhaus's [70] security analyses achieve similar performances for the coherent state QKD. Intuitively, we should get a similar optimal μ as given in Ref. [70], $\mu \approx \eta/2$.

From Eq. (7.8), we can see that the gain $Q_{\mu,j}$ ($j = 0, 1$) is in the order of $\mu\eta$. To keep $Q_{1,0}$ or $Q_{1,1}$ in Eq. (7.14) positive, μ should be in the order of η . By assuming μ , η and Y_{0B} are small, we can simplify Eq. (7.8):

$$\begin{aligned}
 Q_{\mu,0} + Q_{\mu,1} &\approx \eta\mu \\
 E_{\mu,0} &\approx E_{\mu,1} \approx e_d \\
 Q_{1,0}^L + Q_{1,1}^L &\approx \eta\mu - \mu^2 \\
 e_1^U &\approx \frac{\eta e_d}{\eta - \mu}
 \end{aligned} \tag{B.5}$$

where $Q_{1,0}^L + Q_{1,1}^L$ is the lower bound of $Q_{1,0} + Q_{1,1}$ and e_1^U is the upper bound of e_1 from Eq. (7.14). Since the error rates from triggered ($j = 1$) and non-triggered ($j = 0$) detection events are the same, the key generation rate given by Eq. (7.19) can be simplified to:

$$\begin{aligned}
 R &\geq q\{-f(E_\mu)Q_\mu H_2(E_\mu) + Q_1[1 - H_2(e_1)] + Q_0\} \\
 &\approx q\{-f(e_d)\eta\mu H_2(e_d) + (\eta\mu - \mu^2)[1 - H_2(\frac{\eta e_d}{\eta - \mu})]\}
 \end{aligned} \tag{B.6}$$

By taking the derivative of R , the optimal $\mu \equiv x\eta$ satisfies:

$$-f(e_d)H_2(e_d) + 1 - 2x + e_d \log_2 \frac{e_d}{1-x} + (1 - e_d - 2x) \log_2(1 - \frac{e_d}{1-x}) = 0. \tag{B.7}$$

Here if set $e_d = 0$, then we get $x = 1/2$, which is compatible with Lütkenhaus' result [70]. Note that $x = 1/2$ essentially maximizes the probability of the single photon source $Q_{1,0}^L + Q_{1,1}^L$ in Eq. (B.5). More precisely, we can solve Eq. (B.7) numerically, see Figure B.3.

From Figure B.3, we can see that the optimal μ for triggering PDC+non-decoy is $\mu = O(\eta)$, which will lead the final key generation rate $R = O(\eta^2)$.

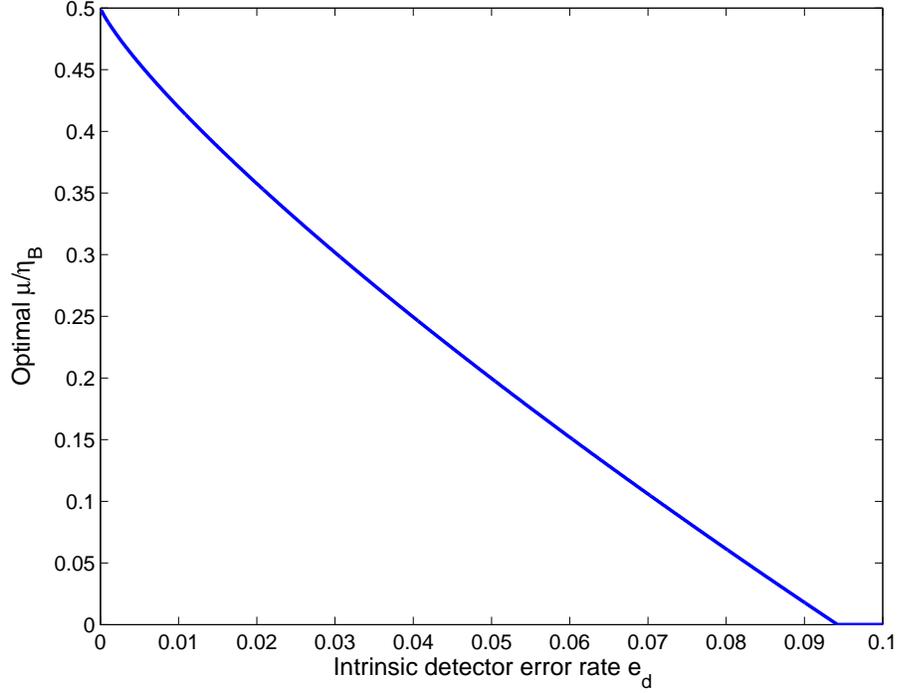


Figure B.3: Plot of the optimal μ in terms of e_d for triggering PDC+non-decoy. Here, we use $f(e_d) = 1.22$.

