Doctoral Dissertation

Practical quantum key distribution system robust against side-channel attacks

サイドチャネル攻撃耐性のある実用的量子鍵配送システム

Muataz Mezaal Alhussein

January - 2020

Graduate School of Engineering,

Osaka University

Abstract

Quantum mechanics is a theory that brings a new understanding of the world especially around a microscopic scale, in which some phenomena look fundamentally different from our intuitive sense. Applications of this theory have revolutionized technologies that we use in our daily life. These days, one particular field known as quantum information processing is being investigated for its potential to bring tools that can solve some of key questions in science. For example, a quantum system enables distant two parties to generate an identical secret key for a cryptosystem, which is secure against any eavesdropping permitted by physical law. It relied on the fact that measuring any quantum system would change its state, from which eavesdropping is revealed. The scheme to create a secret key as above is called “Quantum Key Distribution” or “QKD” for short.

The security of QKD is mathematically provable, and a system assuming ideal devices has been proved to be unconditionally secured. However, any implementation would have to use some currently available technologies, which have some gaps from the original theoretical model. Then, there is a question if the theoretical security is still hold with such gaps. In other words, can quantum mechanics still provide provable security to actually implemented systems?

The above question opens a new kind of research, where eavesdropping taking advantage of actual devices’ gap from the theoretical model, called side-channel attacks, is searched, and a countermeasure against it is devised, in order to make practically implemented systems secure. This thesis is involved in this kind of study, and proposes some countermeasures against the most powerful side-channel attack, i.e., detector blinding and control attack.

This thesis consists of seven chapters, which is organized as follows:

Chapter 1 is the introduction of the thesis. The history of quantum cryptography is briefly introduced. Then, the purpose of this thesis is described.

Chapter 2 describes the quantum key distribution algorithm in general. We explain in brief the theoretical security of quantum key distribution. Some examples of quantum key distribution systems are also presented.

Chapter 3 introduces side-channel attacks, including operating properties of a single-photon detector. We describe loopholes in a single-photon detector and attacks taking advantage of the loopholes. Some previously proposed countermeasures are also introduced with some discussion.

In **Chapter 4**, we propose a countermeasure using post processing in four-states QKD protocols, which utilizes photon statistics of weak coherent light, monitoring coincident clicks at a measurement system, to detect eavesdropping. We also provide an analysis estimating the number of coincident clicks, and conduct an experiment to confirm the feasibility of this scheme.

In **Chapter 5**, we conduct experiments of four-state QKD systems with the countermeasure proposed in Chapter 4. A novel receiver configuration is also proposed and demonstrated, which enables a simpler setup than conventional QKD receivers.

In **Chapter 6**, we propose a countermeasure against side-channel attack in differential phase shift QKD. We perform theoretical estimation and simulations to evaluate the system performance of the proposed scheme.

Finally, we conclude the thesis in **Chapter 7**.

Acknowledgements

First of all, I would like to gratefully and sincerely thank my supervisor, **Prof. Kyo Inoue**, for his guidance, understanding, and patience during my graduate studies at Osaka University. His keen insight and wealth of creative ideas have always provided me with precise guiding frameworks for performing my research. I have learned many valuable lessons through my collaboration with him. I have been truly lucky to have this opportunity to study under his supervision. I have been influenced by his personality both as a scientist and a person; his commitment, hardworking, and achievements are of my admiration.

I would like to express my grateful appreciation to Professor Tetsuya Takine, Professor Noboru Babaguchi, Professor Atsuko Miyaji, Professor Takashi Washio, Professor Seiichi Sampei, and Professor Kazunori Komatani, of the course of Information and Communications Technologies, Division of Electrical, Electronic, and Information Engineering, Graduate School of Engineering, Osaka University. They provide me with thoughtful discussions during my PhD research.

I would like to express my appreciation to Associate **Prof. Koji Igarashi** of Division of Electrical, Electronic, and Information Engineering, Graduate School of Engineering, Osaka University. I have learned a lot from him.

I am deeply grateful to **Prof. Akihiro Maruta** of Division of Electrical, Electronic, and Information Engineering, Graduate School of Engineering, Osaka University, for his careful review and invaluable comments, which have improved this dissertation.

I would like to give my appreciation to **Dr. Toshimori Honjo** of NTT basic research laboratories for his invaluable advice and help on my research, his advices and support during my experiment was absolutely appreciated. The one-day internship was really significant for me, in which I learned a lot of skills about scientific research.

I would like to express my sincere appreciation to all the past and present members of the Advanced Optical Communications Lab. (Inoue Lab.) in the Division of Electrical, Electronic, and Information Engineering, Graduate School of Engineering, Osaka University for giving me a

lot of helpful suggestions and discussions about this thesis. Especially, I would like to thank **Ms. Shizuka Yoshizawa**, who has always been very helpful and supportive during my research activities.

In addition, I would like to thank all friends I made during my studies in Japan, and from all over the world. Their understanding and support really help me to face all the challenges and stress in my research and life: **Abbas Mousa**, **Hamza Bahr-al-Uloom, Mousa Nabeel**, and many others. Special thanks to **Reona Katsuda** for always being there for me, and for the ultimate support and understanding during my ups and downs. Without this support, I would not be able to stand along.

I would like to thank my father **Mazeel Hussein**, mother **Maysoon Muosa**, sisters **Zainab, Ayat** and brothers **Ahmed, Muhannad, Mazin**. Without their understanding and support, I am unable to complete my research in Japan.

Finally, I would like to express my gratitude for Japanese government and Japanese embassy in Iraq for giving me this chance to study and explore Japan under **MEXT scholarship**. I was lucky to have their full support. I have been very lucky to know such rich and unique culture, thank you Japan.

Special note: I dedicate this work for the innocent people of Iraq who lost their lives during the current demonstration all over Iraq, while I am preparing my defense. Moreover, I would dedicate this work to the soul of **Hussein Ali** (my cousin), who died in the morning of my defense. During the time of my submission, I am watching with concern the news and wish this year brings peace to Iraq and the world.

Contents

Chapter 1

Introduction

1.1 Introduction

Cryptography originates from the Greek words *kryptos* meaning hidden and *graphein* meaning writing. The combination of these two words means an art of writing messages with their contents hidden from anyone but intended receiver. The importance for such art can be clearly understood in some situations, for instance the famous Enigma machine and its impact during the second world war. The field of cryptography has a long history and has helped the evolution of human society through lasting improvement, from the ancient Greece through wars in the medieval times to the second world war, and up to today's online banking.

On the other hand, quantum mechanics is a theory describing phenomena that cannot be explained by classical mechanics. This theory has fundamentally changed the way of viewing the physical world surrounding us, specifically microscopic worlds of atomic scales. It may sometimes counter our intuition for some physical phenomena. Examples are quantum-mechanical principles of quantum uncertainty and superposition. Many experiments performed ever since the advent of quantum mechanics have shown that this theory accurately models the physical reality. Stimulated by its impact, intensive researches have been conducted to reveal properties of quantum mechanical systems and their applications to the field of information processing, named quantum information processing. With time, this field has diverged into two main applications: computation and communication. The former is quantum computing that aims at solving some problems that cannot to be solved by conventional computers within a realistic time. On the other hand, the latter aims at introducing novel functions into communications that cannot be achieved by conventional communications, especially cryptography, where the ultimate security is a long-cherished target. Quantum cryptography is a technology that can achieve the ultimate security, which is treated in this thesis.

1.2 History of the quantum cryptography

Quantum cryptography can be traced back to an idea firstly introduced by Stephen Wiesner in the late 1960s, when he wrote the paper entitled “conjugate coding”. However, his innovative paper was unpublished and went unnoticed at that time. In that paper, Wiesner explained the principle of using quantum mechanics to produce bank notes that is impossible to be faked, and also introduced how to implement it in what he called “multiplexing channel”. After that, Charles H. Bennett knew Wiesner and heard about his unpublished paper, which is acknowledged in his famous paper on quantum cryptography [1]. Then, quantum cryptography was publically proposed, when Charles and Gilles Brassard met on the 20th IEEE symposium on the Foundation of Computer Science held in Puerto Rico in 1979. Their proposal in a crypto 82 [2] revived the Wiesner’s paper, which was subsequently published in Sigact News [3].

When quantum cryptography was firstly proposed, everyone (including the authors) thought it as a work of science fiction. This is because technologies required to implement it were out of reach at that time. This event, unfortunately, left most audience in that conference (i.e., crypto ’82) an impression that anything to do with quantum cryptography was unrealistic.

Fortunately, when Bennett and Brassard realized that photons can be used for transferring information not for storing, their idea became main breakthrough in quantum cryptography (this idea should be also credited to Wiesner’s original paper, that explicitly described the use of quantum physics for transmission of information). It led to the possibility of employing one-time pad cryptosystem [4], which offers perfect security but had been regarded as unpractical.

Later, Bennett came up with an idea of *quantum key distribution channel* or shortly *QKD* in 1984, which uses quantum mechanics for distributing a secure key, and Brassard designed somewhat less realistic *quantum coin tossing protocol* [5], [6]. This protocol of distributing a secret key is called BB84, which has been the standard QKD protocol. Besides QKD, Bennett, Brassard, and Crpeau have developed quantum protocols to achieve bit commitment and coin-tossing [7, 8].

Following BB84, some other QKD protocols have been proposed. Ekirt proposed a protocol [9] utilizing quantum entanglement, which is based on the fact that measurement of quantum-mechanically entangled particles gives correlated results, even when the two particles are at

distant locations each other. Quantum mechanics tells that any measurement on an entangled pair collapses the "nonlocality" [10] of the particles, from which eavesdropping can be revealed because any eavesdropping accompanies with some measurement. The protocol proposed by Ekert is known as E91 or simply the Ekert protocol. In 1992, Bennett proposed another protocol that uses two non-orthogonal states to implement secure system [11], known as B92 protocol. Another protocol is also proposed, known as differential phase shift (DPS) QKD [12], in which a train of weak coherent pulses with phase difference between adjacent pulses is used to encode the information. DPS-QKD features a simple setup and efficient use of the time domain.

After the theoretical proposal, Bennett and others demonstrated the first experiment of a BB84 QKD system in 1992 [1], which was a lab-bench experiment conducted over 32 cm free-space quantum channel, using polarization-encoded photons as information carrier. Encouraged by this experiment, the interest for QKD has increased. Moreover, the researches' attraction to QKD have further increased after the invention of Shor's algorithm, which is a quantum computing algorithm for solving factorization. RSA cryptosystem, that is widely used presently, can be easily broken with Shor's algorithm. This event also encouraged the QKD research. Then, some QKD experiments were demonstrated over a long fiber line [13]. These days, the distance has been increased to 250 km over an optical fiber [14]. In this experiment, a practical QKD protocol called coherent one way (COW) was performed, where a train of pulses grouped in pairs are used to encode the information by the position of the pulse within the pair. Another achieved distance was 144 km in a free space [15], in which entanglement-based quantum key distribution was used. In addition, there exist several commercial companies that supply QKD systems.

While experimental efforts have been conducted, theoretical studies have been significantly developed since 1984. One important discovery includes privacy amplification [16], which makes it possible to remove eavesdropping's partial knowledge on a secret key. Eventually, the first security proof was established [17–20], which proved the unconditional security of BB84 using perfect devices. Then, research started to consider system models assuming real devices in security analysis [21-23]. Although QKD using ideal devices has been proven to be secured, there implementation is still considerably challenging. The most challenging QKD device is a single-photon source that emits just one photon per pulse. Therefore, practical QKD system use weak coherent light instead of single-photons. However, a coherent light source sometimes emits more

than one photon in one pulse even when its output is strongly attenuated. Taking an advantage of this imperfection, a powerful attack named photon-number-splitting (PNS) attack [24, 25] was proposed, where an eavesdropper picks up and keeps a photon from pulses that include multiple photons, while blocks pulses including just one photon. This attack severely restricts the QKD performance [21, 22,26]. Then a countermeasure against the PNS attack, called decoy method, was proposed [27-28], which allows implementations of QKD systems using a coherent source and has been widely employed in QKD experiments.

The above QKD protocols are usually referred as “discrete variable QKD”. On the other hand, another types of QKD scheme, called “continuous variable QKD (CV-QKD)”, was introduced, which uses weak coherent light and homodyne detection instead of single-photon detection [29].

Table 1.1. Brief history of QKD study sequence

<table>
<tr><th></th><th>QKD protocol</th><th>Security</th><th>Experiments</th></tr>
<tr><td>1980</td><td>Frist idea of BB84 protocol was proposed</td><td></td><td></td></tr>
<tr><td>1990</td><td>E91, B92 protocols</td><td rowspan="2">Theoretical proofs in the frame of quantum mechanics, considering conceptual quantum attacks</td><td rowspan="2">Experimental demonstration for the QKD systems</td></tr>
<tr><td>2000</td><td>DPS QKD, decoy BB84 protocols</td></tr>
<tr><td>2010</td><td></td><td>Side-channel attack, outside the frame work of quantum mechanics</td><td>Demonstration of the side-channel attack against QKD systems</td></tr>
<tr><td></td><td>MDI-QKD against side-channel attack is proposed</td><td></td><td>Lab test only</td></tr>
</table>

1.3 Practical security in QKD

While the theoretical study on the security has been developed as described above, security loopholes out of the theoretical framework have been discovered. Eavesdropping utilizing such loopholes is called as side-channel attacks [30–43], because they are outside the framework of quantum mechanics. Among several side-channel attacks, the detector control attack is known as the most successful and strongest attack, because it has been demonstrated and Eve could obtain full key without being detected [41]. In this attack, Eve exploits the operation characteristics of an actual single-photon detector, by which she can fully obtain a secret key, without being noticed. This attack was experimentally demonstrated using off-the-shelf devices [41]. Eavesdropping capturing a full secret key from a QKD system by a side-channel attack was also demonstrated at the National University of Singapore [42].

In order to avoid such side-channel attacks, device-independent QKD (DI-QKD) [44] was proposed, in which a number of assumptions on devices are excluded so that the security proof does not need to care about imperfect devices. However, its implementation relies on a loophole-free Bell test, which requires a high detection probability at Bob. A novel protocol focusing on side-channel attacks exploiting detector's characteristics was also proposed, which is called measurement device independent (MDI) QKD [45]. In this protocol, detectors are removed from authenticated parties, and measurement is performed by an untrusted third party. Therefore, the system is free from detector control attacks. However, MDI QKD requires a Bell state measurement, which is not easy to implement in practice. Therefore, a practical countermeasure against side-channel attacks is desired.

1.4 Purpose of this thesis

QKD has moved from a science fiction to a theoretically and experimentally implemented system, for which various security proofs have been presented, and several start-ups were established. However, more improvement is required in term of security, key creation rate, practicality, and transmission distance. Especially, side-channel attacks utilizing loopholes in actual devices are

an issue these days. Without countermeasure against it, a QKD system cannot be regarded as secure in practice.

On the above backgrounds, this thesis aims to fill a security loophole in actual QKD systems. To be specific, we propose countermeasures against side-channel attacks, especially the detector blinding and control attack, which is known as the strongest side-channel attack as it was demonstrated and full key was obtained by Eve without being detected. Although MDI-QKD was proposed and has been intensively studied to be free from this side-channel attack, its implementation requires highly advanced technologies. Therefore, this thesis presents a QKD system equipping a simple and easily implementable countermeasure against the detector blinding and control attack, including the evaluation of its performance.

1.5 Thesis organization

This thesis organized as follows. In Chapter 2, we introduce a general protocol of QKD, including discussion on its theoretical security. Some examples of concrete QKD protocols are also presented. Chapter 3 introduces the idea of side-channel attacks against QKD, including the operation characteristics of actual detectors, and describes some concrete attacks. Previously proposed countermeasures are also presented. Chapters 4, 5, and 6 present our research. Chapter 4 describes our proposal of countermeasure against detector blinding and control attack for four state protocols (i.e., BB84 and DQPS-QKD), in which we propose to utilize the discarded events in the conventional protocol to monitor the side-channel attack. Chapter 5 describes an experiment demonstration of the countermeasure proposed in Chapter 4, employing a newly proposed receiver circuit that enables the configuration simpler than conventional receivers used in four-states QKD systems. Chapter 6 proposes a countermeasure against blinding and control attack for DPS-QKD protocol, the structure of this protocol is different from the previous one for which the countermeasure is ineffective. We install a variable attenuator to monitor the side-channel attack. The optimization of the operating condition and the evaluation of the system performance are also presented. Finally, we conclude this thesis in Chapter 7.

The abovementioned organization is summarized in Fig. 1.1.

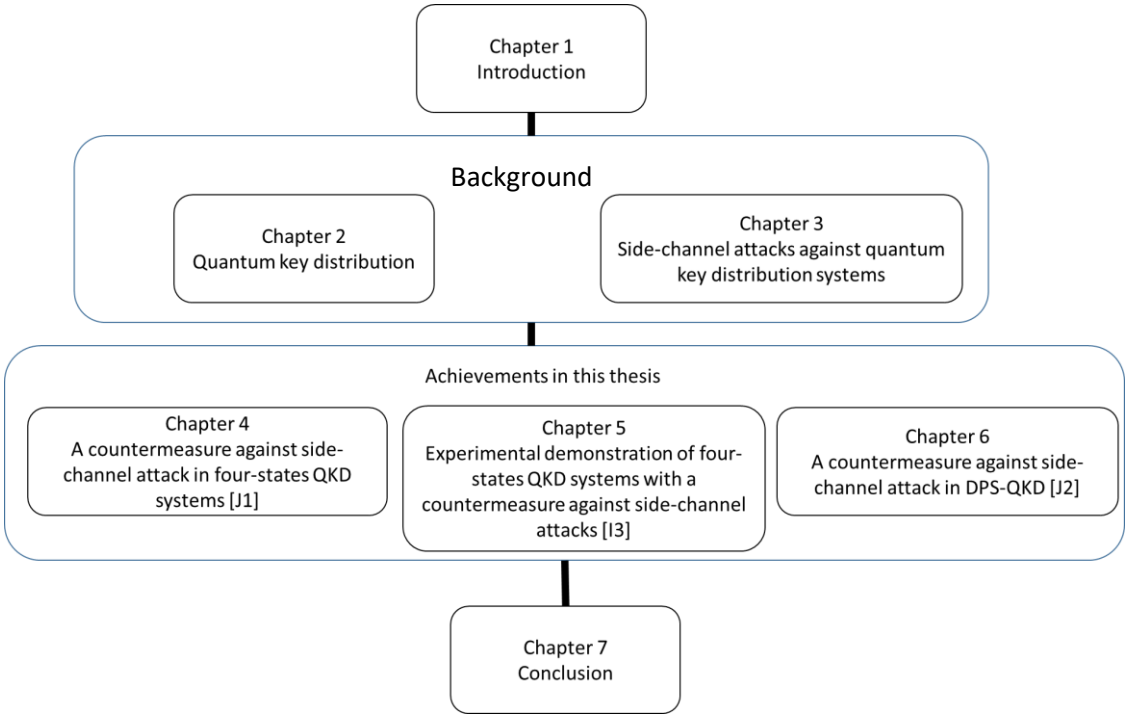

Fig. 1.1. Thesis organization. (J1), (J2), (I3): publication lists, where J, I refer to Journal and International conference, respectively.

Chapter 2

Quantum key distribution

2.1 Introduction

Exchanging secret messages between two parties is one of the primary interests of human beings. Up to the present, people has come up with ideas for this issue of establishing secure communication, i.e., cryptography. In other words, people have devised methods of preventing malevolent eavesdroppers from accessing the information on message.