B.2.2 With decoy states

With decoy states, Alice and Bob can estimate Q_1 and e_1 better. Here, we consider the infinite decoy state case with threshold detectors. Under the assumption that η and Y_{0B} are small, we can simplify Eqs. (7.8) and (7.9):

$$\begin{aligned}
 Q_{\mu,0} + Q_{\mu,1} &\approx \eta\mu \\
 E_{\mu,0} &\approx E_{\mu,1} \approx e_d \\
 Q_{1,0} + Q_{1,1} &\approx \frac{\eta\mu}{(1+\mu)^2} \\
 e_1 &\approx e_d
 \end{aligned} \tag{B.8}$$

With these approximations, the key generation rate given in Eq. (7.19) can be simplified to:

$$R \approx q \left\{ -f(e_d)\eta\mu H_2(e_d) + \frac{\eta\mu}{(1+\mu)^2} [1 - H_2(e_d)] \right\}. \tag{B.9}$$

The optimal μ satisfies:

$$\frac{1-\mu}{(1+\mu)^3} = \frac{f(e_d)H_2(e_d)}{1-H_2(e_d)} \tag{B.10}$$

Here, if set $e_d = 0$, then we get $\mu = 1$ with which the probability to getting a single photon state is maximized. The numerical result of Eq. (B.10) is shown in Figure B.4.

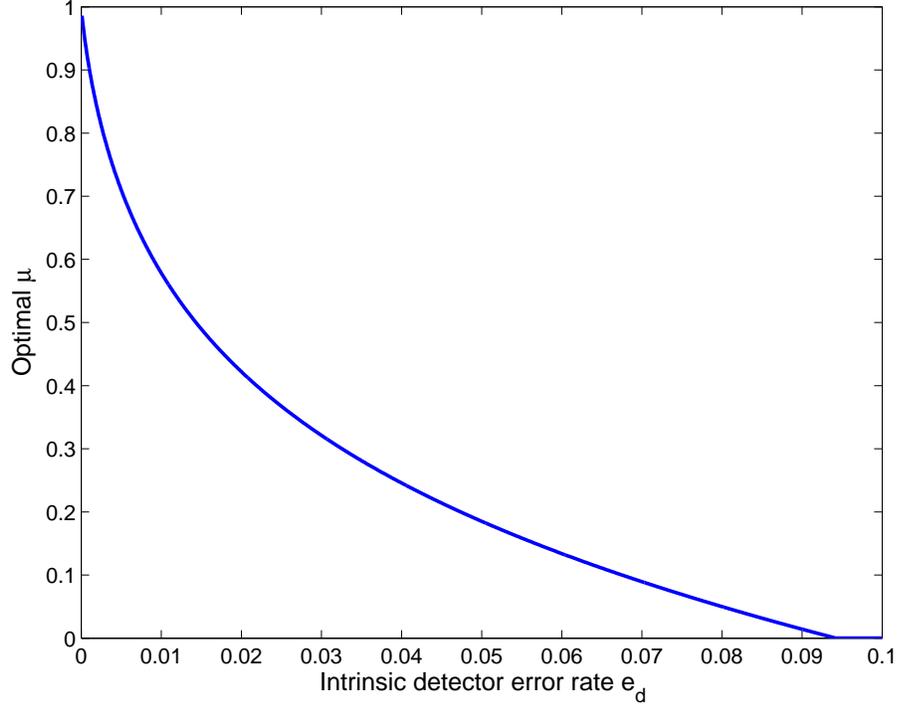


Figure B.4: Plot of the optimal μ in terms of e_d for the triggering PDC+infinite decoy. Here, we use $f(e_d) = 1.22$.

From Figure B.4, which is similar to the case coherent state QKD with decoy states [77], one can see that the optimal μ is independent of channel loss η for the infinite decoy state case with threshold detectors, i.e., $\mu = O(1)$, which will lead the final key generation rate $R = O(\eta)$.

B.2.3 Numerical checking

Now we would like to numerically compare the optimal μ with and without decoy states by simulating a recent PDC experiment [115], with parameters listed in Table 7.1. In the simulation, we numerically optimize μ for the key rate given by Eq. (7.13) for the non-decoy and infinite decoy methods. For this particular setup, the optimal μ is shown in Figure B.5.

From the figure, we can see that the optimal μ for the non-decoy case is in the order of η , while the optimal μ for the infinite-decoy case is in the order of 1. This is consistent with the results of the analysis in the two previous subsections.