The problem in cryptography is that there is always a hacker who could break cryptographic algorithms, and there have been open battles between defenders and hackers. In today's communication, cryptographic systems are based on the computational complexity of decryption. Thus, how difficult it is to break an encrypted code is an issue, meaning that a system is secure if an eavesdropper needs an intractable task to break a code. Here, an intractable cryptographic algorithm is one for which the execution time of decryption scales up exponentially as the size of a code increases. The famous RSA public key cryptography is based on such an algorithm. However, the problem in such algorithms is that they do not have a mathematical proof of the security. There is always a possibility of sufficient computational power breaking codes, such as quantum computers.

In order to solve the above problem of the security, the one-time pad protocol is promising, which uses a secret key with a length equal to one message just once. The security of this scheme has been mathematically proven. However, the question is how to securely pre-share such a key between distant parties. Quantum information technologies propose a way of using quantum mechanics to distribute a secret key for one-time pad cryptosystems. Therefore, the scheme is called quantum key distribution (QKD).

This chapter introduces QKD. First, we describe the general protocol of QKD. Next, its security is discussed. Then, the typical QKD protocol called BB84 is introduced, including a particular attack named photon number splitting attack, because this attack seriously degrades the performance of practical BB84 using weak coherent light as quasi single-photons. Finally, the summary is described.

2.2 Quantum bit (qubit)

In quantum systems, information is encoded onto a quantum bit which is called “qubit”. A qubit is a quantum mechanical bit corresponding to a bit used in classical systems. A quantum bit is defined in a two-dimensional Hilbert space, which is formed by two basis states corresponding to binary 0 and 1, respectively, that are used to encode information similar to a classical bit. A quantum bit is a superposition of the two basis states, and exhibits quantum mechanical coherency such that coefficients of a superposition are complex numbers having a relative phase. Thus, any classical information protocol can be encoded with qubits, whereas quantum information protocols cannot be encoded using classical bits. One example is quantum cryptography, which is a method of distributing a secure key, as described in the following sections.

2.3 Process of key creation

In this section, we describe the general protocol of QKD. Figure 2.1 illustrates a block diagram of steps to generate a secure key in QKD. It includes quantum transmission, sifting, error correction, and privacy amplification, which are described in the following subsection for each.

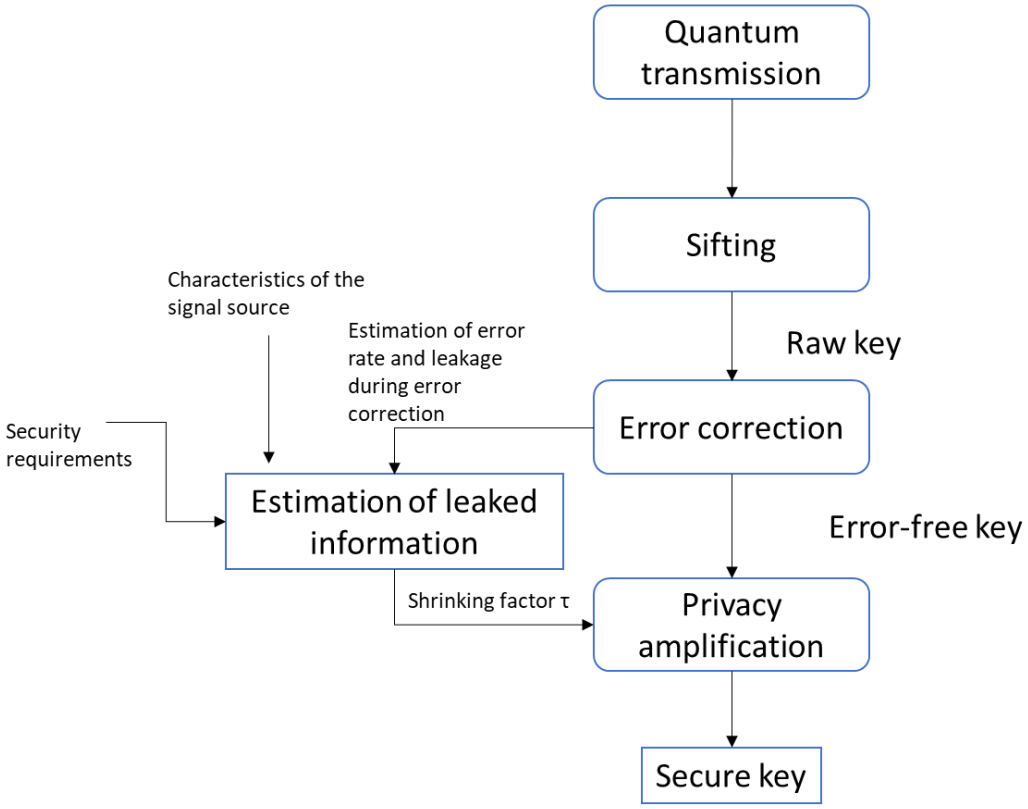

Fig. 2.1. Block diagram of general quantum key distribution algorithm.

2.3.1 Quantum transmission

Quantum transmission is a step in which some quantum states are transmitted over a transmission medium such as a fiber or a free space. The transmitted state is a single photon or entangled photons. There are three types of QKD schemes. One type utilizes single-photons, whose security is based on the uncertainty principle in measuring a quantum state. Examples of this type include BB84, B82, Koashi01, and six-state protocols [6,11,46,47]. BB84 is the firstly proposed QKD protocol which is described in detail in the latter sections in this chapter. Another type of QKD uses entangled photons, whose security is based on a nonlocal quantum correlation in a photon pair. Examples of this type include BBM92 and E91[9,48]. In addition, instead of single photons or entangled photons, a weak coherent light can be used to encode quantum information. Protocols using weak coherent light include CV-QKD and DPS [12, 29].

2.3.2 Sifting

Sifting is a step where two parties who try to share a secure key, usually referred as Alice and Bob, announce some information related to quantum transmission to each other through a public channel, that can be a traditional communication channel. The exchanged information may include what basis Alice chose for the transmitted state, and which basis Bob used for his measurement. Besides, whether a photon was measured or not is also informed from Bob to Alice because a photon can be lost during the transmission. It should be noted here that they do not disclose any information regarding the state itself and the measurement result itself.

Through this step, Alice and Bob have a string of bits, which is called a sifted key or raw key. If the system is perfect with no error, Alice and Bob have a secure key through the above sifting step. Eve, who is an unauthorized party, cannot perform any attack without disturbing a quantum state. Thus, Eve introduces bit errors in a raw key when eavesdropping is conducted, and her presence is revealed by checking some test bits. However, in any practical communication system, bit errors unavoidably occur due to imperfections in the system. It is impossible for Alice and Bob to distinguish such system errors from those caused by eavesdropping. Thus, it cannot be claimed for actual system that bit errors straightforwardly reveal Eve's existence.

In order to deal with such bit errors, additional two steps are conducted. They are error correction and privacy amplification, which are described in the following subsections. These two steps are classically processed using a public channel.

2.3.3 Error correction

Error correction is a step that estimates the bit error rate and corrects errors. In this step, Alice and Bob exchange a piece of information on their raw keys in order to find and correct error bits. For example, they group their bits into blocks and checking the parity of each block. The exchange of such information is performed over a public channel; thus, during the error correction step, leakage of some information to an eavesdropper is unavoidable. This information leakage should be as small as possible. The minimum number (r) of bits to be exchanged for error correction is given by the classical information theory, i.e. Shannon's noiseless coding theorem [49]. For a

given probability of error independent for each bit, *e*, the theorem asserts that the number of exchanged bits *r* relative to the sifted key length *n* is expressed as

$$\lim_{n\to\infty} \frac{r}{n} = -e \log_2 e - (1-e) \log_2 (1-e) \equiv h(e). \quad (2.1)$$

For system implementation, an error-correction algorithm that has a performance close to this limit is desired. There are two classes for the error correction algorithm: unidirectional and bidirectional schemes. In the former one, information is sent from Alice to Bob, and Bob finds bits mismatched to Alice's ones. It is difficult to design this type of error correction algorithm to provide the computational efficiency close to the Shannon limit [50,51]. In the latter scheme, the information flow is bi-directional. In this type, Alice uses Bob's feedback to determine information that she must provide to him.

Other than the above classification, there is another categorization for error correction algorithm; one discarding errors or one correcting them. The former is employed to prevent additional information leakage to Eve. while the latter results in additional information leakage to Eve, which should be accounted in privacy amplification.

2.3.4 Privacy amplification

The final step in creating a secret key is privacy amplification, through which information leaked during the previous steps, i.e., the quantum transmission and the error correction, is eliminated. In this step, a key obtained from the error correction (error-corrected key) is compressed to form a final key that has a required security level. The compression rate is determined by the amount of information that Eve may obtain during the previous steps. A security proof provides the upper bound of the amount of information leaked to Eve, and privacy amplification is performed accordingly.

A simple example of privacy amplification goes as follows: Alice and Bob replace two bits with a single bit of the XOR of the two bits even. If Eve knows one of the two bits, she knows nothing about the newly created bit. In this example of privacy amplification, the key length becomes half as a result of the process. A more efficient algorithm can be employed in practice: two-universal hashing. Such a hash function re-maps *n*-bit inputs to *m*-bit outputs, where $m < n$. The upper-bounded collision probability of two-universal hash functions *F* is $p\,(f(x) = f(x')) \leq 1/2^m$, where

$f \in F$, and all $x, x' \in (\mathbb{Z}^2)^n$. Therefore, Alice and Bob can obtain the secret key $s = f(x)$, where x is a key after error correction, by randomly choosing a function $f \in F$. If Eve has a somewhat different key x', the probability of Eve obtaining same key $f(x')$ is equal or less than $1/2^m$.

2.4 Security in theory

As described in the previous sections, it is important to estimate the amount of information leaked by eavesdropping to obtain a theoretically secured key. This section describes the security treatment for that task. When quantum cryptography was firstly proposed, i.e., BB84 protocol, a simple type of attack was considered alone, namely intercept-resend-attack [52, 53]. Later on, a more generalized attack was discussed based on quantum mechanics. There are three categories in general attacks: individual, collective, and coherent attacks. Figure 2.2 shows the concept of these attacks against a single-photon based QKD system. In the first type, i.e., individual attacks, Eve entangles a quantum probe to each transmitted photon independently. The entangled probes are kept in a quantum memory until the information exchange over a public channel in the sifting step. After that, each of these probes is quantum mechanically measured independently based on the disclosed information. BB84 is proven to be secure against this attack [51,54-56]. In the second type, i.e., collective attack, Eve obtains probes entangled to Alice's photons as in the individual attacks, and then conducts a generalized measurement on the probes with quantum processing. The quantum processing enables Eve to utilize correlations in the information exchange during error correction and privacy amplification for deciphering. BB84 is also proven to be secure against this kind of attack [57]. In the third type, which is the most general attack, Eve regards the quantum transmission as one system, and uses a massive-dimension probe to be entangled with the transmission system. The security proof against this type of attack is achievable considering an ideal or practical qubit source [19,21].

As a matter of fact, the above general attacks are beyond today's technology reach in practice. As mentioned above, these attacks utilize the information of the photon detection time and the bases, which is exchanged between Alice and Bob at an arbitrarily time after the quantum transmission. Therefore, Eve should have a quantum memory with the infinite long decay time. Such a quantum memory is not feasible with the current technology.

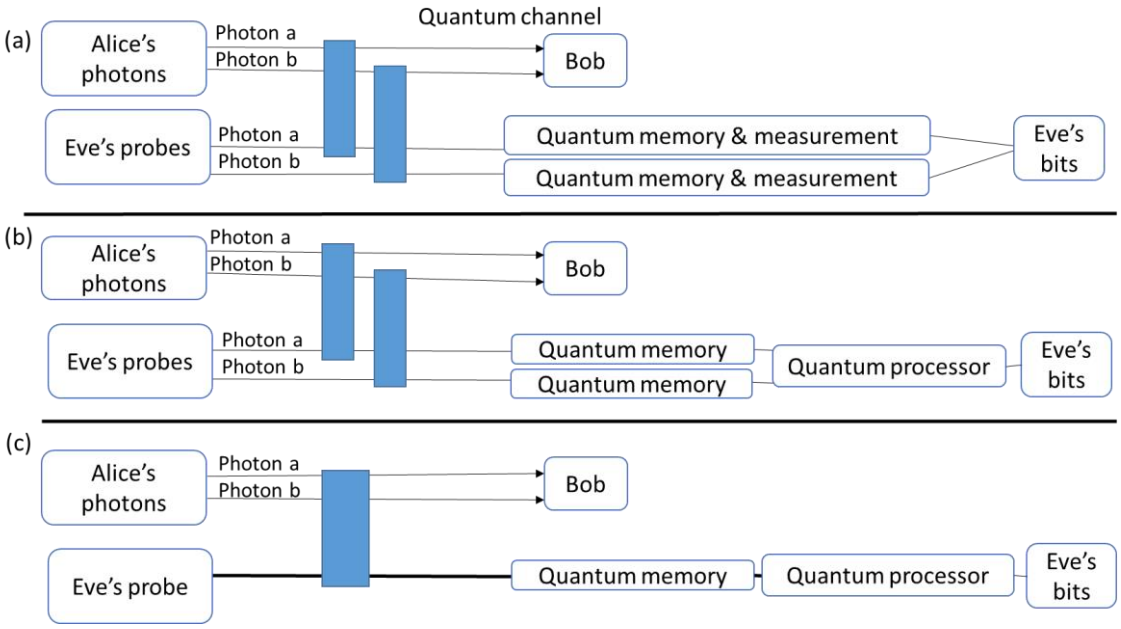

Fig 2.2. The concept of the generalized attacks. (a) Individual attacks: each photon is entangled with single probe, which stored in quantum memory until public exchange; (b) collective attacks: quantum processor is used to utilize the correlation between the probes; (c) coherent attacks: quantum transmission system is entangled to massive-dimension probe and quantum memory, then quantum processor is used to extract the information.

In addition to quantum memories, the coherent attack and the collective attack need some quantum processing, which is conceptual and further distant from the current technologies. These attacks are virtual. However, QKD pursuits the ultimate security, which is guaranteed even against unrealistic but quantum mechanically allowable eavesdropping.

In the step of privacy amplification, the shrinking factor τ, with which an error corrected key is compressed, is determined first, based on an error rate estimated in the error correction step. Then, privacy amplification is applied with the shrinking factor provided by a security proof, through which Eve's residual information becomes less than a negligible value (theoretically limited value) [16]. The estimation of the information leakage assumes the worst-case scenario that all bit errors are attributed to eavesdropping.

After the privacy amplification, a final key is obtained, whose length f is given by the generalized privacy amplification theory as:

$$f = n\tau - r - t\,, \tag{2.2}$$

where n is the length of a sifted key, r is the number of bits disclosed during error correction, and t is a security parameter. The shrinking factor τ in the above equation is given by:

$$\tau = \frac{-\log_2 P_c}{n}\,, \tag{2.3}$$

where P_c is the average collision probability representing the probability of an Eve's bit coinciding with an Alice's or a Bob's bit. The main task of a security proof is to estimate the upper bound of P_c, for a given QKD protocol, e.g., BB84, considering eavesdropping against it.

Equation (2.2) expresses the final secure key length. In order to indicate the system performance, it may be convenient to use the communication rate in the unit of bits/pulse rather than the absolute number of key bits. Provided N is the number of pulses sent from Alice, the secure key generation rate is given by:

$$R = <\frac{f}{N}> \; = R_{sifted} \;\; (\tau - \frac{r}{n} - \frac{t}{n}), \tag{2.4}$$

where < > represents the average, R_{sifted} denotes the sifted key, rate and Eq. (2.2) is substituted.

In practice, however, there exists no error-correction algorithm that is computationally feasible at the Shannon limit. Therefore, an additional factor $f(e)$ is introduced to take the inefficiency of practical algorithms into account, which indicates the performance of an actual error correction algorithm relative to the Shannon limit. Using this $f(e)$, the ratio of information leakage via error correction is

$$<\frac{r}{n}> \; = -f(e)\,[e \log_2 e + (1 - e) \log_2(1 - e)] = f(e)\, h(e). \tag{2.5}$$

$f(e)$ is equal to 1 at the Shannon limit. Then, the final secure key generation rate R is expressed as:

$$R = R_{sifted}\,\{\tau + f(e)\,[e \log_2 e + (1 - e) \log_2(1 - e)]\}. \tag{2.6}$$

R_{sifted} and τ in the above equation is determined by the QKD protocol and eavesdropping.

2.5 Original BB84 protocol

The previous sections describe QKD protocol in general. The latter half of this chapter is dedicated to some specific protocols. In this section, the first QKD protocol proposed by Bennett and Brassard in 1984, known as the BB84 protocol [6], is introduced. The system setup of polarization encode BB84 is shown in Fig. 2.3. Alice encodes her information in a single-photon using either one of two bases; the computational basis and the rotational basis, which are non-orthogonal each other. The original proposal of BB84 utilizes the polarization mode for the information carrier. In this case, the computational basis includes the linear horizontal state $|\leftrightarrow\rangle$ for bit "0"and the linear vertical state $|\updownarrow\rangle$ for bit "1". On the other hand, the rotational basis includes right rotation state $|\circlearrowright\rangle$ for bit "0" and left rotation state $|\circlearrowleft\rangle$ for bit "1". Alice chooses randomly one of the two bases with an equal probability, follow by a random choice of a binary bit 0 or 1 with an equal probability. Then, she sends one of the four states according to the choice of basis and bit.

Bob receives the incoming Alice's state, and measures it, while randomly selecting either the computational or rotational basis measurement with an equal probability. Here, Bob's basis selection method can be passive or active. The former's setup is shown in Fig. 2.3. It uses a 50/50 beam splitter that passively and randomly routes a photon to one of two measurement systems corresponding to each basis. When Bob's basis is matched to Alice's one, his measurement result is deterministic and he definitely knows Alice's state. When Alice's and Bob's bases are mismatched, on the other hand, Bob's measurement result is random and he cannot identify Alice's state.

The active basis selection can be implemented using a polarization modulators based on the electro-optical effect to change the polarization state [21]. Polarization encoding, however, has a problem of the birefringence in a transmission fiber, which makes it difficult to stably control the system operation. To overcome the polarization rotation through a fiber line, some schemes have been proposed, for instance a one-way polarization modulator [54], a two-way polarization modulator [54], a Faraday-Sagnac interferometer [16, 24]. Although, the active basis selection is more cost-effective than the passive basis selection, because of use of one measurement system, it is not stable in practice.

In the sifting process, Alice and Bob reveal their basis choice and the photon detection time (in case of Bob), without revealing the state and the measurement results. Then, they discard bits for which a photon is not detected and the basis is mismatched. Because Bob chooses his basis with an equal probability, 50% of the measurement results is left, which is called “sifted key”.

Table 2.1 shows the detection probability in the passive basis selection, where each of the measurement systems receives a photon with a 50% probability. In a basis-matched case, only one of the detectors clicks with a detection probability of 50%. On the other hand, in a basis-mismatched case, either one of two detectors click with a 25% probability.

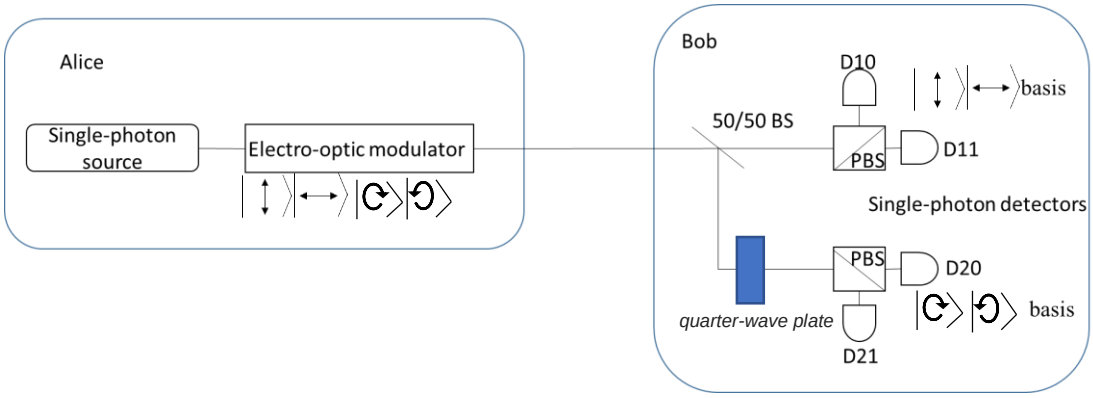

Fig. 2.3. Setup of BB84 protocol with polarization encoding and passive basis-selection measurement. BS: beam splitter; PBS: polarization beam splitter; and D: single-photon detector.