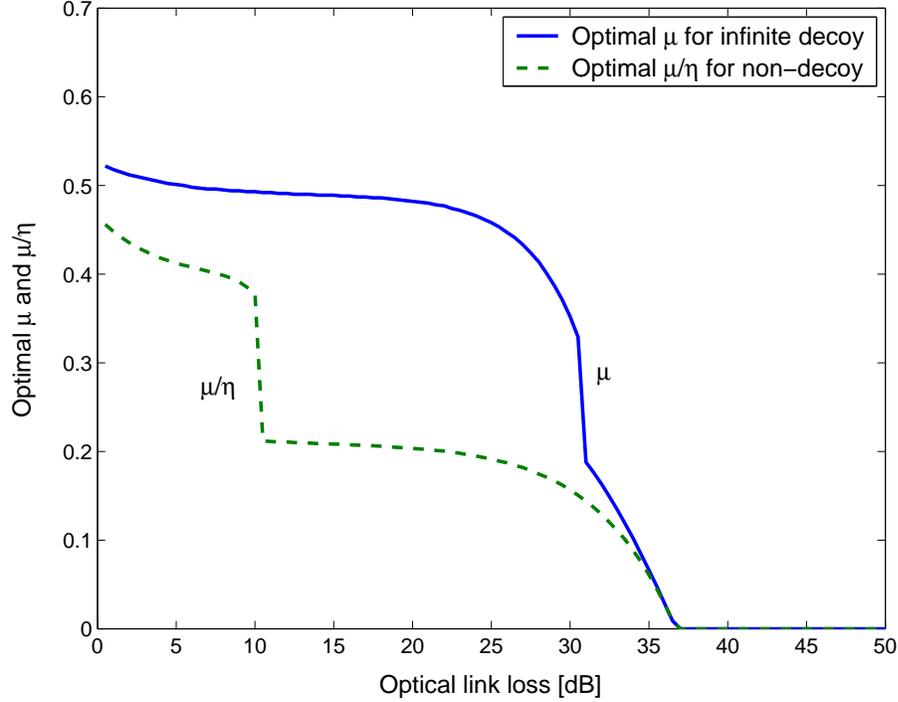


Figure B.5: Plot of the optimal μ in terms of optical loss for triggering PDC+non-decoy and triggering PDC+infinite-decoy. Here, we use $q = 1/2$ and $f(E_\mu) = 1.22$. Simulation parameters are listed in Table 7.1.

B.3 Entanglement PDC QKD

The optimal μ for the coherent state QKD has already been discussed [70, 77]. Here, we need to determine the optimal μ for the entanglement PDC QKD. In the following calculation, we will focus on optimizing the parameter λ ($= \mu/2$) for the key generation rate given in Eq. (8.10).

By assuming η_B to be small and neglecting Y_0 , we can simplify Eq. (8.8):

$$Q_\lambda \approx 2\eta_B\lambda\left[1 - \frac{1 - \eta_A}{(1 + \eta_A\lambda)^3}\right]. \quad (\text{B.11})$$

The overall QBER given in Eq. (8.9) can be simplified to:

$$E_\lambda \approx \frac{1}{2} - \frac{(1 - 2e_d)(1 + \lambda)(1 + \eta_A\lambda)}{2(1 + 3\lambda + 3\eta_A\lambda^2 + \eta_A^2\lambda^3)}. \quad (\text{B.12})$$

In order to maximize the key generation rate given by Eq. (8.10), the optimal λ satisfies:

$$\frac{\partial Q_\lambda}{\partial \lambda} [1 - (1 + f(E_\lambda))H_2(E_\lambda)] - Q_\lambda [1 + f(E_\lambda)] \frac{\partial E_\lambda}{\partial \lambda} \log_2 \frac{1 - E_\lambda}{E_\lambda} = 0. \quad (\text{B.13})$$

Here, we treat $f(E_\lambda)$ as a constant. In the following, we will consider two extremes: $\eta_A \approx 1$ and $\eta_A \ll 1$.

When $\eta_A \approx 1$, the overall gain and QBER are given by:

$$\begin{aligned} Q_\lambda &\approx 2\eta_B\lambda \\ E_\lambda &\approx \frac{2e_d + \lambda}{2 + 2\lambda}. \end{aligned} \quad (\text{B.14})$$

Thus, Eq. (B.13) can be simplified to:

$$1 - [1 + f(E_\lambda)]H_2(E_\lambda) - \lambda[1 + f(E_\lambda)]\frac{1 - 2e_d}{2(1 + \lambda)^2} \log_2 \frac{1 - E_\lambda}{E_\lambda} = 0. \quad (\text{B.15})$$

When $\eta_A \ll 1$,

$$\begin{aligned} Q_\lambda &\approx 2\eta_A\eta_B\lambda(1 + 3\lambda) \\ E_\lambda &\approx \frac{e_d + \lambda + e_d\lambda}{1 + 3\lambda}. \end{aligned} \quad (\text{B.16})$$

Thus, Eq. (B.13) can be simplified to:

$$(1 + 6\lambda)\{1 - [1 + f(E_\lambda)]H_2(E_\lambda)\} - \lambda[1 + f(E_\lambda)]\frac{1 - 2e_d}{1 + 3\lambda} \log_2 \frac{1 - E_\lambda}{E_\lambda} = 0. \quad (\text{B.17})$$

The solutions to Eqs. (B.15) and (B.17) are shown in Figure B.6.

From Figure B.6, we can see that the optimal $\mu = 2\lambda$ for the entanglement PDC is in the order of 1, $\mu = 2\lambda = O(1)$, which will lead the final key generation rate to be $R = O(\eta_A\eta_B)$.

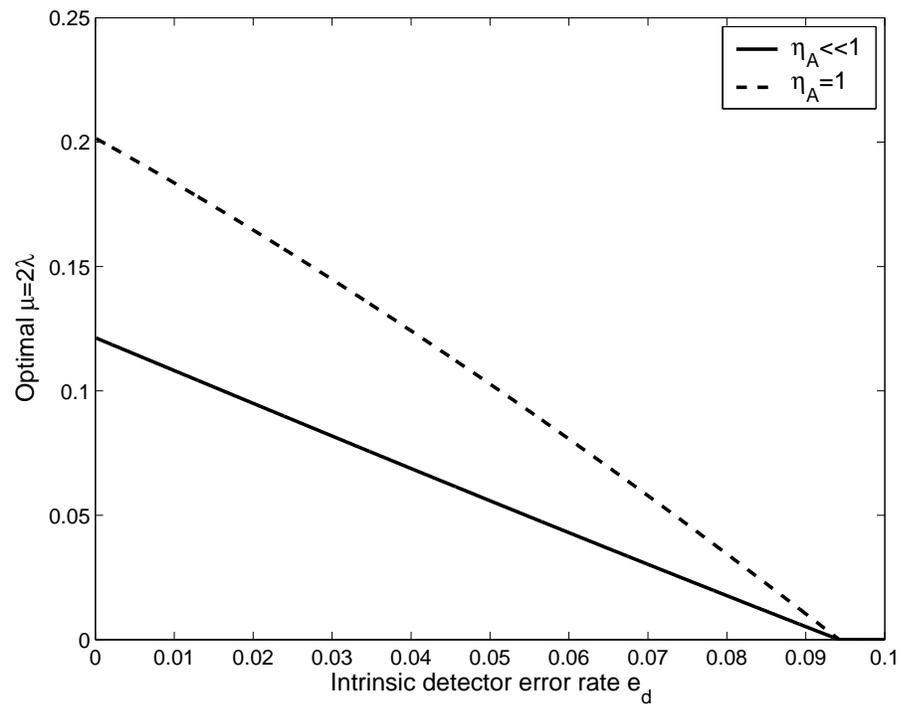


Figure B.6: Plot of the optimal μ in terms of e_d for the entanglement PDC QKD. $f(e_d) = 1.22$.

Bibliography

- [1] A. Acín, N. Gisin, and L. Masanes. From bell's theorem to secure quantum key distribution. *Phys. Rev. Lett.*, 97:120405, 2006.
- [2] Y. Adachi, T. Yamamoto, M. Koashi, and N. Imoto. Simple and efficient quantum key distribution with parametric down-conversion. *Phys. Rev. Lett.* , 99:180503, 2007.
- [3] G. Alber, A. Delgado, N. Gisin, and I. Jex. Efficient bipartite quantum state purification in arbitrary dimensional hilbert spaces. *J. Phys. A: Math. Gen.*, 34:8821, 2001.
- [4] N. Antonietti, M. Mondin, G. Brida, and M. Genovese. On the numerical characterization of atmospheric effects on an earth-space quantum communication channel. *arXiv:quant-ph/0609049*, 2006.
- [5] A. Aspect, P. Grangier, and G. Roger. Experimental tests of realistic local theories via bell's theorem. *Phys. Rev. Lett.*, 47:460, 1981.
- [6] M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. R. Leeb, and A. Zeilinger. Long-distance quantum communication with entangled photons using satellites. *IEEE Journal of Selected Topics in Quantum Electronics, special issue on Quantum Internet Technologies*, 9:1541–1551, 2003.
- [7] N. J. Beaudry, T. Moroder, and N. Lütkenhaus. Squashing models for optical measurements in quantum communication. *arXiv:0804.3082*, 2008.
- [8] J. S. Bell. On the einstein-podolsky-rosen paradox. *Physics*, 1:195, 1964.
- [9] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* , 68:3121, 1992.