Table 2.1. Detection probabilities at Bob’s detectors in passive selection.

		Bob’s detector			
		D10	D11	D20	D21
Alice’s state	$\|\leftrightarrow\rangle$	0.5	0	0.25	0.25
	$\|\updownarrow\rangle$	0	0.5	0.25	0.25
	$\|\circlearrowleft\rangle$	0.25	0.25	0.5	0
	$\|\circlearrowright\rangle$	0.25	0.25	0	0.5

If there is no error in the system, a sifted key created as above is unconditionally secure and can be used as a secret key, whose security relies on the fact that Eve does not priorily know Alice's basis choice and cannot correctly identify Alice's state as described below. Let us assume a straightforward attack called intercept and resend attack, whose setup is shown in Fig. 2.4. Eve intercepts and measures Alice's signal travelling through the quantum channel, and resends an imitated signal to Bob according to the measurement result. Here, Eve does not know the basis chosen by Alice and thus cannot correctly measure Alice's signal. Then, an errant copy of Alice's signal is sent to Bob, which induces bit error in Bob's measurement. For example, suppose that Eve measures Alice's state with the same measurement setup as Bob's, and chooses a wrong basis (which occurs with a 50% probability), and resends a wrong state, e.g., $|\circlearrowright\rangle$ instead of $|\leftrightarrow\rangle$. When Bob measures the Eve's state with a basis matched to Alice, he creates a bit that would be wrong with a 50% probability, e.g., $|\circlearrowright\rangle$ measured by the computational basis results in $|\leftrightarrow\rangle$ or $|\updownarrow\rangle$ with an equal probability. Therefore, the intercept-resend attack induces a 25% bit error rate. Such errors can be utilized to detect the presence of Eve. Alice and Bob collate their bits each other, sacrificing a fraction of the sifted key, and if there are bit mismatches, they judge that the key is eavesdropped and discard it. Eve is able to use a basis other than the computational basis to perform her measurement, yet it is not difficult to show that the measurement result of such a choice would give a 25% bit error rate.

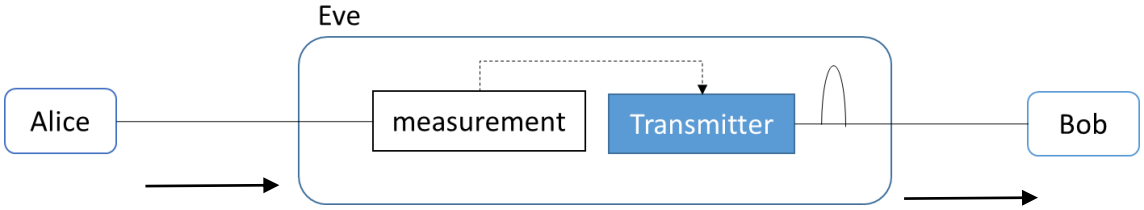

Fig. 2.4. Intercept-resend attack.

The above intercept-resend attack is one example of eavesdropping. Eve can perform a generalized attack with a setup shown in Fig. 2.5, where Eve applied an Optimal Positive Operator Value Measurement (POVM), which is a measurement with a non-negative self-adjoin operators on a Hilbert space and its integral is the identity operator, on Alice's state, followed by a delayed

measurement on her probe state resulting from the POVM to get information about the Alice's state.

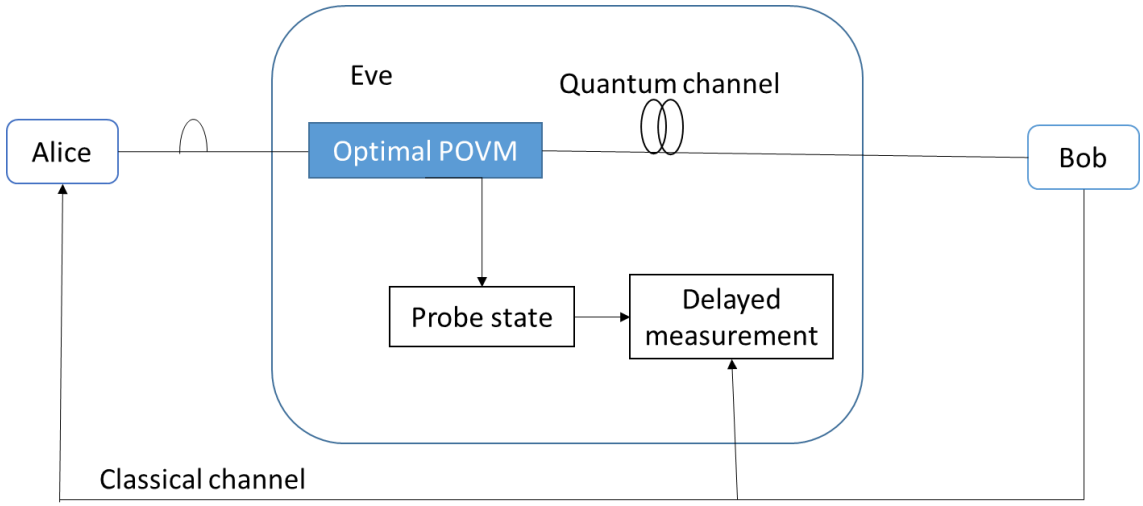

Fig. 2.5. General individual attack.

Although the above general individual attack is more powerful than the intercept-and-resend attack, it also introduces bit errors due to the uncertainty principle and the non-cloning theorem, and any eavesdropping is noticed in principle.

As mentioned above, any eavesdropping induces bit errors. In other words, induced error rate indicates how much information is leaked to Eve. Here, the ratio of information known to Eve is indicated by the collision probability that is the probability of Eve's and Bob's bits being coincident. In BB84 using an ideal single-photon source, the collision probability P_{c0} when general individual attacks are conducted is bounded as [54]

$$P_{c0} \leq \frac{1}{2} + 2e - 2e^2, \tag{2.7}$$

where e is system error rate.

This expression shows that, when $e = 0$, the collision probability is 1/2, meaning that Eve gets no information about a key if there is no error in the system. The average collision probability for the n-bit string can be obtained from Eq. (2.7) as $P_c = P_{c0}^n$, so the shrinking factor is calculated using Eq. (2.3):

$$\tau = \frac{-\log_2 P_c}{n} = \ -\log_2 P_{c0} = \ - \ \log_2\left(\frac{1}{2} + 2e - 2e^2\right). \tag{2.8}$$

Note that this result is only applied on ideal single-photon source.

2.6 Decoy BB84 protocol

2.6.1 Photon number splitting attack

The original BB84 protocol utilizes single-photons as an information carrier. However, a single-photon source is hard to obtain in practice, and a strongly attenuated laser light is usually used as quasi single-photons. The photon number splitting attack is an eavesdropping strategy utilizing properties of laser sources that emit coherent states instead of single-photons. Some pulses generated from a laser contain multi-photons even when they are strongly attenuated, which enable Eve to perform this attack [24]. This eavesdropping became a serious problem when it was proposed, and the BB84 protocol has been modified to overcome this problem. This section introduces the photon number splitting (PNS) attack.

In this attack, Eve measures the number of photons in Alice's signal with a non-demolition measurement, that does not disturb Alice's signal other than the conjugated physical quantity of the photon number, i.e., the phase. When Eve finds more than one photon, she picks up and keeps one of them for herself, while passing the others to Bob. In case of only one photon in Alice's signal, Eve blocks that signal. After the quantum transmission is completed, Bob announces his measurement basis to Alice, based on which Eve can correctly measure her photon, and knows a key bit. It should be noted that the implementation of a non-demolition measurement is still challenging with the current technologies; thus, this eavesdropping is just a theoretical one.

Additional photon loss is introduced by the above attack from the viewpoint of Bob, because Eve blocks Alice's signal having just one photon. In practice, however, a quantum channel has a transmission loss, which allows Eve to conceal the photon loss due to the attack, such that she replaces the lossy channel with a lossless one, and blocks and removes a number of photons corresponding to the original transmission loss.

There are several pieces of study evaluating the secret key rate under such attack [21, 22, 25]. This attack imposes upper bounds the secret key rate depending on the transmittance of the quantum channel and the mean photon number (μ) per pulse sent from Alice. The probability of a laser pulse having *n* photons, p_n, follows a Poisson distribution:

$$p_n = \frac{\mu n\ e^{-\mu}}{n!} \quad , \tag{2.9}$$

where μ is the average photon number. From this probability distribution profile, the probability of more than one photon in a pulse is given by

$$p_{n\geqq 1} = 1 - \ p_0 \simeq \mu, \qquad (\mu << 1) \tag{2.10}$$

and that of more than two photons is

$$p_{n\geqq 2} = 1 - p_1 - \ p_0 \simeq \ \frac{\mu^2}{2} \ . \tag{2.11}$$

Provided that the mean photon number sent from Alice is μ, Bob's detectors are perfect (i.e., 100% detection efficiency and no dark count), and the channel transmittance is *t*, Bob's photon detection probability is approximately μt, while Eve positioning just at Alice's output has a pulse having more than two photons with a probability of $\mu^2/2$. Then, the secret key rate under the PNS attack, *R*, is approximated as

$$R = \mu t - \frac{\mu^2}{2}. \tag{2.12}$$

This equation suggests that *R* is maximized when $\mu = t$, thereby *R* is proportional to (t^2). Here, *R* has a critical value for *t* at which no key is created due to system errors. This indicates that the PNS attack severely restricts the QKD transmission distance. Therefore, the BB84 protocol using a coherent light source needs some countermeasure against the PNS attack.

2.6.2 Decoy state method

The PNS attack severely degrades the system performance of the original BB84 protocol, as described above. To beat the PNS attack, the decoy state method was proposed [28, 58, 59]. It uses a signal source that emits a mixture of different mean photon-numbers instead of a fixed mean photon-number. For implementation of this scheme, Alice additionally equips an intensity

modulator that changes the intensity of coherent states emitted from her laser source, by which the mean photon number is arbitrarily chosen. One mean-photon-number is assigned to signal pulses carrying key information, while the others are assigned to decoy pulses to find the PNS attack. Eve does not know the mean photon number of each pulse, and conducts the PNS attack assuming the mean photon number of a signal pulse for any pulse. Then, the photon statistics in decoy pulses change, from which the eavesdropping is revealed [59]. In practice, Alice can emit one signal states (its mean photon number is $\mu_s \approx 1$), and two different decoy states, one is a deficient photon number ($\mu_{d1} < 1$) and one is vacuum ($\mu_{d2} = 0$) [60].

The decoy method beats the PNS attack and can be generally implemented in fiber systems as well as free-space systems [61, 62]. Currently, the decoy method is standardly employed in BB84 systems [63].

2.7 Phase-encoding BB84

The firstly proposed QKD protocol, called BB84, uses the polarization state of a single-photon for conveying key information. However, this scheme is not suitable for fiber-based QKD systems because the polarization state randomly changes during fiber transmission. Therefore, instead of polarization-encoding BB84, phase-encoding BB84 [11] is widely employed in current QKD systems, which does not suffer from the polarization state change in principle.

Figure 2.6 (a) shows the basic configuration of phase-encoding BB84, where Alice and Bob equip an asymmetric Mach-Zehnder interferometer with a phase modulator in one arm. Alice prepares two weak coherent pulses, where the first one is a reference pulse and the second one is a signal pulse onto which Alice's phase shift is imposed. Alice randomly selects the bit and the basis, and imposes one of four phase shifts $\{0, \pi/2, \pi, 3\pi/2\}$ onto her phase modulator according to the selected bit and basis. At the other end of the transmission, Bob selects one of two bases, and imposes one of two phases $\{0, \pi/2\}$ onto his modulator according to the selected basis. At the output of the Bob's interferometer, a photon can be detected at three time-slots, as illustrated in Fig. 2.6 (b). At the second time-slot, interference between the first and second pulses occurs, and one of the detectors clicks, depending on the relative phase of the two pulses. When the phase difference between Alice and Bob is $\{0, \pi\}$, which is a basis-matched case, the relative phase is

{0, π} and which detector clicks is deterministic. On the other hand, when the phase difference is {π/2, 3π/2}, which is a basis mismatched case, one of the detectors randomly clicks.

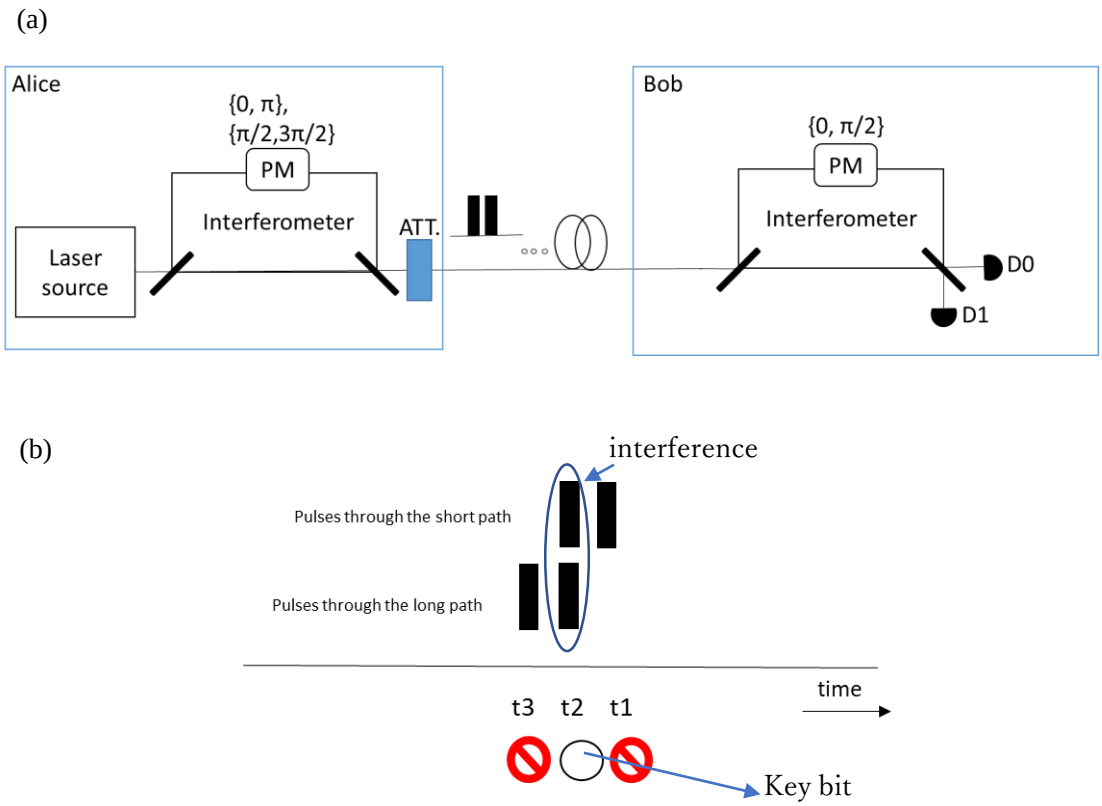

Fig. 2.6. Phase-encoded BB84 system. (a) Basic setup. PM: phase modulator; D0, D1: single-photon detectors; and Att. : attenuator. (b) Detection event at Bob.

After the quantum transmission is completed, Bob tells Alice the photon detection time and whether the MZI phase was 0 or π/2 at the detection. Alice then tells Bob whether her phase difference corresponding to Bob's detection was {0, π} or {π/2, 3π/2}. At this point, both Alice and Bob discard basis-mismatched events. Then, Alice creates bit "0" or "1" when her phase difference was {0, π/2} or {π, 3π/2}, respectively. Bob, on the other hand, creates bit "0" or "1", when D0 or D1 clicked. Alice's and Bob's binary bits created as above are identical and can form a secure key.

This scheme of the phase-encoded system has been widely used in QKD experiments, including a high rate experimental demonstration of over 1 Mbit/s secret key rate over 50 km [64].

2.8 Differential phase shift protocol

There are several QKD protocols other than BB84. Differential-phase shift (DPS) QKD is one of them. This section describes this protocol, because it is practical and the present thesis treats it. Figure 2.7 shows the configuration of a DPS-QKD system [12], where Alice prepares a sequence of weak coherent pulses whose phase is modulated by either $\{0, \pi\}$ for each pulse, and transmits it to Bob. The mean photon number in one pulse is less than 1 (e.g., 0.1–0.2). At Bob's site, the phase difference of neighboring pulses is measured with a one-pulse delayed Mach–Zehnder interferometer followed by photon detectors, where detector 0 or 1 (D0, D1) conclusively clicks when the phase difference is 0 or π, respectively. The detectors click irregularly owing to the low photon-number and the transmission loss. During the measurement, Bob records the photon-detection time and the detector that clicks.

Using the above setup, Alice and Bob create key bits as follows. First, Alice sends signal and Bob measures it, as described above. Then, Bob announces the photon detection time to Alice via a public channel. Referring to her modulation data corresponding to the detected time-slot, Alice creates key bits such that bits "0" and "1" from phase differences of 0 and π, respectively. On the other hand, Bob creates his key bits such that bits "0" and "1" from the clicks by "D0" and "D1", respectively. The bits created as above are identical between Alice and Bob, and can be a secret key.

The security of the above system is considered as follows. For example, Eve may conduct an intercept-resend attack against this system, using a copy of Bob's set up to measure Alice's signal. However, it is impossible for Eve to perform it without inducing Bob's bit errors, because the mean photon number sent from Alice is around 0.1 per pulse, which makes Eve impossible to measure all phase differences, but some of them. When Eve succeeds in the measurement, she resends a photon super-positioned over two pulses with the measured phase difference, while sending the vacuum state at the other time-slots because she has no information on them. When such two pulses arrive at Bob, he detects a photon possibly at three time-slots as shown in Fig. 2.8. At the second time-slot, interference correctly occurs, thereby no error in Bob's bit. For clicks at the other two time-slots, on the other hand, the detection result is random because no

interference occurs. This detection event can cause an error in Bob's bit, from which the eavesdropping is revealed.

The DPS-QKD protocol is robust against the photon number splitting attack, because the phase information is collapsed owing to the uncertainty relationship between the photon number and the phase, when Eve probes the photon number for picking up and storing extra photons. As a result, an error bit is induced at Bob [65], from which the PNS attack is revealed.

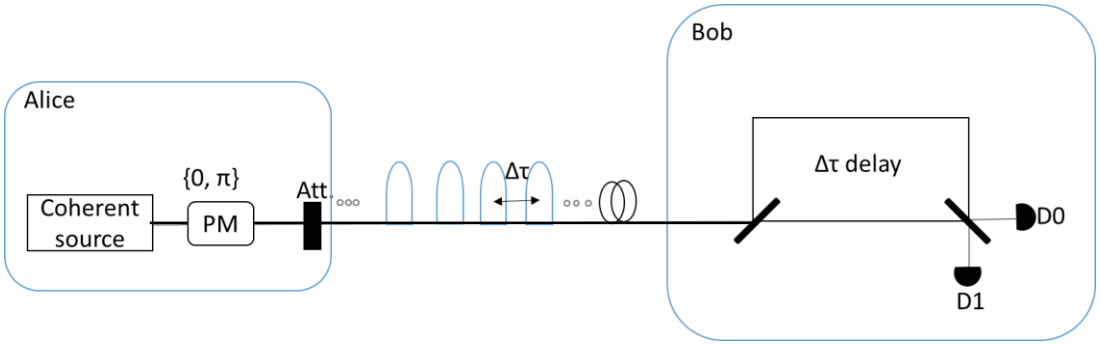

Fig. 2.7. DPS-QKD set up. PM: phase modulator; MZI: delay Mach–Zehnder interferometer; D0, D1: single-photon detectors; Att: attenuator, and Δτ : time interval between two adjacent pulses.