- [10] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. A. Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5(1):3–28, 1992.
- [11] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179, Bangalore, India, 1984. IEEE, New York.
- [12] C. H. Bennett, G. Brassard, and N. D. Mermin. Quantum cryptography without bells theorem. *Phys. Rev. Lett.*, 68:557, 1992.
- [13] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed state entanglement and quantum error correction. *Phys. Rev. A*, 54:3824, 1996.
- [14] M. Bourennane, F. Gibson, A. Karlsson, A. Hening, P. Jonsson, T. Tsegaye, D. Ljunggren, and E. Sundberg. Experiments on long wavelength (1550nm) "plug and play" quantum cryptography systems. *Optical Express*, 4(10):383–387, May 1999.
- [15] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders. Security aspects of practical quantum cryptography. *Phys. Rev. Lett.* , 85:1330, 2000.
- [16] G. Brassard and L. Salvail. Secret-key reconciliation by public discussion. In G. Goos and J. Hartmanis, editors, *Advances in Cryptology EUROCRYPT '93*. Springer-Verlag, Berlin, 1993.
- [17] D. Bruss. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.* , 81:3018, 1998.
- [18] A. R. Calderbank and P. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098, 1996.
- [19] J. F. Clauser and M. A. Horne. Experimental consequences of objective local theories. *Phys. Rev. D*, 10:526, 1974.
- [20] M. Curty, M. Lewenstein, and N. Lütkenhaus. Entanglement as precondition for secure quantum key distribution. *Phys. Rev. Lett.* , 92:217903, 2004.
- [21] J. Dehaene, M. V. den Nest, B. D. Moor, and F. Verstraete. Local permutations of products of bell states and entanglement distillation. *Phys. Rev. A*, 67:022310, 2003.

- [22] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera. Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Phys. Rev. Lett.*, 77:2818, 1996. Erratum *Phys. Rev. Lett.* **80**, 2022 (1998).
- [23] M. D. Eisaman, A. André, F. Massou, M. Fleischhauer, A. S. Zibrov, and M. D. Lukin. Electromagnetically induced transparency with tunable single-photon pulses. *Nature*, 438:837, 2005.
- [24] A. K. Ekert. Quantum cryptography based on bell’s theorem. *Phys. Rev. Lett.* , 67:661, 1991.
- [25] 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.
- [26] M. Ferrero, T. W. Marshall, and E. Santos. Bell’s theorem: Local realism versus quantum mechanics. *Am. J. Phys.*, 58:683, 1990.
- [27] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres. Optimal eavesdropping in quantum cryptography. i. information bound and optimal strategy. *Phys. Rev. A*, 56:1163, 1997.
- [28] C.-H. F. Fung, K. Tamaki, and H.-K. Lo. Performance of two quantum-key-distribution protocols. *Phys. Rev. A*, 73:012337, 2006.
- [29] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma. Security proof of quantum key distribution with detection efficiency mismatch. *arXiv:0802.3788v1*, 2008.
- [30] A. Garg and N. D. Mermin. Detector inefficiencies in the einstein-podolsky-rosen experiment. *Phys. Rev. D*, 35:3831, 1987.
- [31] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. *Rev. of Mod. Phys.*, 74:145–195, JANUARY 2002.
- [32] C. Gobby, Z. L. Yuan, and A. J. Shields. Quantum key distribution over 122 km of standard telecom fiber. *Appl. Phys. Lett.*, 84:3762–3764, 2004.
- [33] D. Gottesman and I. L. Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 402:390, NOVEMBER 1999.

- [34] D. Gottesman and H.-K. Lo. Proof of security of quantum key distribution with two-way classical communications. *IEEE Transactions on Information Theory*, 49(2):457, 2003.
- [35] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill. Security of quantum key distribution with imperfect devices. *Quant. Inf. Comput.*, 4:325, 2004.
- [36] J. W. Harrington, J. M. Ettinger, R. J. Hughes, and J. E. Nordholt. Enhancing practical security of quantum key distribution with a few decoy states. *ArXiv.org:quant-ph/0503002*, 2005.
- [37] J. Hasegawa, M. Hayashi, T. Hiroshima, and A. Tomita. Security analysis of decoy state quantum key distribution incorporating finite statistics. *arXiv:0707.3541*, 2007.
- [38] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim. Secure key from bound entanglement. *Phys. Rev. Lett.*, 94:160502, 2005.
- [39] B. Huttner, N. Imoto, N. Gisin, and T. Mor. Quantum cryptography with coherent states. *Phys. Rev. A*, 51:1863, 1995.
- [40] W.-Y. Hwang. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.* , 91:057901, August 2003.
- [41] H. Inamori, N. Lütkenhaus, and D. Mayers. Unconditional security of practical quantum key distribution. *Eur. Phys. J. D*, 41:599, 2007.
- [42] K. Inoue, E. Waks, and Y. Yamamoto. Differential phase shift quantum key distribution. *Phys. Rev. Lett.* , 89:037902, 2002.
- [43] E. Jeffrey, N. A. Peters, and P. G. Kwiat. Towards a periodic deterministic source of arbitrary single-photon states. *New Journal of Physics*, 6:100, 2004.
- [44] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger. Quantum cryptography with entangled photons. *Phys. Rev. Lett.*, 84:4729, 2000.
- [45] R. Kaltenbaek, M. Aspelmeyer, T. Jennewein, C. Brukner, A. Zeilinger, M. Pfenigbauer, and W. R. Leeb. Proof-of-concept experiments for quantum physics in space. In R. E. Meyers and Y. Shih, editors, *Proc. of SPIE: Quantum Communications and Quantum Imaging*, volume 5161, page 252, February 2004.