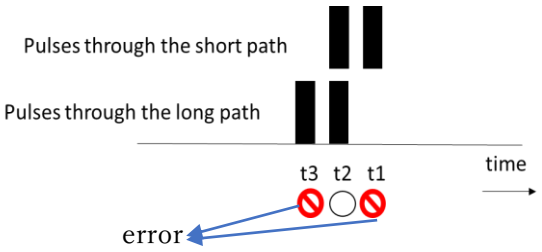

Fig. 2.8. Bob's detection when an intercept-resend attack is conducted against DPS-QKD.

2.9 Differential quadrature phase shift protocol

Phase-encoding BB84 is the most popular QKD scheme implemented over fiber-transmission systems. Differential quadrature phase shift (DQPS) QKD is a protocol that introduces the idea of DPS QKD to BB84. It uses a train of weak coherent pulses, not two pulses as in BB84, owing

to which the photon number splitting attack is prevented, and the time domain is efficiently used, resulting in a high key creation speed [12, 66]. Some conditional security analysis has been reported [67].

Figure 2.9 shows the configuration of DQPS-QKD. Alice sends a coherent pulse train that is randomly phase-modulated by one of four phases {0, π, π/2, 3π/2} for each pulse, whose mean photon number is less than one per pulse (e.g., 0.1–0.2). In this Alice's signal, the adjacent phase differences {0, π} and {π/2, 3π/2} correspond to two non-orthogonal bases, respectively, similarly to phase-encoding BB84. Bob receives Alice's signal through a delayed Mach-Zander interferometer (MZI) with a delay equal to the pulse interval of Alice's signal, where the phase in the longer arm is randomly switched with 0 or π/2 [Fig. 2.9 (a)]. Single-photon detectors (SPDs) count photons at the interferometer outputs. The 0 and π/2 phases in the MZI correspond to {0, π} and {π/2, 3π/2} basis measurements, respectively, i.e., active basis selection. In this setup shown in Fig. 2.9 (a), a phase modulator is inserted at the long arm in MZI, which is difficult to stably implement in practice. Instead of this setup, Bob can split the incoming signal into two delayed interferometers (MZI1, MZI2) whose path phase differences are 0 and π/2, respectively, followed by four SPDs, as shown in Fig. 2.9 (b). Photon detection at the outputs of MZI1 and MZI2 correspond to {0, π} and {π/2, 3π/2} basis measurements, respectively, i.e., passive basis selection. This setup includes no phase modulation in a MZI, enabling the stable operation, though two sets of the measurement system is necessary.

Using this setup, the key bit creation is conducted as follows. Bob counts a photon occasionally and randomly in time, where which detector clicks depends on the phase difference of adjacent pulses. After the quantum transmission is completed, Bob tells Alice the photon detection time and whether the MZI phase was 0 or π/2 at the detection. Alice then tells Bob whether her phase difference corresponding to Bob's detection was {0, π} or {π/2, 3π/2}. For each detected time-slot, Alice and Bob first discard basis mismatch events. Then, Alice creates bit "0" or "1" when her phase difference was {0, π/2} or {π, 3π/2}, respectively. Bob, on the other hand, creates bit "0" or "1", when D0 or D1 clicked in case of the active basis selection [Fig. 2.9 (a)], respectively, or when {D10, D20} or {D11, D21} clicked in case of the passive basis selection [Fig. 2.9 (b)]. Alice's and Bob's binary bits created as above are identical and can constitute a secure key.

The security of the DQPS-QKD is considered to be similar to BB84. In an intercept-resend

attack, for example, when Eve has a successful measurement, she resends two sequential pulses; Bob detects a photon at possible three time slots, the detection from the first or third time-slots induces an error in addition to the basis-mismatching error at the second time-slots as in BB84, from which Bob can reveal the eavesdropping in DQPS-QKD.

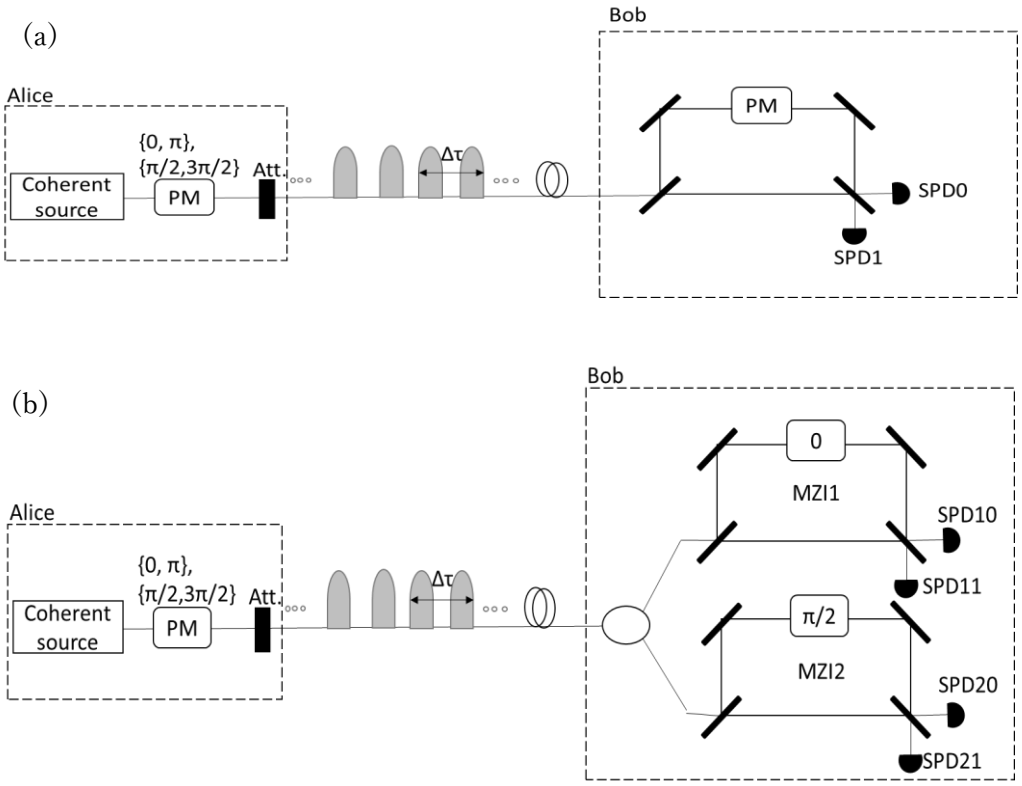

Fig 2.9. DQPS-QKD setup. (a): Active basis selection; and (b): Passive basis selection. PM: phase modulator, MZI: Mach Zander interferometer, and SPD: single-photon detector.

2.10 Summary

In this chapter, we firstly explained the general protocol of quantum key distribution (QKD), including the four steps to complete the secure key creation. Then, we discussed the theoretical security in general, where the three types of general attacks were introduced; individual, collective, and coherent attacks. Then, typical protocol called BB84 was described with its security. Against the original BB84, there is a powerful eavesdropping that seriously restricts the QKD performance,

i.e., photon number splitting (PNS) attack. This attack is introduced followed by a modified BB84 protocol to beat the PNS attack, which is widely employed at the present. Other QKD protocols, called differential-phase shift QKD and differential quadrature phase shift QKD, were also introduced, which are treated in the latter chapter in this thesis.

Chapter 3

Side-channel attacks against quantum key distribution systems

3.1 Introduction

The advantage of quantum cryptography over conventional cryptography is that, for quantum cryptography systems, there is a promise of provable security based on the law of physics. The ultimate security is achievable in theory [6, 9, 68, 69]. However, in practical implementation, it is questionable if the theoretical security is obtained.

The question for the practical security comes from a question if assumptions employed in the theoretical framework are actually satisfied. Indeed, for actually implemented systems, exploiting security loopholes is possible, especially loopholes resulting from imperfections in photon detectors. Such imperfections in actual devices open a door to tactical attacks called side-channel attacks. Several side-channel attacks have been proposed and demonstrated [70-83]. For quantum key distribution to be practical, it is desired to beat those side-channel attacks.

This chapter describes side-channel attacks against QKD systems. We first explain avalanche photodiode (APD) based single-photon detectors (SPDs), which is the main target of side-channel attacks, and then introduce typical side-channel attacks against QKD systems using APD-SPD. Previously proposed countermeasures against side-channel attacks are also described, followed by discussion and open problems. Finally, the summary is presented.

3.2 Single-photon detector

Single-photon detectors (SPDs) are the key component in single-photon based QKD, which severely determine the QKD performance. There have been considerable efforts to develop high-performance SPDs [84, 85]. There are typically two types of SPD; APD based and superconductor based ones. In this section, the former type is overviewed, because it is compact and low-cost, compared with the latter type, and widely employed in practical QKD systems, and also because it is relevant to this thesis.

The operation mechanism of an APD-SPD is as follow. First, an incident photon is absorbed and creates an electron-hole pair in an absorption layer of a semiconductor. With an electric field applied to the absorption layer, the excited electron and holes are driven in the opposite direction. When the electric field is large enough, these running particles acquire energies higher than the ionization energy of the semiconductor, which then generates additional electron-hole pairs through the collision with the lattice, causing an avalanche of charges. As a result, macroscopic current can be induced from an incident photon. This macroscopic current is converted to the voltage through a load resistance R_{basis} in a receiver circuit shown in Fig. 3.1.(a), when a sufficiently large bias voltage V_{HV} is applied across the APD.

An APD operates in two modes; the linear mode and the Geiger mode depending on the applied voltage. In the linear mode, where a moderate voltage is applied to an APD, the photocurrent is generated linearly proportional to the incident light power. In the Geiger mode, on the other hand, a high voltage is applied and an APD is sensitive to a single-photon, as described above. The voltage value at which the APD behavior transits between the linear and the Geiger modes is called breakdown voltage. For detecting single-photons, an APD is usually operated in the Geiger mode, in which an APD is reversely biased above the breakdown voltage. APD-based SPDs can be either passively or actively quenched by photon detection; the APD voltage drops below the breakdown voltage just after an avalanche occurs, by which the avalanche is reset. Figure 3.1(b) and its caption describe the operation of an APD.

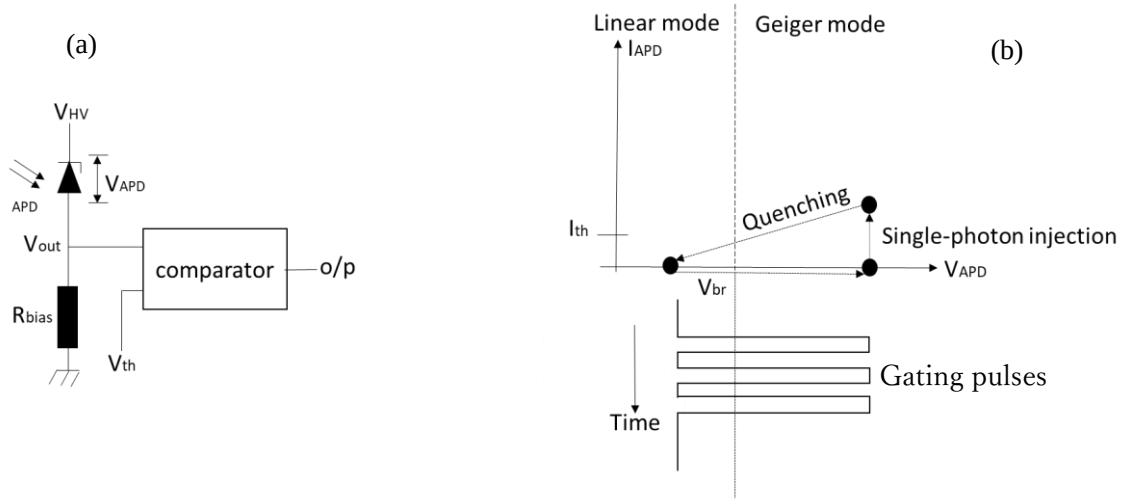

Fig. 3.1. APD used as a single-photon detector. (a) A typical receiver circuit. The reverse voltage (V_{HV}) is applied to an APD, which is connected to the ground via a load resistor R_{bias}. Through the load resistor, the output voltage V_{out} is induced. (b) Photo-current I_{APD} as a function of the applied voltage in an APD. In Geiger mode, a voltage larger than the breakdown voltage (V_{br}) is applied to APD, during which single-photon incidant induces a large photo-current. A click is reported when the output voltage (V_{out}) exceeds the comparator threshold V_{th}. After that, the APD voltage (V_{APD}) goes back below the breakdown voltage in a linear mode where the output voltage V_{out} responds linearly to the incident optical power.

The dark count, which is a false detection event, is crucial in SPDs based on an InGaAs/InP APD, that are usually used in fibre-based QKD systems because of their sensitivity to the fibre communication wavelength band. Those semiconductor devices have a high density of impurities, which causes a high dark-count rate. One solution is to switch them to the Geiger mode from the linear mode by applying a gating voltage pulse (gating) as illustrated in Fig. 3.1 (b), only when a photon is expected.

One crucial parameter determining the dark count property is temperature. A thermally excited electron causes a dark count, and the excitation probability is strongly dependent on the device temperature, such that a lower temperature results in a lower dark count rate. However, a low temperature causes another problem called "after-pulse". An InGaAs/InP APD has a large number of impurities, as described above, whose energy levels can trap electrons left in the conduction band after an avalanche occurs. Then, with the next gating voltage, the trapped electron is excited, induces an avalanche, and causes a detector's click, even when there is no incident photon. This fake photon count is called after-pulse. The after-pulse restricts the repetition rate of gating pulses,

such that the pulse interval should be longer than the lifetime of a trapped electron staying at an impurity's energy level. This lifetime depends on the device temperature, i.e., low-temperature results in a long lifetime. Therefore, a low temperature restricts the gating frequency. Some techniques to improve the gating frequency of APD based SPDs have been proposed, solving the above problem [86-89]. One solution uses a very short gating pulse with a voltage slightly above the breakdown voltage, so that the avalanche current is reduced and the after-pulses probability is small.

3.3 Side-channel attack

In this section, side-channel attacks are introduced, that take advantage of imperfections in practical systems [90, 91].

3.3.1 Detector efficiency mismatch

As mentioned in the previous section, APD-based SPDs are operated in the Geiger mode to be sensitive to single-photon receipt. For reducing the dark count rate, they are switched to the Geiger mode for a short time by a gating pulse, while being in the liner mode outside that gating time window. Here, quantum cryptography protocols require more than two detectors to obtain two different bit values, and thus, precise synchronization is needed for the detectors to have identical gating time when the pulse shape is not ideal rectangular. Mismatch in the gating time, as well as imperfections in the manufacturing process, results in a detector efficiency mismatch [33], which opens a door for an attack utilizing the mismatch in the gating time between detectors. There have been several reports showing the possibility of utilizing this loophole [37, 92]. In addition, Eve may intentionally create such efficiency mismatch by manipulating the signal timing at each detector [73]. Although one may suggest using one detector in a time-multiplexing system to avoid such a loophole, the detection window for each bit can also be tricked, and therefore the same attack can be carried out.

The attack utilizing the detector efficiency mismatch, which is a kind of intercept-resend attack, is as follow. Eve measures signal coming from Alice with a randomly chosen basis and obtains a

measurement result. Afterwards, she resends a fake signal with a bit value opposite to her measurement result on the other basis. Eve's fake signal is resent so that it reaches Bob's detectors at a time when the detector corresponding to her measurement result has much higher detection efficiency than the other one. To understand how Eve can obtain a bit value, let's assume the extreme case where the timing manipulation makes one detector blind due to zero detection efficiency and the other one clickable. In such a scenario, when Eve measures Alice's signal successfully, she resends fake signal that can be detected only when Bob chooses the same basis as Eve, otherwise no click is registered at Bob's detectors due to the blinding of one detector. Therefore, in this extreme case of efficiency mismatch, Eve can have full information about a key. However, when one detector is not completely blinded in this attack, Eve introduces quantum bit error rate (QBER) depending on the efficiency mismatch between two detectors. For example, she introduces about 11% QBER if the efficiency is reduced to be 0.066 [33], from which the eavesdropping can be revealed. However, it might be possible for Eve to utilize a combination of partial detector efficiency mismatch attack and general individual attacks to keep her additional QBER below 11% when the efficiency is less than 0.25 [93].

There is another strategy utilizing the detector efficiency mismatch called *time-shift attack* where no fake signal is resent [34]. Eve randomly manipulates the arriving time of Alice's signal at Bob's detectors on her desire by, for example, introducing an additional delay. Eve can obtain partial information from Bob's announcement such that, when Bob announces a receipt of a photon at a given time, it is more likely to be detected by the detector that is chosen by Eve. No additional QBER is introduced in this attack. A fault of this time-shift attack is that Eve does not have full key information. This side-channel attack was experimentally conducted, demonstrating that a commercial QKD system was vulnerable to this attack [37].

Against the above eavesdropping, some countermeasures have been proposed. The most popular one is four-state Bob, which is a modification from the phase-encoding BB84 such that Bob uses four phases $\{0, \pi/2, \pi, 3/2\pi\}$ instead of two $\{0, \pi/2\}$ in the basis selection [33, 34, 94]. The additional two phases allow Bob to not only randomly choose the measurement basis, but SPD for bit "0" or bit "1". In the public announcement, Bob announces his basis choice, while keeping his choice of detector (for bit "0" or "1") secret. This countermeasure prevents Eve from having key bit information, even if she knows about the detector's click. QKD system with four

states has been proven to be secure against the detector efficiency mismatch attack assuming an ideal single photon source [95], though the assumption of ideal single-photon receipt is impractical. It should be mentioned that Bob's using four-state is effective only to the time-shift attack [96].

3.3.2 Trojan-horse attack

Trojan-horse attack is another type of side-channel attack, which was proposed in [31, 32]. Its idea is that Eve uses a powerful probe laser to access Alice's sites. Phase-encoding QKD systems equip a phase-modulator at Alice, into which Eve injects an intense light from the outside. Then, the back-reflection from the phase modulator can reveal the phase imposed onto the modulator, from which Eve obtains key information. Countermeasures against this attack include use of a narrow band-pass filter because the probe light wavelength should be different from the QKD signal, use of a beam splitter followed by a power meter to monitor incident light to Alice, and use of an isolator at the entrance to prevent light incident from the outside.

3.3.3 Detector control attacks

Detector control attack is one of the most severe side-channel attacks against real QKD systems, because it has been implemented and full key was obtained without being detected [97]. This is a kind of intercept-resend attack, which works as follows for phase-encoding BB84. Eve firstly sends a bright illumination onto Bob's APD-based SPDs outside the gating time window in the linear mode, and generates a large photocurrent by which the APD basis voltage is reduced through the voltage drop due to the load resistor. Here, the illumination is sufficiently intense for the reduced bias voltage to be so low that the APD voltage does not exceed the breakdown voltage when a gating pulse is applied as shown in Fig. 3.2. This stage is called *blinding* detectors. The blinded condition lasts for a while after the bright illumination, because of a finite recovery time of an APD circuit, during which the detectors are insensitive to single-photons.

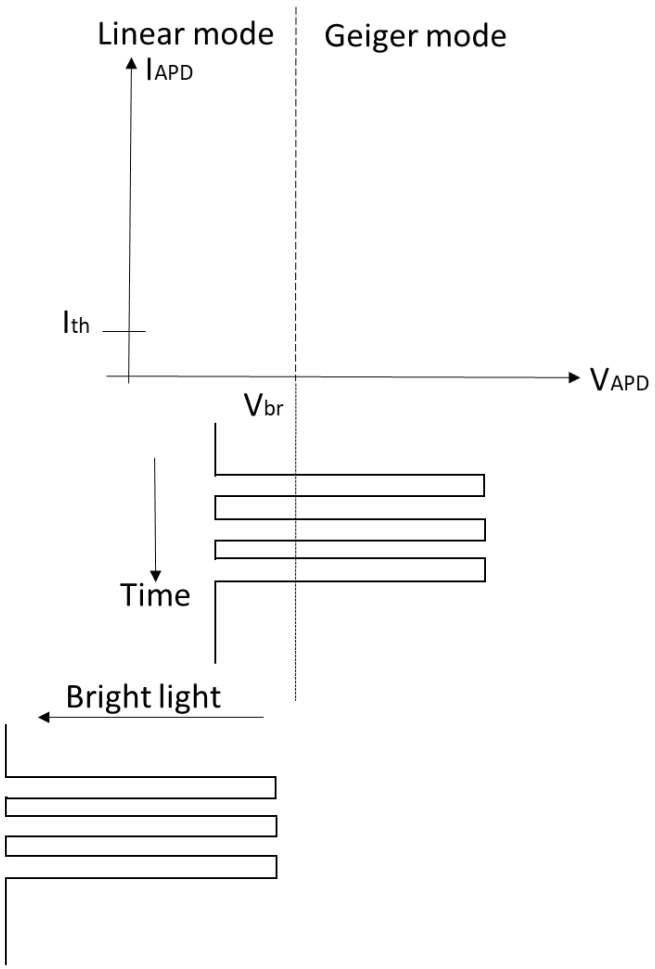

Fig. 3.2. The effect of the bright illumination onto APD-SPD.

When Eve successfully measures Alice's signal in an intercept-resend attack, she resends a fake signal within the blinded period. Here, she sends two optical pulses with a power level P_o for each, which is chosen so that Bob's detector in the linear mode records a detection event when P_o is incident, but never reports detection for $P_o/2$. Figure 3.3 illustrates how Bob's setup works against this attack. Alice's two pulses reach Bob's detectors at three time-slots after MZI. At first and third time-slots, there is no interference and the incident power is not enough to make click. The interference occurs at the middle time-slot only. When Alice's, Eve's, and Bob's bases are identical, Alice's and Bob's bits are matched while Eve has the same bit as theirs, as shown in Fig. 3.3 (a). This is because Eve's pulses have a correct phase difference, and the power level goes to a correct detector at the middle time position is P_o, making the detector report a photon

count. Eavesdropping succeeds without being noticed in this case. On the other hand, when Alice's and Bob's bases are matched but Eve's is not, Eve's pulses go to both Bob's detectors with a power level of $P_o/2$ for each at the middle time position, which register no detection event, as shown in Fig. 3.3 (b). Bob does not create a bit, and no bit error is introduced in this basis mismatch case, unlike in a conventional intercept-resend attack against BB84. This attack reduces Bob's total photon detection rate by 50% because there is no click in the basis mismatched case. Nevertheless, Eve may position just at Alice's output and compensate for the photon loss in the basis-mismatched case by replacing the transmission line with a lossless one. Importantly, this attack, capturing full key information while introducing no bit error at Bob, can be carried out with the current technologies. This detector control attack is also effective against polarization encoding BB84, SARG04, COW, DPS-QKD, and DQPS-QKD protocols [98]. The attack against DQPS and DPS is described in detail in Chapters 4 and 6, respectively, where a countermeasure against the attack is proposed and evaluated for each protocol. The blinding and control attack has been experimentally demonstrated against commercial QKD systems [42]. Since then, it became a crucial issue for the QKD security in the real world. Therefore, it is believed to be the strongest and most realistic side-channel attack, for which a countermeasure is desired.

The detector blinding attack can be performed with moderate power of Eve's injection, and thus a countermeasure of Bob monitoring the incident optical power alone may not be effective to reveal this attack [72].

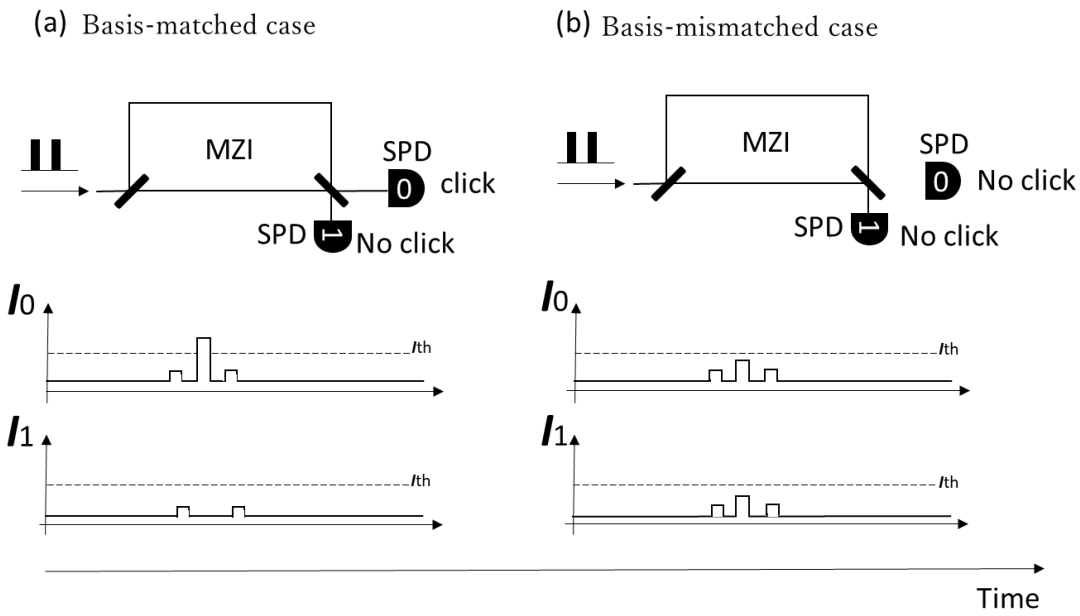

Fig. 3.3. Detector blinding attack against active basis selection system. The upper diagram is Bob's setup and the lower one illustrates the photocurrent at Bob's detectors. MZI: delayed interferometer, I_0, I_1 photo-current induced at detectors 0 and 1, respectively. (a) When Eve's and Bob's bases are matched, the full pulse hits one detector with P_o. (b) When Eve's and Bob's bases mismatch, the pulse equally hits both Bob's detectors with P_o /2 and no detection event is registered.

3.4 Countermeasure against side-channel attacks

3.4.1 Measurement Device Independent (MDI) QKD

In order to beat side-channel attacks, especially that manipulate Bob's detectors, measurement device independent (MDI) QKD was proposed [45], which has been intensively studied since then. In this protocol, both two legitimate parties (i.e., Alice and Bob) send signals, and an untrusted third party (Charlie) performs a measurement, namely Bell state measurement, on Alice's and Bob's signals, as shown in Fig. 3.3. Alice and Bob have no detector, thus there is no way of side-channel attack manipulating Bob's detectors. Charlie has detectors instead, but manipulating his detectors does not provide any key information to Eve, as described below. Far

from that, it does not matter if Charlie is taken over by Eve.

The MDI-QKD protocol operates as follow. Alice and Bob respectively prepare one of four BB84 states and send them to Charlie who is located at the middle between Alice and Bob. Charlie performs Bell state measurement (BSM), which is a joint quantum-mechanical measurement on two quantum states based on a kind of quantum interference, and determines the relationship between the two states. The measurement result provides the relationship between Alice's and Bob's signals. It should be noted that BSM determines only the relationship between the two quantum states but not the states themselves. After the quantum transmission, Charlie announces his measurement results to Alice and Bob through a public channel. From Charlie's information, Alice and Bob know the relationship between their signals and identify the other party's signal, referring to their own signals, then create an identical bit. The created bit is unknown to the third party (even Charlie), because Charlie does not measure the states themselves. It should be noted that a key bit is created from the combination of Charlie's measurement and Alice's/Bob's signal. Thus, manipulating Charlie's detectors alone gives no key bit information to Eve.

When the MDI-QKD protocol was proposed, it attracted researchers as a QKD protocol free from side-channel attacks manipulating SPDs. In addition, MDI-QKD offers a benefit of doubling the QKD distance, because Charlie positions at the middle between Alice and Bob and thus the QKD distance is double the photon transmission distance. However, a drawback is that its implementation is difficult in practice. In order to successfully perform BSM, photons sent from Alice and Bob should be indistinguishable, and some synchronization should be established between them in term of, for example, the temporal position, the polarization state, and the spectrum shape. Stable implementation of such synchronization is not easy in practice.

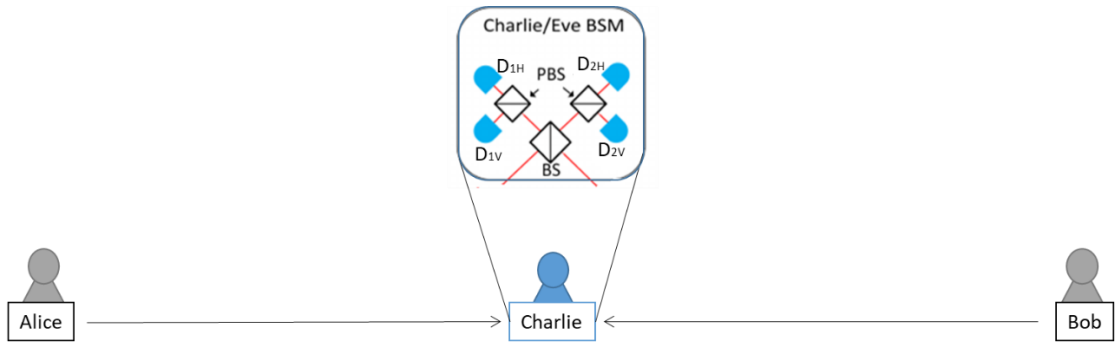

Fig. 3.3. The configuration of measurement device independent QKD against polarization-encoding BB84. Alice and Bob prepare states and send them to Charlie at the middle between Alice and Bob, who performs Bell state measurement (BSM) shown in the inset above Charlie. BS: beam splitter; and PBS: polarization beam splitter; and D_{1H}, D_{2H}, D_{1V}, D_{2V} : single-photon detectors.

3.4.2 Other countermeasures

In the previous section, a QKD protocol free from side-channel attacks manipulating single-photon detectors is described. However, its implementation is challenging, and thus researchers search for practical solutions to counter specific side-channel attacks. In this section, practical countermeasures against blinding and control attack are presented.

There have been several proposals of practical countermeasures against the blinding and control attack, that is the most powerful side-channel attack [83, 99, 101]. This attack has two steps: (i) Eve blinds Bob's detectors by injecting bright light, and then (ii) controls the detectors such that they behave as Eve wishes, i.e., click and no click when Eve's and Bob's basis are matched and mismatched, respectively. A straightforward countermeasure is to monitor whether detectors are blinded or not by measuring, for example, a fraction of the optical power incident to Bob [83] or the photo-current flowing through the detector circuit [99]. However, this countermeasure is feasible under the condition that how Bob's detectors response to Eve's blinding light is provided, i.e., how much power is required for blinding or how much photo-current is flown when blinded. Therefore, it depends on the properties of each device and is not a general solution to guarantee the security irrespective of detectors.

Another way to monitor the status of a single-photon detector is use of known light, such that the single-photon sensitivity is occasionally checked by injecting faint pulses from a calibrated

light source inside Bob [42]. However, this scheme requires additional apparatus, and spends the measurement time during which key bits are not created, resulting in reduction of the key generation rate.

A detector circuit robust against the blinding attack was also proposed [100]. With a low bias-resistance in the detector circuit, the voltage drop is small, and thus the detector is not blinded even when bright light is incident. However, this scheme is not a general solution available to any detector. Besides, it may sacrifice the detector performances such as the response time and the detection efficiency. Other than the above, some countermeasures were proposed and demonstrated using an asymmetrical coupler followed by two identical receiver setups [101]. However, they require additional equipment, which makes the system complex and costly.

3.5 Summary

In this chapter, we described side-channel attacks against QKD systems. Several specific attacks were introduced, especially detectors blinding and control attack. Some countermeasures previously proposed were also introduced, including a novel QKD protocol named MDI-QKD, that is free from attacks manipulating detectors in principle but not easy to implement in practice, and schemes monitoring the status of detectors, that is practical but device-dependent.

In view of such a situation, this thesis presents alternative countermeasures, which is practical and device-independent, in the following sections.

Chapter 4

A countermeasure against side-channel attack in four-state QKD systems utilizing discarded events

4.1 Introduction

In Chapter 3, we describe side-channel attacks against QKD systems. Countermeasures against them are also described, as well as their issues such that practical implementation is not easy (in case of MDI-QKD) or they are not a general solution independent of detector's properties. Therefore, this thesis proposes novel countermeasures against side-channel attacks which is simple and independent on device properties. This chapter especially treats four-states QKD systems such as BB84 and DQPS-QKD [82].

The chapter is organized as follows: Section 4.2 describes the side-channel attack against the DQPS-QKD protocol; Section 4.3 presents how to find the eavesdropping; Section 4.4 presents an experiment and simulations on the system performance, confirming the feasibility of the proposed scheme; and Section 4.5 presents discussion and summary.

4.2 Detector blinding and control attack against DQPS-QKD

In Chapter 3, a side-channel attack called detector blinding and control attack against BB84 is introduced. This attack is also applicable to DQPS-QKD described in Section 3.3.3. In conventional DQPS-QKD, a bit error can be induced when Eve conducts an intercept-resend attack with basis-mismatched measurement, as in BB84, from which the eavesdropping is revealed. Moreover, in an intercept-resend attack, when Eve has a successful measurement, she resends two sequential pulses, Bob detects a photon possibly at three time slots, and the detection at the first or third time-slot can induce an error in addition to the above basis-mismatching error, from which Bob can reveal the eavesdropping. The blinding attack can suppress such unwanted Bob's click, and is effective against DQPS-QKD.

4.3 Monitoring coincident clicks

To prevent the detector blinding and control attack against BB84 using weak coherent light or DQPS-QKD, this thesis proposes to monitor coincident clicks to find the eavesdropping. Practical BB84 and DQPS-QKD systems use a coherent light source, whose photon number follows a Poisson distribution, having a finite probability of including more than two photons per pulse. In the protocol, they utilize two sets of non-orthogonal bases (four states in total) for the security, where 50% of detection events are basis-mismatched and discarded. These basis-mismatched detection events are utilized for finding the eavesdropping in our proposed scheme. It needs no additional equipment, but just post data-processing, featuring the simplicity in term of hardware.

Our countermeasure against the detector blinding attack is as follow. In BB84 or DQPD-QKD under the normal condition, two detectors can simultaneously count photons, i.e., coincident clicks, in basis-mismatched measurement, because a photon goes to either detector with an equal probability, as indicated in Table 2.1 in Chapter 2, and there can be multiple photons at one time-slot according to a Poisson distribution. However, when Eve performs the detector blinding and controlling attack, Bob's detectors are blinded, or just one targeted detector clicks, and thus no coincident click occurs. Therefore, Bob can notice Eve by monitoring coincident click in basis-mismatched measurement, prohibiting the eavesdropping.

One may ask if it is possible to cheat this countermeasure. To answer this question, let us consider a possible scheme of Eve's cheating strategy. To cheat the Bob's monitoring, Eve should induce a coincident click by, for example, sending incoherent pulses with a high power level, for which no interference occurs and two detectors equally click. However, coincident click by incoherent light occurs in basis-matched measurement as well as basis-mismatched one, whereas coincident clicks should occur in basis-mismatched measurement under the normal condition. Thus, Eve's strategy of intentionally inducing coincident is revealed from coincident click in basis-matched measurement.

It should be noted that our countermeasure of monitoring coincident click is effective not only for the bright illumination attack but also for other side-channel attacks. For example, in the time-shift attack or the detector efficiency mismatch attack [2,3], described in Section 3.3, where Eve shifts the pulse arrival time at Bob so that one of his detectors has a much lower detection efficiency than the other (ideally totally blinded). Coincident counts under this attack are much smaller than those in normal conditions. Therefore, Bob can reveal the eavesdropping.

The advantage of our scheme is that its implementation is much easier than MDI-QKD, that is widely studied to beat side-channel attacks these days. An advantage of MDI-QKD, on the other hand, is that it is generally secure against side-channel attacks manipulating single-photon detectors, while our scheme aims at specifically preventing the blinding illumination attack, that is known as the strongest side-channel attack, the time-shift attack, and the detector efficiency mismatch attack. Besides, MDI-QKD offers a benefit of doubling the QKD distance.

Ideally, Bob can find the eavesdropping when the coincident count is lower than the value estimated from system conditions such as the transmission distance and the detector efficiency. In practice, however, the coincident counts fluctuate because of a finite monitoring time. Eve can partially conduct the eavesdropping, utilizing this fluctuation. Therefore, when the measured coincident count is lower than the expected value, Bob attributes the reduction to partial eavesdropping, and excludes the information amount possibly leaked to Eve from a raw key by privacy amplification. Taking this partial side-channel attack into account, the final key length, *R*, for BB84 is expressed as

$$R_{BB84} = R_{shit}\left\{1 - \left(\frac{P_{est}^{(c)} - P_{meas}^{(c)}}{P_{est}^{(c)}}\right) - \tau - f(e)\left[e\ \log_2 e + (1-e)\log_2(1-\ e)\right]\right\},$$

(4.1)

and it is expressed for DQPS-QKD assuming the general individual attack [53] as

$$R_{DQPS-QKD} = R_{shit}\left\{1 - \left(\frac{P_{est}^{(c)} - P_{meas}^{(c)}}{P_{est}^{(c)}}\right) - (1 - 2\,\mu\,)\log_2\left[0.75 - \frac{e^2}{8} - \frac{(1-3e)^2}{4}\right] - f(e)[e\ \ \log_2 e + (1-e)\log_2(1-\ \ e)]\right\}, \tag{4.2}$$

where R_{sift} is the sifted key rate, τ is the data compression factor given by Eq. (2.3), $P_{est}^{(c)}$ is the expected coincident count, $P_{meas}^{(c)}$ is the measured coincident count, μ is the average photon-number sent from Alice, e is the system error rate, and $f(e)$ is a factor representing the error correction efficiency.

4.4 Number of coincident counts

4.4.1 Theoretical estimation

The previous section presents an idea of utilizing coincident counts in basis-mismatched measurement to reveal the side-channel attacks. However, it is questionable to have a sufficient number of the coincident count in practice, especially in long-distance systems where the mean photon number received by Bob is small. Therefore, an evaluation of the coincident counts in practical BB84 or DQPS-QKD systems is presented in this section.

The probability of more than one photon being included in one coherent pulse with a mean photon number of n is given by $P(n) \approx n$ for $n << 1$. In basis-mismatched measurements in the active basis selection, a coherent pulse with $n = 0.5\mu T$ goes to each detector, where μ is the average number of photons per pulse sent from Alice and T is the transmittance from Alice to Bob including Bob's apparatuses. Thus, taking the detection efficiency η and the detector's dark count rate D into account, the coincident probability $P^{(c)}{}_{est}$ in basis-mismatched measurement is:

$$P^{(c)}{}_{est} = \{P(0.5\mu\eta T) + D\} * \{P(0.5\mu\eta T) + D\} \quad (4.3)$$
$$= (0.5\mu\eta T + D)^2$$
$$= 0.25\ (\mu\eta T)^2 + \mu\eta T D + D^2.$$

In the passive basis selection, Bob detects photons by four SPDs at the outputs of two MZIs corresponding to the two measurement bases for each as shown in Fig. 2.9 (b). The probabilities of each SPD clicking for a signal with a mean photon-number of *n* per pulse in this system are summarized in Table 4.1.