- [46] J. Kim, O. Benson, H. Kan, and Y. Yamamoto. A single-photon turnstile device. *Nature*, 397:500, 1999.
- [47] E. Knill, R. Laflamme, and G. J. Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409:46, JANUARY 2001.
- [48] M. Koashi. Unconditional security of coherent-state quantum key distribution with a strong phase-reference pulse. *Phys. Rev. Lett.* , 93:120501, 2004.
- [49] M. Koashi. Security of quantum key distribution with discrete rotational symmetry. *arXiv:quant-ph/0507154v1*, 2005.
- [50] M. Koashi. Simple security proof of quantum key distribution via uncertainty principle. *arXiv:quant-ph/0505108*, 2005.
- [51] M. Koashi. Efficient quantum key distribution with practical sources and detectors. *arXiv:quant-ph/0609180*, 2006.
- [52] M. Koashi. Unconditional security proof of quantum key distribution and the uncertainty principle. *J. Phys. Conf. Ser.*, 36:98, 2006.
- [53] M. Koashi. Complementarity, distillable secret key, and distillable entanglement. *arXiv:0704.3661*, 2007.
- [54] M. Koashi and J. Preskill. Secure quantum key distribution with an uncharacterized source. *Phys. Rev. Lett.* , 90:057902, 2003.
- [55] P. Kok and S. L. Braunstein. Postselected versus nonpostselected quantum teleportation using parametric down-conversion. *Phys. Rev. A*, 61:042304, 2000.
- [56] B. Kraus, N. Gisin, and R. Renner. Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Phys. Rev. Lett.*, 95:080501, 2005.
- [57] A. Kuzmich, W. P. Bowen, A. D. Boozer, A. Boca, C. W. Chou, L.-M. Duan, and H. J. Kimble. Generation of nonclassical photon pairs for scalable quantum communication with atomic ensembles. *Nature*, 423:731, 2003.
- [58] M. J. LaGasse. Secure use of a single single-photon detector in a qkd system. *US patent application*, (20050190922), 2005.

- [59] C. Langrock, E. Diamanti, R. V. Roussev, Y. Yamamoto, M. M. Fejer, and H. Takesue. Highly efficient single-photon detection at communication wavelengths by use of upconversion in reverse-proton-exchanged periodically poled linbo3 waveguides. *Optics Letters*, 30:1725, 2005.
- [60] H.-K. Lo. Quantum key distribution with vacua or dim pulses as decoy states. In *Proc. of IEEE ISIT*, page 137. IEEE, 2004.
- [61] H.-K. Lo. Getting something out of nothing. *Quantum Information and Computation*, 5:413–418, 2005.
- [62] H.-K. Lo and H.-F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283:2050, 1999.
- [63] 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.
- [64] H.-K. Lo and N. Lütkenhaus. Quantum cryptography: from theory to practice. *Physics in Canada*, 63:191, 2007.
- [65] H.-K. Lo, X. Ma, and K. Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.* , 94:230504, June 2005.
- [66] H.-K. Lo and J. Preskill. Phase randomization improves the security of quantum key distribution. *arXiv: quant-ph/0504209*, 2005.
- [67] H.-K. Lo and J. Preskill. Security of quantum key distribution using weak coherent states with nonrandom phases. *arXiv:quant-ph/0610203*, 2006.
- [68] B. Lounis and W. E. Moerner. Single photons on demand from a single molecule at room temperature. *Nature*, 407:491, 2000.
- [69] N. Lütkenhaus. Quantum key distribution: theory for application. *Appl. Phys. B*, 69(5-6):395–400, December 1999.
- [70] N. Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A*, 61:052304, 2000.