Table 4.1. Detection probabilities in passive basis selection in DQPS-QKD. *n*: average photon-number.

The phase difference of received pulse

SPD number	**0**	**π**	**π/2**	**3π/2**
D10	0.5*n*	0	0.25 *n*	0.25 *n*
D11	0	0.5 *n*	0.25 *n*	0.25 *n*
D20	0.25 *n*	0.25 *n*	0.5 *n*	0
D21	0.25 *n*	0.25 *n*	0	0.5 *n*

There are several combinations of two detectors clicking at one time-slot. The total probability of coincident clicks is as follows. For a phase difference of 0, for example, coincident clicks occur between D10 and D20, D10 and D21, or D20 and D21, with probabilities of $P(0.5n) * P(0.25n) *\{1 - P(0.25n)\}$, $P(0.5n) * P(0.25n) * \{1 - P(0.25n)\}$, $P(0.25n) * P(0.25n) * \{1 - P(0.5n)\}$, respectively. Subsequently, the coincident probability in passive basis selection systems is expressed by

$$P_{est}^{(c)} = 2 * \{P(0.5n) + D\} * \{P(0.25n) + D\} * \{1 - P(0.25n)\}$$
$$+\{P(0.25n) + D\} * \{P(0.25n) + D\} * \{1 - P(0.5n)\}$$
$$= \{0.25(\mu\eta T)^2 + 1.5\mu\eta TD + 2D^2\}\{1 - 0.25\mu\eta T\}$$
$$+\{0.25\mu\eta T + D\}^2 * \{1 - 0.5\mu\eta T\}. \quad (4.4)$$

4.4.2 Experiment

We experimented to confirm the feasibility of monitoring coincident clicks, whose setup is shown in Fig. 4.1. A coherent pulse train was created by intensity-modulating (IM) continuous-wave light from a laser source (wavelength 1550 nm). The pulse width and interval were 200 ps and 5 ns, respectively. The pulse sequence was attenuated to be 0.2 photons per pulse on average to simulate Alice's signal.

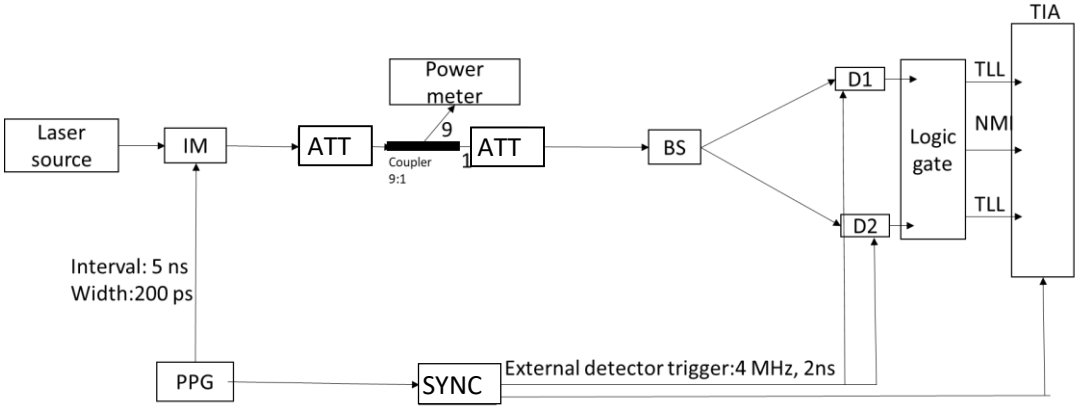

Fig. 4.1. Experimental setup for measuring coincident count. IM: intensity modulator; ATT: attenuator; BS: beam splitter; PPG: pulse pattern generator; TIA: time interval analyzer; D1, D2: single-photon detectors; and SYNC: synchronization source.

The signal light was passed through a variable attenuator (ATT) that simulated the transmission loss, and then was divided and coupled into two photon detectors (D1, D2) via a 50:50 beam splitter (BS). We used APD-based SPDs (IdQuantique: ID200) as photon detectors, whose detection efficiency and dark count rate were 10 % and 300 Hz, respectively. The APDs were

gated at 4 MHz with a time window of 2.5 ns. Under this operating condition, one gating window accepted one optical pulse. The detectors' outputs were input to a time interval analyzer (TIA) via a logic gate, where the detection time and which detector clicked were recorded. The TIA was set to scan over 1.2 μs in one measurement.

Using the above setup, we measured the coincident count for several attenuation levels that simulated the transmission loss. The result is shown in Fig. 4.2, where the measured number of total and coincident clicks are donated by circles and triangles, respectively. In the figure, the calculation result by Eq. (4.3) with parameters of μ = 0.2, detection efficiency = 10%, and dark rate = 300 Hz, which correspond to this experiment is also plotted by the dotted line. The experimental and calculation results are consistent, confirming our theoretical estimation. In addition, the results show that it is possible to obtain enough counts in practice, indicating our countermeasure is feasible.

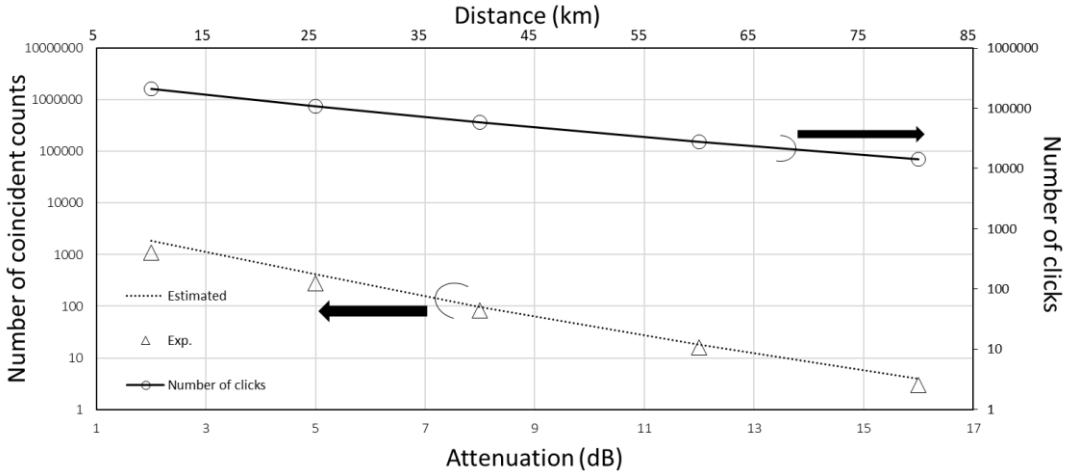

Fig. 4.2. Number of clicks as a function of attenuation. Triangle represents the measured coincident click; the circle represents experimental results of the total click; dotted line represents the estimated coincident counts.

4.5 Simulations

Based on the previous section, we estimated the number of coincident counts in BB84 transmission systems employing active and passive basis selection setups, using Eqs. (4.3) and (4.4), respectively. The effectiveness of the proposed scheme is strongly dependent on the SPD

performance. Therefore, two product models of a SPD were assumed; IdQuantique ID200 and IdQuantique ID 210, their characteristics are listed in the table 4.2.

Table 4.2. Characteristics of Single-photon detector.

	IdQuantique ID200	**IdQuantique ID 210**
Detection efficiency	10 %	25 %
Gating frequency	4 MHz	100 MHz
Dark count rate	300 Hz	30 Hz

The former model is one we have in our laboratory, and the latter is the latest model released from the same manufacture.

Figures 4.3 and 4.4 show the simulation results of the number of counts as a function of the attenuation corresponding to the transmission loss for active and passive basis selection setups, respectively. In the figures, the solid line plots the total number of clicks obtained in the experiment. The dotted line is the coincident count with ID 200 and the broken line is that with ID210.

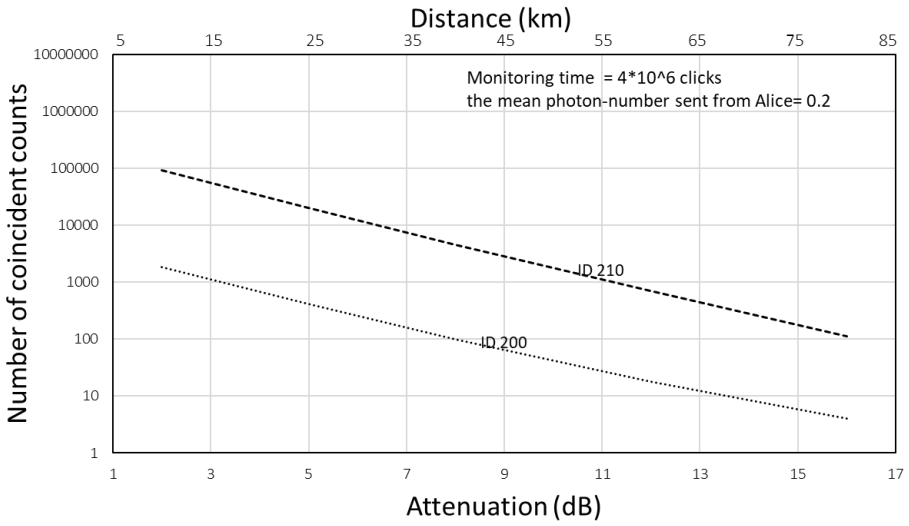

Fig. 4.3. The number of clicks as a function of attenuation in active basis selection system. The circle represents the experimental results of the total click. The dotted line represents estimation result assuming SPD (ID200) used in the experiment, whose dark count rate = 300Hz, gating frequency = 4 MHz, and detection efficiency = 10 %. The broken

line represents estimation results assuming ID210 detector model with dark count rate = 30 Hz, detection efficiency = 25 %, and gating frequency = 100 MHz, the transmission loss is assumed to be 0.2 dB/km.

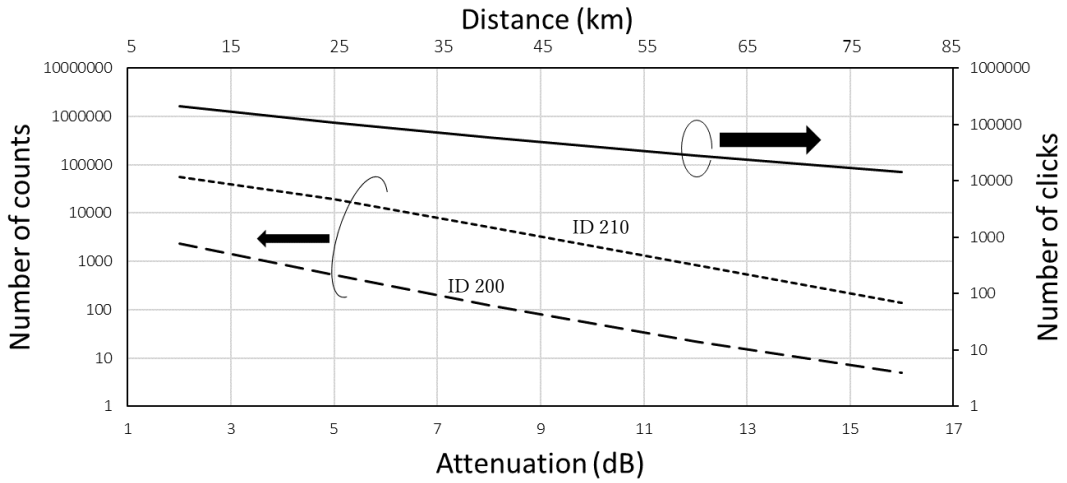

Fig. 4.4. The number of coincident counts as a function of attenuation in passive basis selection system.

Figs. 4.3 and 4.4 shows that the coincident count is obtainable within the feasible quantum protocol distance, these coincident counts are inversely proportional to the distance due to the attenuation. The table 4.3 below shows that larger number of coincident counts is expected at longer distance in passive basis selection systems thanks to the use of four SPDs, enhancing the feasibility of our scheme to find the side-channel attack.

Table 4.3. Coincident counts for active and passive systems using two different SPD models

Distance(km)	Active system		Passive system	
	ID200	ID210	ID200	ID210
40	98	4591	123	5194
60	18	700	22	850
80	4	113	5	140

4.6 Summary

In this chapter, we proposed a countermeasure against the detector blinding and control attack for BB84 and DQPS-QKD. The proposed countermeasure utilizes coincident clicks in basis-mismatched measurements, which are normally discarded, to monitor the existence of eavesdropping. Any reduction in the expected number of coincident clicks is assumed to be due to Eve's attack. We also discussed the effect of photon-number fluctuation on the system performance. The simulation and experimental results showed the feasibility of implementing our countermeasure in four-states QKD protocols.

Chapter 5

Experimental demonstration of BB84 and DQPS systems with a countermeasure against side-channel attacks

5.1 Introduction

Chapter 4 proposes a countermeasure against side-channel attacks in QKD protocols using four states, i.e., BB84 and DQPS-QKD. This chapter presents experimental demonstration of BB84 and DQPS systems with the proposed countermeasure.

In four-state based QKD, the receiver should equip a setup functioning the basis selection, for which there are two choices: active selection and passive selection. The former actively switches the condition of one measurement system. The latter prepares two measurement systems corresponding to two non-orthogonal bases for each, which are passively selected by a beam splitter. Conventional QKD experiments usually employs the latter scheme because of its stable operation. In contrast, we try to perform the former scheme in this thesis because it needs just one measurement system. However, there is a problem in implementing the active basis selection. That is polarization fluctuation induced through fiber transmission. In active basis selection, an optical modulator is used to switch the measurement condition, which usually has polarization dependency. Thus, fluctuation of the polarization state of the received signal prevents the stable operation of the basis selection. In this chapter, we introduce a novel active basis selection scheme insensitive to the polarization state, and demonstrate its stable operation.

This chapter organized as follow. First, the polarization problem in the active basis selection is explained. Second, our proposed circuit is described. Then, QKD experiments using the proposed

receiver setup with countermeasure against side-channel attacks is presented, followed by summary.

5.2 Active basis selection

Figure 5.1 shows the conventional setup of the active basis selection for phase-encoding BB84. Bob's receiver consists of a Mach-Zhender interferometer with a phase modulator placed on one of interferometer arms, which imposes Bob's phase choice onto a half of Alice's pulses. With this setup, Alice's two pulses arriving at Bob, composed of a reference pulse and a signal pulse for which Alice's phase is imposed, are split into two paths, onto one of which Bob's phase is imposed, and are recombined with one-pulse shift. Then, interference occurs between the signal and reference pulses at the recombining beam splitter at the middle time-slot, whose relative phase is determined by Alice's and Bob's phases. Here, Bob's phase is chosen either 0 or $\pi/2$. Then, in case that Alice's phase is $(0, \pi)$ or $(\pi/2, 3\pi/2)$ and Bob's phase is 0 or $\pi/2$, a photon is deterministically counted by one of the two detectors, respectively. Namely, $(0, \pi)$-basis and $(\pi/2, 3\pi/2)$-basis measurements are selected by Bob's phase of 0 and $\pi/2$, respectively. This active basis selection scheme enables a simple receiver setup, as it requires a single measurement system. However, its practical implementation has some problems, as described below.

The stability of the system is mainly determined by the interferometer, i.e., stable interference between two pulses passing through the long and short arms, respectively, is required. In the setup shown in Fig. 5.1, the length of the long interferometer arm includes a phase modulator which is usually module-packaged with fiber pigtails. Thus, it is not easy to accurately and stably set the optical length as required, resulting in unstable interference. Moreover, a phase modulator is polarization-dependent, for which the polarization state of incident signal randomly changes through fiber transmission, mainly due to the birefringence of the fiber resulting from stress or asymmetry in the fiber fabrication and installation. For practical QKD systems, a stable and polarization-insensitive active basis selection scheme is desired.

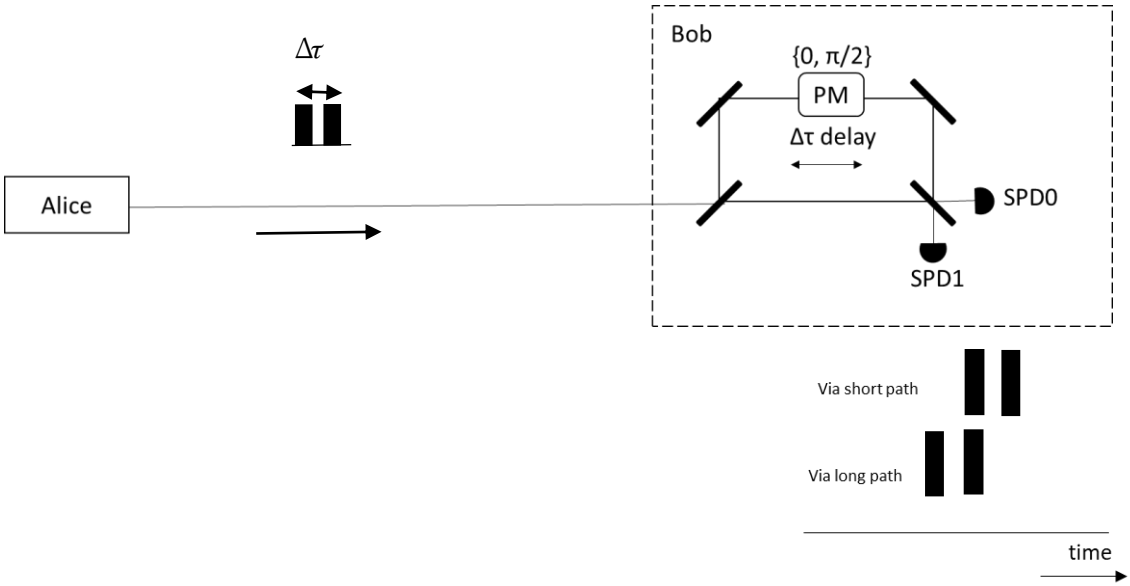

Fig. 5.1. Bob's active basis selection measurement setup. SPD: singe-photon detector; PM: phase modulator.

5.3 Polarization-insensitive measurement system

In this thesis, we propose a polarization-insensitive active basis selection scheme, the configuration of which is shown in Fig. 5.2 [102]. In our proposed scheme, the receiver equips a phase modulation circuit (PMC), followed by a Mach-Zehander interferometer. The PMC splits incoming two sequential pulses, where the first and second pulses are a reference and a signal with Alice's phase, respectively, into two polarization components (vertical and horizontal) by a polarization beam splitter (PBS). Each polarization component is fed into a phase modulator that is aligned to match the incident polarization state, so that phase modulation is properly and stably imposed onto the incident light. In addition, the modulation timing is adjusted so that the second pulse is modulated in each path. Then, the outputs from the phase modulators are recombined by another PBS. Here, the two paths from the first to second PBSs are constructed with an identical length of polarization maintaining fibers. The output of the second PBS is coupled to a polarization-insensitive waveguide MZI, followed by two single-photon detectors, one of which clicks according to the phase difference between the first and second pulses at the middle time-slot.

The above setup can achieve polarization-insensitive operation, thanks to a polarization

diversity configuration. Any polarization state is decomposed to the vertical and horizontal states, for which phase modulation is imposed by polarization aligned phase-modulators, respectively. The polarization state incident into each phase modulator is constant irrespective of the polarization state incident to the receiver. Therefore, the polarization-insensitive operation is achieved. In addition, a passive waveguide MZI enables stable interference because it is fabricated on one substrate. The above operation of the PMC is for phase-encoding BB84. For DQPS-QKD that uses a pulse train, the phase modulation is imposed onto every pulse.

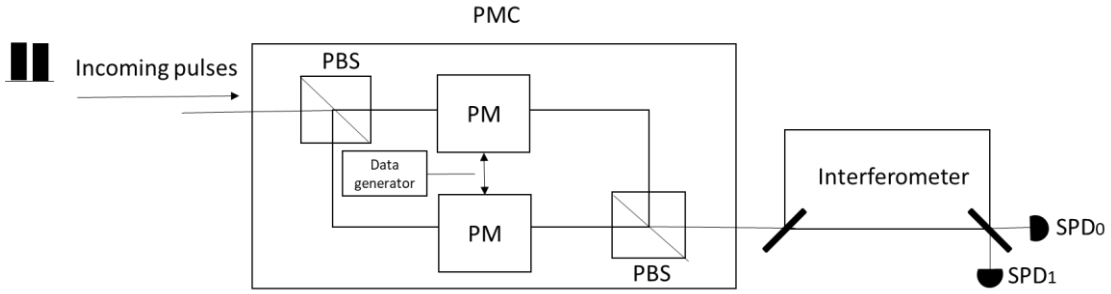

Fig. 5.2. Proposed polarization-insensitive measurement circuit. PMC: phase-modulation circuit; PBS: polarization beam splitter; PM: phase modulator.

5.4 Experiments

5.4.1 Setup

We carried out QKD experiments to demonstrate the polarization-insensitive operation with our countermeasure against side-channel attacks manipulating single-photon detectors. The experimental setup is shown in Fig. 5.3. This setup could run two types of four-states based QKD protocols, i.e., BB84 and DQPS-QKD. The main difference between these two protocols is the pulse sequence prepared by Alice. In BB84, Alice prepares a sequence of two pulses, with vacant at the neighboring slots, while she prepares a train of pulses in DQPS-QKD. Such signal preparation was achieved by intensity-modulating light from a laser source (LS). The pulse interval was chosen as 1 ns. Alice prepared a laser source from which 1550-nm wavelength light

was emitted with a power level of 5 dBm. The laser light passed through an intensity modulator (IM), from which a pulse sequence was generated. In BB84, one of the two pulses was randomly phase-modulated (PM) with one of the four phases $\{0, \pi\}$ $\{\pi/2, 3\pi/2\}$, while each pulse is phase-modulated in DQPS-QKD with one of the four phases, and then they were attenuated to be 0.1 photons per pulse on average by an attenuator (ATT). This Alice's signal passed through a polarization controller (PC), a coupler, and an attenuator that simulated the transmission loss. The PC was used to vary the polarization state, which was monitored by an optical coupler followed by a polarizer and a power meter. The signal passing through the attenuator was received by a measurement system whose setup is described in the previous section, where the outputs of the MZI were coupled to APD-based SPDs (idQuantique: ID200) gated at 4 MHz.

In our PMC, the polarization alignment was obtained by using phase modulators with polarization maintaining fiber pigtails. The phase modulators were driven by signals from two output ports of a data generator, respectively. The modulation timing was adjusted by the delay function of the date generator. The lengths of the two paths in the PMC were adjusted using an optical delay line.

The MZI needed to be controlled such that the phase difference between the two paths was stable at a given value. The path-length difference was set equal to the time interval between incident sequential pulses. The optical length should be set for the difference of the propagation phases through the two paths to be $2m\pi$ (m is integer). Our MZI was made of glass waveguides, whose optical length could be adjusted by the waveguide temperature through the thermo-optic effect. With the temperature of the MZI substrate around 22.10˚ C, almost entire power went to D1 for CW light input, with a crosstalk ratio between D1 and D2 being more than 20 dB, suggesting the optical length was properly set at this temperature. On the other hand, when $(0, \pi)$ phase modulation was imposed in front of the MZI, the almost entire power went to D2.

The output from the SPDs were coupled to a logic gate, followed by a time interval analyzer (TIA). The role of this logic gate was to send signals to the TIA, with which the TIA recorded the detection time and which detector clicked.

In our setup, the gating time window accepted only one pulse at one gating, which allowed the implementation of our countermeasure of monitoring coincident count.

In order to confirm the polarization-independent operation, the polarization controller (PC)

inserted between Alice and Bob was manually operated to exhibit various polarization states. The state of the polarization at the PC output was monitored by splitting a fraction of the PC output, passing it through a polarizer, and measuring the optical power at the polarizer output. The attenuator in front of Bob, was set at 6 dB, which corresponded to a 30-km fiber transmission.

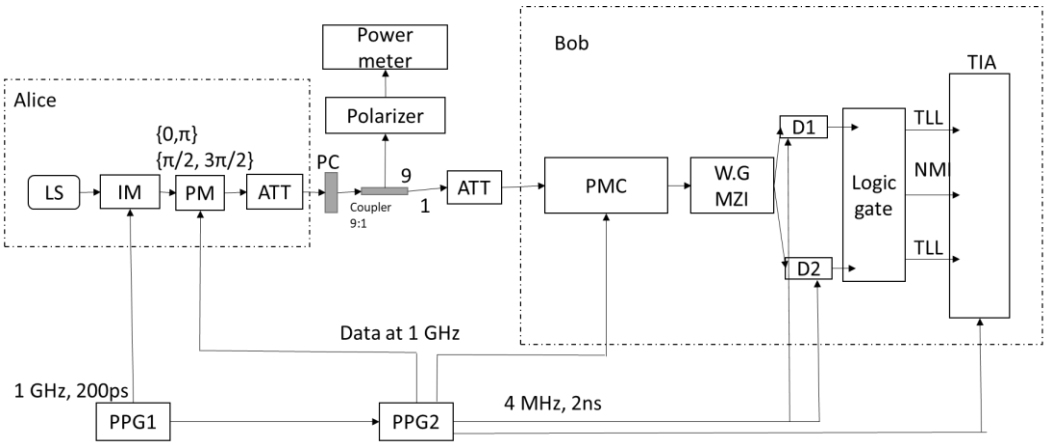

Fig. 5.3. Experimental setup. PMC: phase modulation circuit, LS: laser source, IM: intensity modulator, PM: phase modulator, ATT: attenuator, PC: polarization controller, PBS: polarization beam splitter, D1, D2: single-photon detectors, MZI: Mach-Zehnder interferometer, and TIA: time interval analyzer.

5.4.2 Results

The results of the BB84 and DQPS-QKD experiments are shown in Figs. 5.4 and 5.5, respectively, where the sifted key rate and the quantum bit error rate (QBER) are plotted as a function of the measured power at the polarization monitoring system, normalized by the maximum value, in (a) and (b), respectively. The horizontal axis indicates the power ratio of two orthogonal polarization components, i.e., R = (power in one component) / (total power), and R changing from 0 to 1 means that the polarization state fully varies from one polarization basis to the orthogonal one. The sifted key rate and the quantum bit error rate (QBER) were within 1.4–1.7 kbps and 2.9–3.55% in BB84, and were 1.95–2.57 kbps and 2.2–3.3% in DQPS, respectively, for various polarization states. Therefore, the polarization-insensitive operation was confirmed. These values of QBER allow error-correction and privacy amplification, described in Sections 2.2.3 and 2.2.4, to create a final

secret key. The variation observed in the results might be due to the residual power imbalance in the two paths in the PMC and slight polarization dependency of the waveguide MZI.

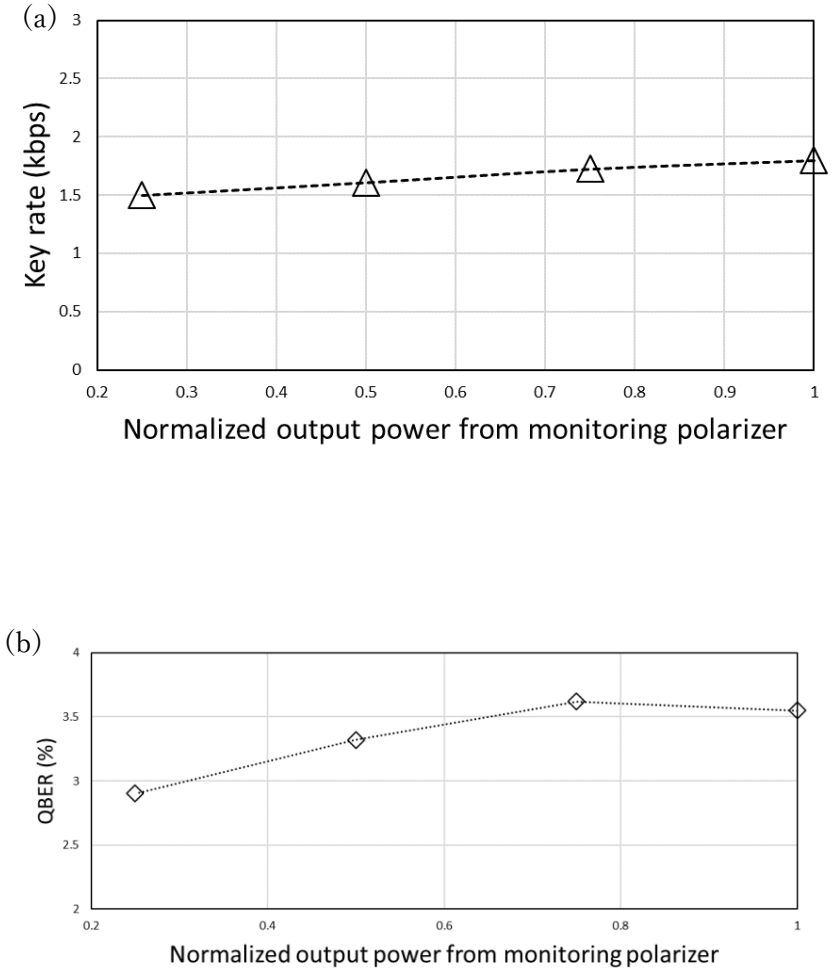

Fig. 5.4. Experimental results in BB84.

(a) Sifted key creation rate, and (b) QBER.

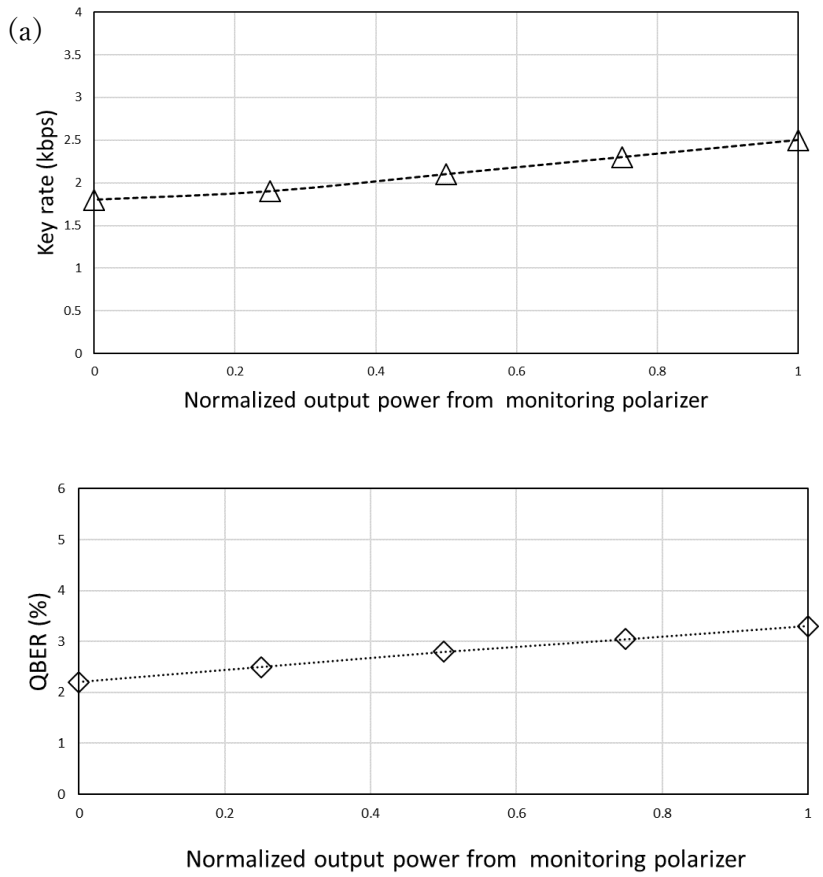

Fig. 5.5. Experimental results in DQPS-QKD.

(a) Sifted key creation rate, and (b) QBER.

The obtained results show that the DQPS-QKD has a higher key rate compared to that of BB84. This is because of efficient use of the time domain in DQPS-QKD, where Alice uses a train of pulses instead of two sequential pulses in BB84.

Figures 5.6 and 5.7 show the measured coincidental counts in the BB84 and DQPS-QKD experiments, respectively. The measurement time was of 4×10^6 clicks, which was determined by the memory size of our device. A number of coinciding counts were actually obtained, demonstrating the feasibility of our countermeasure against the detector blinding and control attacks, proposed in Chapter 4.

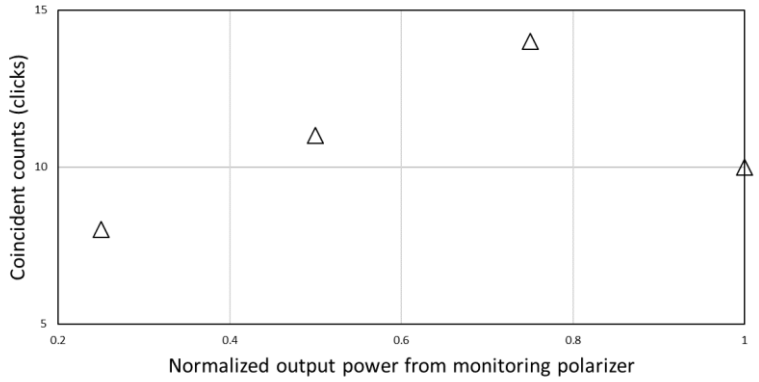

Fig. 5.6. Measured coincident clicks in BB84.

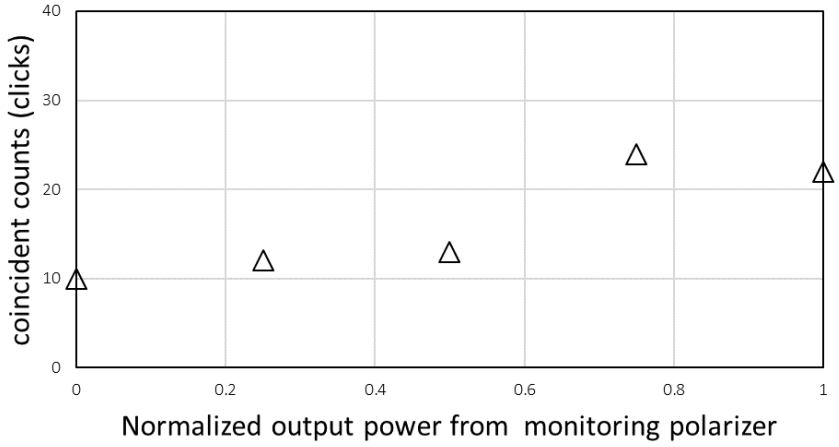

Fig. 5.7. Measured coincident clicks in DQPS-QKD.

5.5 Summary

In this chapter, we conducted QKD experiments equipping the countermeasure against side-channel attacks manipulating single-photon detectors, proposed in Chapter 3. The experiments also introduced a novel scheme of stable and polarization-insensitive active basis selection at the receiver, which simplified QKD systems compared with a passive basis selection scheme that is usually employed in QKD experiments. Both phase-encoding BB84 and DQPS-QKD protocols were implemented. Sifted-key bits and coincident counts were obtained almost constant for various polarization states, with allowable QBERs. Therefore, the QKD operation was successfully demonstrated, featuring our countermeasure against side-channel attacks and a polarization-insensitive receiver.

Chapter 6

A countermeasure against side-channel attacks in DPS-QKD by employing variable attenuator

6.1 Introduction

In Chapter 4, we propose a novel countermeasure against side-channel attacks, which is applicable to four-state based QKD protocols such as BB84 and DQPS-QKD. However, this countermeasure does not work for side-channel attacks against differential phase-shift quantum key distribution (DPS-QKD) protocol introduced in Section 2.6, because of no basis-mismatched measurement in this protocol. Therefore, an alternative solution is desired for DPS-QKD.

This chapter proposes a novel countermeasure against the detector blinding and control attack in DPS-QKD that uses APD-based single-photon detectors [103]. We first introduce a side-channel attack designed for DPS-QKD, and then present a countermeasure against it. The performance of a DPS-QKD system with the proposed countermeasure is also evaluated. Finally, discussion and the conclusion are described.

6.2 Blinding and control attack against DPS-QKD

In Chapter 3, Eve's strategy of manipulating an APD-based single-photon detector is introduced in detail. That is, Eve first injects bright illumination into an APD to force the APD bias voltage sufficiently below the breakdown voltage to avoid the APD to be switched to the Geiger mode by a gating pulse. This stage is called blinding a detector, during which the detector is insensitive to single-photons. Next, Eve sends a fake signal with a power level appropriate to make a click at a target detector. In Chapter 3, we describe that this strategy of manipulating a detector enables Eve to gain full key information in four-states based QKD such as BB84 and DQPS-QKD. This strategy is also available for DPS-QKD. In this section, we introduce how the blinding and control attack is performed against DPS-QKD.

For DPS-QKD, the blinding stage is the same as for BB84, where Eve injects bright illumination to Bob's detectors, but the controlling stage is somewhat different. When Eve successfully measures the phase difference of sequential two pulses in an intercept-resend attack, she resends two pulses with the measured phase difference. Here, the pulse power P_o is chosen such that the photocurrent generated from P_o at Bob's detectors in the linear mode exceeds the threshold I_{th} for the click, while that generated from (P_o /4) does not, i.e., a photon count is registered when the incident power is P_o but not when the incident power is (P_o /4). With this P_o, Eve controllably causes detection events in Bob, as illustrated in Fig. 6.1. Eve sends sequential (n +1) pulses when she consecutively measures n phase-differences (mostly n = 1). At Bob, the incident pulses are split into halves at the first BS and recombined with a time shift at the second BS in an MZI. At the second BS, the first half of the first pulse (passing through the short path) is simply split into half because no interference occurs, and hits Bob's two detectors with P_o /4 for each. Similarly, the second half of the last pulse (passing through the long path) hits the detectors with P_o/4 for each. On the other hand, the second half of the first pulse and the first half of the second pulse interfere with each other at the second BS, and go to one of Bob's detector, as a result of the interference, with P_o. Here, P_o is chosen such that P_o makes a click but P_o/4 does not. Therefore, a click occurs at the middle time-slot, but not at the edge slots.