- [71] N. Lütkenhaus and M. Jahma. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. *New Journal of Physics*, 4:44.1–44.9, 2002.
- [72] X. Ma. Security of quantum key distribution with realistic devices. *arXiv: quant-ph/0503057*, 2004.
- [73] X. Ma. Unconditional security at a low cost. *Phys. Rev. A*, 74:052325, 2006.
- [74] X. Ma, C.-H. F. Fung, F. Dupuis, K. Chen, K. Tamaki, and H.-K. Lo. Decoy state quantum key distribution with two-way classical post-processing. *Phys. Rev. A*, 74:032330, 2006.
- [75] X. Ma, C.-H. F. Fung, and H.-K. Lo. Quantum key distribution with entangled photon sources. *Phys. Rev. A*, 76:012307, 2007.
- [76] X. Ma and H.-K. Lo. Quantum key distribution with triggering parametric down conversion sources. *arXiv:0803.2543v1*, 2008.
- [77] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo. Practical decoy state for quantum key distribution. *Phys. Rev. A*, 72:012326, July 2005.
- [78] V. Makarov, A. Anisimov, and J. Skaar. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A*, 74:022313, 2006.
- [79] E. Maneva and J. Smolin. Improved two-party and multi-party purification protocols. 2000.
- [80] T. W. Marshall, E. Santos, and F. Selleri. Local realism has not been refuted by atomic cascade experiments. *Phys. Lett. A*, 98:5, 1983.
- [81] L. Masanes and A. Winter. Unconditional security of key distribution from causality constraints. *ArXiv: quant-ph/0606049*, 2006.
- [82] W. Maurer and C. Silberhorn. Passive decoy state quantum key distribution: Closing the gap to perfect sources. *Phys. Rev. A*, 75:050305(R), 2007.
- [83] U. M. Maurer and S. Wolf. Unconditionally secure key agreement and the intrinsic conditional information. *IEEE Trans. Inf. Theory*, 45:499, 1999.

- [84] D. Mayers. Unconditional security in quantum cryptography. *Journal of the ACM*, 48(3):351406, May 2001.
- [85] D. Mayers and A. Yao. Quantum cryptography with imperfect apparatus. In *FOCS, 39th Annual Symposium on Foundations of Computer Science*, page 503. IEEE, Computer Society Press, Los Alamitos, 1998.
- [86] P. W. Milonni, J. H. Carter, C. G. Peterson, and R. J. Hughes. Effects of propagation through atmospheric turbulence on photon statistics. *J. Opt. B: Quantum Semiclass. Opt.*, 6:S742, 2004.
- [87] P. M. Pearle. Hidden-variable example based upon data rejection. *Phys. Rev. D*, 2:1418, 1970.
- [88] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan. Experimental long-distance decoy-state quantum key distribution based on polarization encoding. *Phys. Rev. Lett.* , 98:010505, 2007.
- [89] A. E. B. Podolsky and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777, 1935.
- [90] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma. Time-shift attack in practical quantum cryptosystems. *Quantum Information and Computation*, 7:073, 2007.
- [91] B. Qi, C.-H. F. Fung, Y. Zhao, X. Ma, K. Tamaki, C. Chen, and H.-K. Lo. Quantum hacking: attacking practical quantum key distribution systems. In R. E. Meyers, Y. Shih, and K. S. Deacon, editors, *Quantum Communications and Quantum Imaging V*, volume 6710, page 67100I. SPIE, 2007.
- [92] B. Qi, Y. Zhao, X. Ma, H.-K. Lo, and L. Qian. Improve the efficiency of a practical quantum key distribution system. volume 6710, page 671015. SPIE, 2007.
- [93] B. Qi, Y. Zhao, X. Ma, H.-K. Lo, and L. Qian. Quantum key distribution with dual detectors. *Phys. Rev. A*, 75:052304, 2007.
- [94] T. S. Rappaport. *Wireless Communications: Principles and Practice (Prentice Hall Communications Engineering and Emerging Technologies Series)*, chapter 8, page 415. Pearson Education, 2002.

- [95] J. G. Rarity, P. M. Gorman, P. R. Knight, H. Weinfurter, and C. Kurtsiefer. Quantum communications in space. In R. E. Meyers and Y. Shih, editors, *Proc. of SPIE: Quantum Communications and Quantum Imaging*, volume 5161, page 240, February 2004.
- [96] R. Renner. *Security of Quantum Key Distribution*. PhD thesis, Swiss Federal Institute of Technology, 2005.
- [97] G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden. Automated “plug&play” quantum key distribution. *Electronics Letters*, 34(22):2116–2117, 1998.
- [98] R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120, 1978.
- [99] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt. Long-distance decoy-state quantum key distribution in optical fiber. *Phys. Rev. Lett.* , 98:010503, 2007.
- [100] D. Rosenberg, A. E. Lita, A. J. Miller, and S. W. Nam. Noise-free high-efficiency photon-number-resolving detectors. *Phys. Rev. A*, 71:061803(R), 2005.
- [101] V. Scarani, G. R. A. Acin, and N. Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.* , 92:057901, 2004.
- [102] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Phys. Rev. Lett.* , 98:010504, 2007.
- [103] M. O. Scully and M. S. Zubairy. *Quantum Optics*, chapter 2.2, page 50. Cambridge University Press, 1997.
- [104] C. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656, 1949.
- [105] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, page 124, 1994.

- [106] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* , 85(2):441, July 2000.
- [107] A. M. Steane. Multiple-particle interference and quantum error correction. *Proc. R. Soc. London A*, 452:2551, 1996.
- [108] H. Takesue, E. Diamanti, C. Langrock, M. M. Fejer, and Y. Yamamoto. 10-ghz clock differential phase shift quantum key distribution experiment. *Optics Express*, 14:9522, 2006.
- [109] K. Tamaki and H.-K. Lo. Unconditionally secure key distillation from multiphotons. *Phys. Rev. A*, 73:010302, 2006.
- [110] K. Tamaki, N. Lütkenhaus, M. Koashi, and J. Batuwantudawe. Unconditional security of the bennett 1992 quantum key-distribution scheme with strong reference pulse. *arXiv:quant-ph/0607082*, 2006.
- [111] R. T. Thew, S. Tanzilli, L. Krainer, S. C. Zeller, A. Rochas, I. Rech, S. Cova, H. Zbinden, and N. Gisin. Low jitter up-conversion detectors for telecom wavelength ghz qkd. *New Journal of Physics*, 8:32, 2006.
- [112] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin. Quantum cryptography using entangled photons in energy-time bell states. *Phys. Rev. Lett.*, 84:4737, 2000.
- [113] P. D. Townsend. Experimental investigation of the performance limits for first telecommunications-window quantum cryptography systems. *IEEE Photonics Technology Letters*, 10(7):1048–1050, July 1998.
- [114] T. Tsurumaru and K. Tamaki. Security proof for qkd systems with threshold detectors. *arXiv:0803.4226*, 2008.
- [115] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Öemer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger. Entanglement-based quantum communication over 144 km. *Nature Physics*, 3:481, 2007.
- [116] G. S. Vernam. Cipher printing telegraph systems for secret wire and racho telegraphm communications. *J. AIEE*, page 109, 1926.

- [117] P. Villoresi, F. Tamburini, M. Aspelmeyer, T. Jennewein, R. Ursin, C. Pernechele, G. Bianco, A. Zeilinger, and C. Barbieri. Space-to-ground quantum-communication using an optical ground station: a feasibility study. In R. E. Meyers and Y. Shih, editors, *Proc. of SPIE: Quantum Communications and Quantum Imaging II*, volume 5551, page 113, 2004.
- [118] K. G. H. Vollbrecht and F. Verstraete. Interpolation of recurrence and hashing entanglement distillation protocols. *Phys. Rev. A*, 71:062325, 2005.
- [119] D. F. Walls and G. J. Milburn. *Quantum Optics*. Springer, Berlin, 1994.
- [120] Q. Wang, W. Chen, G. Xavier, M. Swillo, T. Zhang, S. Sauge, M. Tengner, Z.-F. Han, G.-C. Guo, and A. Karlsson. Experimental decoy-state quantum key distribution with a sub-poissonian heralded single-photon source. *Phys. Rev. Lett.*, 100:090501, 2008.
- [121] Q. Wang, X.-B. Wang, G. Björk, and A. Karlsson. Improved practical decoy state method in quantum key distribution with parametric down conversion source. *Europhysics Letters*, 79:40001, 2007.
- [122] Q. Wang, X.-B. Wang, and G.-C. Guo. Practical decoy-state method in quantum key distribution with a heralded single-photon source. *Phys. Rev. A*, 75:012312, 2007.
- [123] X.-B. Wang. Beating the *pns* attack in practical quantum cryptography. *Phys. Rev. Lett.*, 94:230503, 2005.
- [124] X.-B. Wang. A decoy-state protocol for quantum cryptography with 4 intensities of coherent states. *Phys. Rev. A*, 72:012322, 2005.
- [125] M. N. Wegman and J. L. Carter. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18:143–154, 1979.
- [126] M. N. Wegman and J. L. Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22:265–279, 1981.
- [127] Q. D. Xuan, R. Alléaume, L. Xiao, F. Treussart, B. Journet, and J.-F. Roch. Intensity noise measurement of strongly attenuated laser diode pulses in the time domain. *Eur. Phys. J. Appl. Phys.*, 35:117, 2006.

- [128] Z.-Q. Yin, Z.-F. Han, W. Chen, F.-X. Xu, Q.-L. Wu, and G.-C. Guo. Experimental decoy quantum key distribution up to 130km fiber. *arXiv:0704.2941*, 2007.
- [129] Z. L. Yuan, A. W. Sharpe, and A. J. Shields. Unconditionally secure one-way quantum key distribution using decoy pulses. *Appl. Phys. Lett.*, 90:011118, 2007.
- [130] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo. Experimental demonstration of time-shift attack against practical quantum key distribution systems. *arXiv:0704.3253*, 2007.
- [131] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian. Experimental quantum key distribution with decoy states. *Phys. Rev. Lett.* , 96:070502, FEBRUARY 2006.
- [132] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian. Simulation and implementation of decoy state quantum key distribution over 60km telecom fiber. In *Proc. of IEEE ISIT*, page 2094. IEEE, 2006.