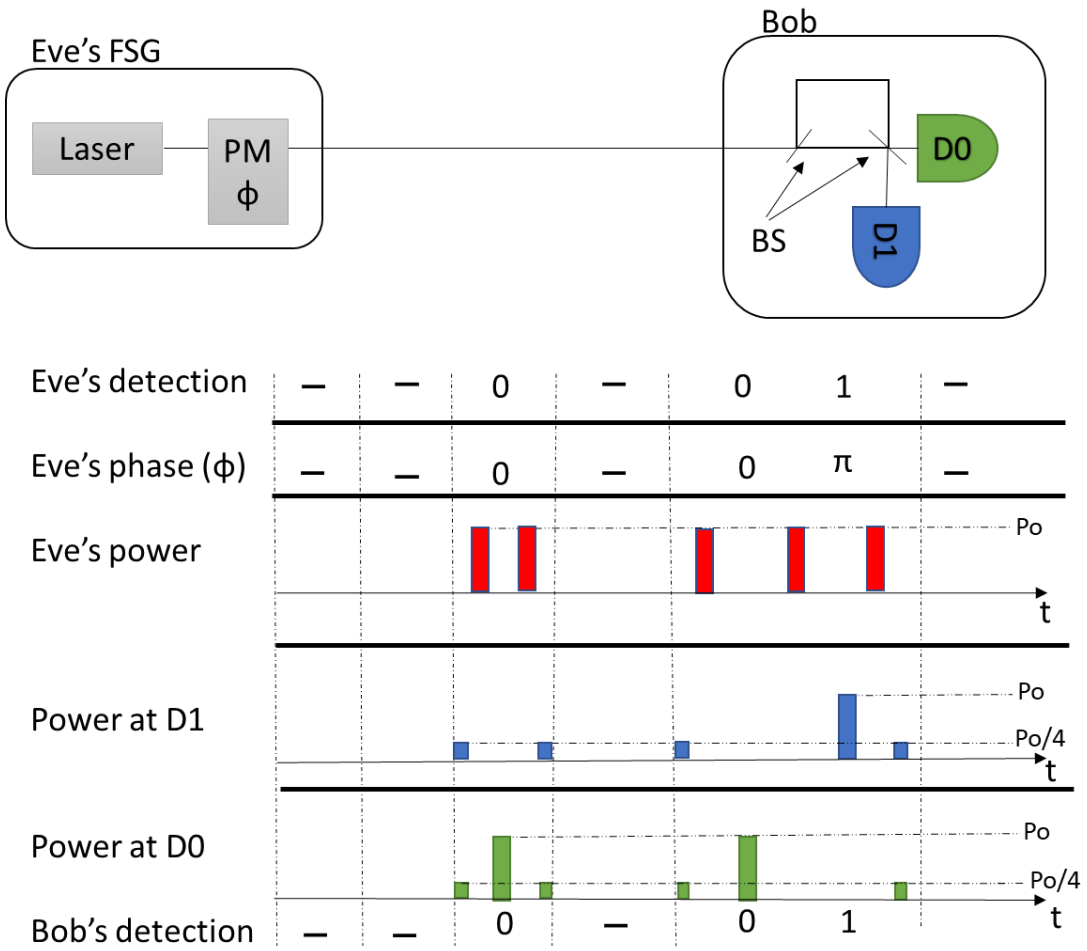

Fig. 6.1 Eve's behavior for controlling Bob's detection. FSG: fake state generator; BS: beam splitter.

A click at the middle time-slot gives a correct bit to Bob because proper interference occurs. In conventional intercept-resend attacks, a click at the edge time-slots can induce a bit error, as described in Section 2.6, from which the eavesdropping is revealed. In the above Eve's attack, however, no click occurs at them, and thus no bit error is induced and the eavesdropping is not noticed.

6.3 DPS-QKD with variable attenuation

In order to find the above side-channel attack, we propose to modify Bob's setup in DPS-QKD,

as shown in the inset in Fig. 6.2. Our scheme places a variable attenuator in front of Bob's interferometer. Alice prepares her pulses in the same way as in conventional DPS QKD and sends them to Bob. Bob usually measures the incoming pulses with no attenuation, similar to the conventional operation. However, randomly and occasionally, he adds a 6-dB attenuation using the attenuator. After the quantum transmission is completed, Bob checks the photon statistics during the attenuated time-slots. From this photon-number statistics, he can reveal the side-channel attack, as described below.

Figure 6.2 illustrates how Bob's circuit behaves against the blinding and control attack. The incoming pulses are attenuated by 6 dB with the attenuator placed just before the interferometer, whose timing is randomly chosen by Bob. Bob obtains the count rate corresponding to the 6-dB attenuation under the normal condition. However, when Eve conducts the blinding and control attack, she resends fake pulses with a power level as described in the previous section to make Bob's detectors click at a target time-slot (i.e., the middle one) but not at undesired ones (i.e., the edge time-slots), as shown in the first row in Fig. 6.2(a). When Eve's fake signal reaches Bob at attenuated time-slots, the pulses are incident onto Bob's interferometer with one quarter of the power level intended by Eve, i.e., (P_o/4), as shown in the second row in Fig. 6.2(a), because of the 6-dB attenuation. With this incident condition, the power level incident onto one of Bob's detectors at the second time-slot is P_o/4, as shown in the third and fourth rows in Fig. 6.2(a), and Bob's photocurrent generated from this power level does not exceed the photo-count threshold I_{th}. Thus, Bob's detectors do not click even at the second time-slot at which Eve tries to make a click. From this unexpected detection event, i.e., no click at the attenuated time-slots, Bob notices the side-channel attack.

As a countermeasure against the above countermeasure, Eve may resend pulses with four times higher power ($4 \times P_o$) to make a click at the second time-slot even when Bob imposes the 6-dB attenuation, as shown in the first row in Fig. 6.2(b). However, when no attenuation is imposed, the power level reaching the detectors at the first and third time-slots is P_o for each, as shown in the third and fourth rows in Fig. 6.2(b), and then coincident clicks of the two detectors are registered. i.e., sequential three detection events always occur with coincident clicks at the first, one clicks at the second, and coincident clicks at the third, when no attenuation. The eavesdropping is revealed from these abnormal detection events. Thus, Eve cannot employ this

strategy of resending pulses with a higher power level.

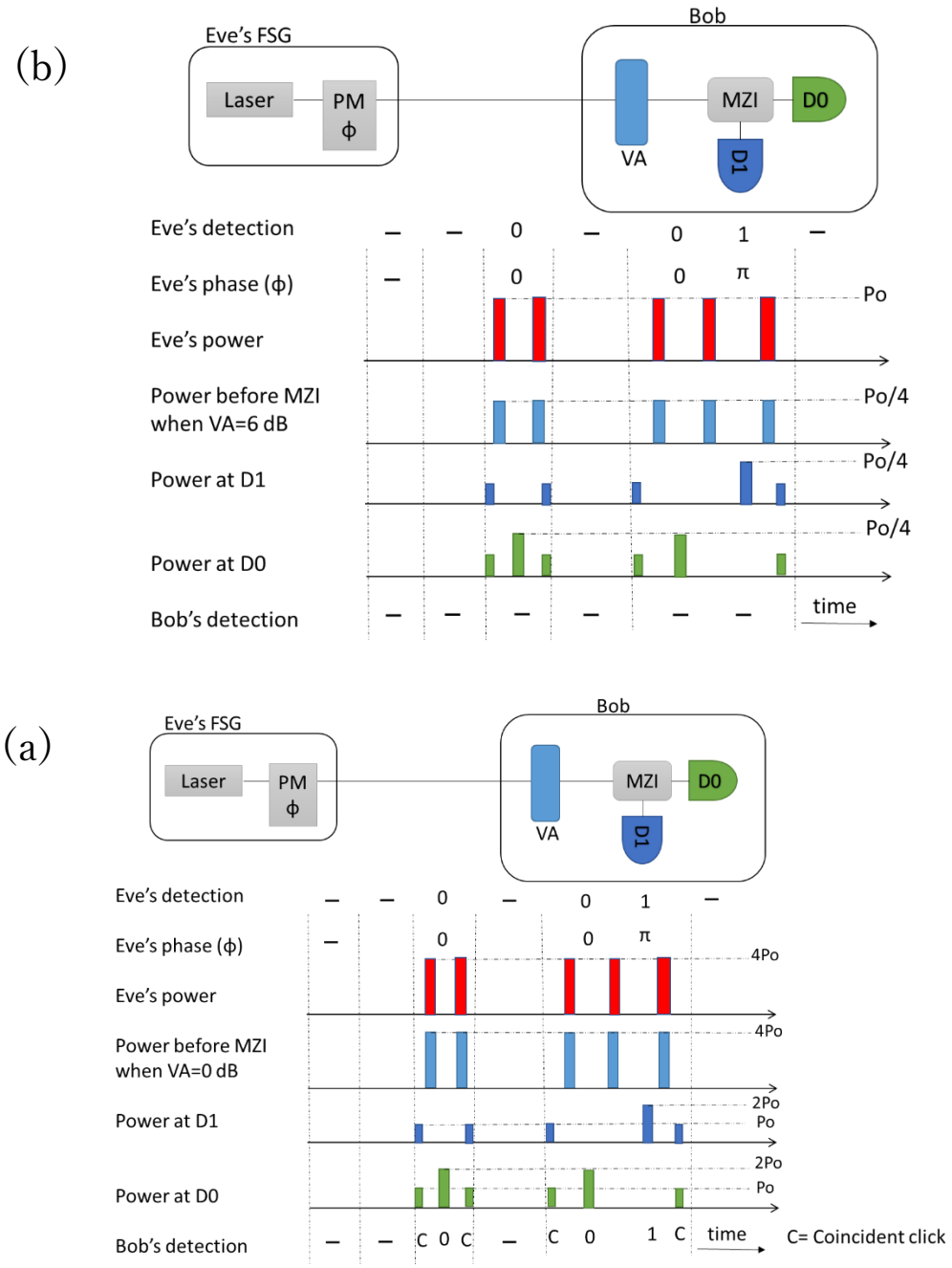

Fig. 6.2. Bob's setup in the proposed scheme and its behavior against Eve's signal. VA: variable attenuator. a) Conventional blinding and control attack. There is no detection at Bob's detectors during attenuated time-slots, when Eve resends fake signal similar to her original attack. b) Modified blinding and control attack. There are three sequential detection events during normal time-slots (i.e., no attenuation), when Eve tries to resend fake pulses with higher power to cause a click at attenuated time-slots.

6.4 Photon-number fluctuation effect

The proposed countermeasure detects the side-channel attack from reduction in photon counts at attenuated time-slots. In principle, a slight reduction in the count rate from a value expected in the normal condition can reveal the eavesdropping. In practice, however, the number of transmitted photons fluctuates according to a Poisson distribution with a variance determined by the measured photon number (i.e., the measurement time) or Bob's memory size. The variance is larger for a shorter measurement time. Eve can partially conduct the side-channel attack masked by this photon-number fluctuation.

The partial eavesdropping ratio masked by the photon-number fluctuation can be estimated as follows. First, we suppose that Bob's click number at attenuated time-slots is n_0 in the normal condition with no eavesdropping. When Bob measures a click number n_m less than n_0, he attributes the reduction of the measured value from the normal one (i.e., $n_0 - n_m$) to the partial eavesdropping, whose ratio can be estimated as $(n_0 - n_m)/n_0$. Here, the normal click number n_0 fluctuates according to a Poisson distribution $P_n(n_0|N_0)$ determined by the average of the normal click number N_0. Therefore, the effective eavesdropping ratio, provided that the mean normal click number is N_0, can be evaluated as

$$r_{sca}(n_m \mid N_0) = \int_{n_m}^{n_0} \frac{(n_0 - n_m)}{n_0} P_n(n_0|N_0) dn_0 = \int_{n_m}^{n_0} \frac{(n_0 - n_m)}{n_0} * e^{-N_0} \frac{(N_0)^{n_0}}{n_0!} dn_0. \quad (6.1)$$

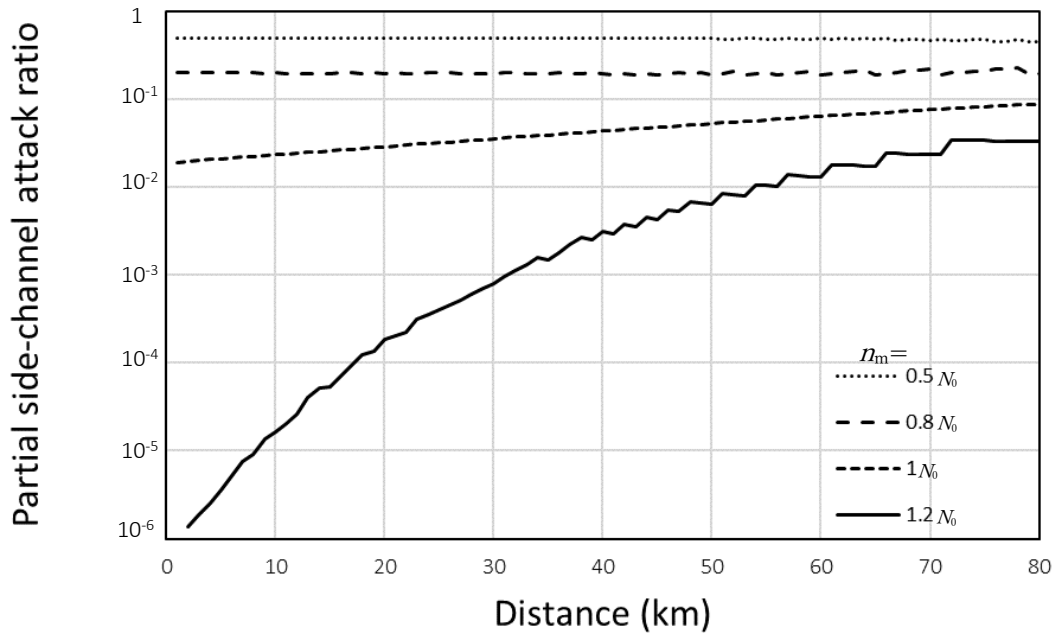

Fig. 6.3. Partial side-channel attack ratio for various measured click numbers (n_{m}) and mean normal click number (N_0) as a function of QKD distance.

For a given measured click number, the partial eavesdropping ratio is estimated as described above. Figure 6.3 shows the partial side-channel attack ratio at various distances for various measured click numbers, calculated using Eq. (6.1). In the calculation, the mean normal click number (N_0) is assumed according to the system conditions that Alice sends 0.1 photons per pulse an average, the attenuation of the transmission line is 0.2 dB/km, Bob's detection efficiency is 10 %, and the number of pulses is 0.5×10^6, and all pulses are assumed to reach Bob at attenuated time-slots. The figure quantitatively shows the dependence of the partial side-channel attack ratio on the measured click number.

The above is an evaluation for a given measured click number. In system design, the expected or average system performance before measurement should be estimated. In order to do it, we assume that the measured click number would have a value following the probability density distribution of a Poisson profile, i.e., the photon-number statistics for a coherent state, and average the eavesdropping ratio over the click number distribution as

$$\bar{r_{\mathrm{p}}} = \int_0^{\infty} r_{sca}(n_{\mathrm{m}} \mid N_0) * \frac{e^{-N_0}(N_0)^{n_{\mathrm{m}}}}{n_{\mathrm{m}}!}\ dn_{\mathrm{m}}, \tag{6.2}$$

where $\bar{r_{\mathrm{p}}}$ is the average partial side-channel attack ratio. Figure 6.4 shows the average partial side-channel attack as a function of distance, which was assumed based on the same system conditions as described above. At a long distance, N_0 is small, and then the partial side-channel attack ratio is large.

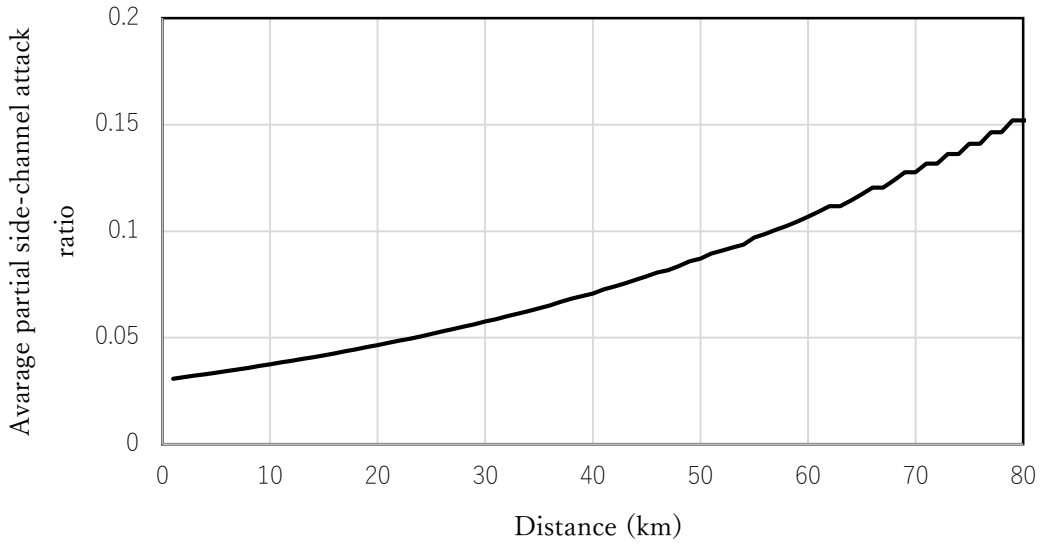

Fig. 6.4. Average partial side-channel attack ratio as a function of transmission distance.

6.5 Simulations

The previous section suggests that the smaller the photon-number fluctuation is at attenuated time-slots, the lower the partial side-channel attack ratio would be. As a result, the key compression ratio (from a sifted to a final keys) in privacy amplification would be small. Thus, a large number of attenuated slots are preferable for a small key compression ratio. On the other hand, the attenuation at Bob reduces the sift-key rate. Therefore, there is an optimum insertion ratio of attenuated time-slots to maximize the final key rate. The total final key rate R_{f}, which consists of the key rates at the normal and attenuated time-slots, is expressed as

$$R_{\mathrm{f}} = r_{\mathrm{att}} R_{\mathrm{att}} + (1 - r_{\mathrm{att}}) R_{\mathrm{n}}, \tag{6.3}$$

where r_{att} is the insertion ratio of the attenuated slots, R_{att} and R_{n} are the final key rates at the attenuated and normal time slots, respectively. Based on the security analysis assuming the general individual attack [104], R_{att} and R_{n} can be expressed as

$$R_{\mathrm{att}} = R_{\mathrm{sift}}^{\mathrm{att}} \left\{1 - \bar{r}_{\mathrm{p}} - 2\,\mu \log_2 \left[1 - e_{\mathrm{att}}^2 - \frac{(1-6e_{\mathrm{att}})^2}{2}\right] + f(e_{\mathrm{att}})\ h(e_{\mathrm{att}})\right\}, \tag{6.4a}$$

$$R_{\mathrm{n}} = R_{\mathrm{sift}}^{\mathrm{n}} \left\{1 - \bar{r}_{\mathrm{p}} - 2\,\mu \log_2 \left[1 - e_{\mathrm{n}}^2 - \frac{(1-6e_{\mathrm{n}})^2}{2}\right] + f(e_{\mathrm{n}})\ h(e_{\mathrm{n}})\right\}, \tag{6.4b}$$

where $R_{\mathrm{sift}}^{\mathrm{att}}$ and $R_{\mathrm{sift}}^{\mathrm{n}}$ are the sifted key rates at attenuated and normal time-slots, respectively, μ is the average photon number sent from Alice, e_{att} and e_{n} are the system error rates at attenuated and normal time-slots, respectively, $f(e_{\mathrm{att,n}})$ is factor representing the error correction efficiency, and $h(e_{\mathrm{att,n}}) = -e_{\mathrm{att,n}} \log_2 e_{\mathrm{att,n}} - (1 - e_{\mathrm{att,n}}) \log_2 (1 - e_{\mathrm{att,n}})$. Note that the sifted-key rate and system error rate at attenuated time-slots are different from those at normal time-slots, because the signal-to-noise ratio at the detection is different due to the 6-dB attenuation.

We evaluated the system performance based on the above considerations, assuming the following system parameters: Bob's dark count rate = 300 Hz, the transmission loss = 0.2 dB/km, the error rate resulting from Bob's interference = 0.01, Bob's detection efficiency = 10 %, $f(e)$ = 1.16, and Alice's average photon number μ = 0.2. Figure 6.5 shows the result, where the final key creation rate and the ratio of no partial side-channel attack ($1 - \bar{r}_{\mathrm{p}}$) are plotted as functions of the insertion ratio of attenuated time-slots. The figure exhibits a trade-off relationship between the sift-key rate and the ratio of no side-channel attack, which indicates that there is an optimum insertion ratio.

We carried out the above calculation for various transmission distances, and plotted the optimized final key creation rate as a function of distance. The result is shown in Fig. 6.6. For comparison, the system performance of conventional DPS QKD suffering from no side-channel attack is also plotted. The figure indicates that the proposed scheme prevents side-channel attacks, sacrificing the transmission distance by about 10 %.

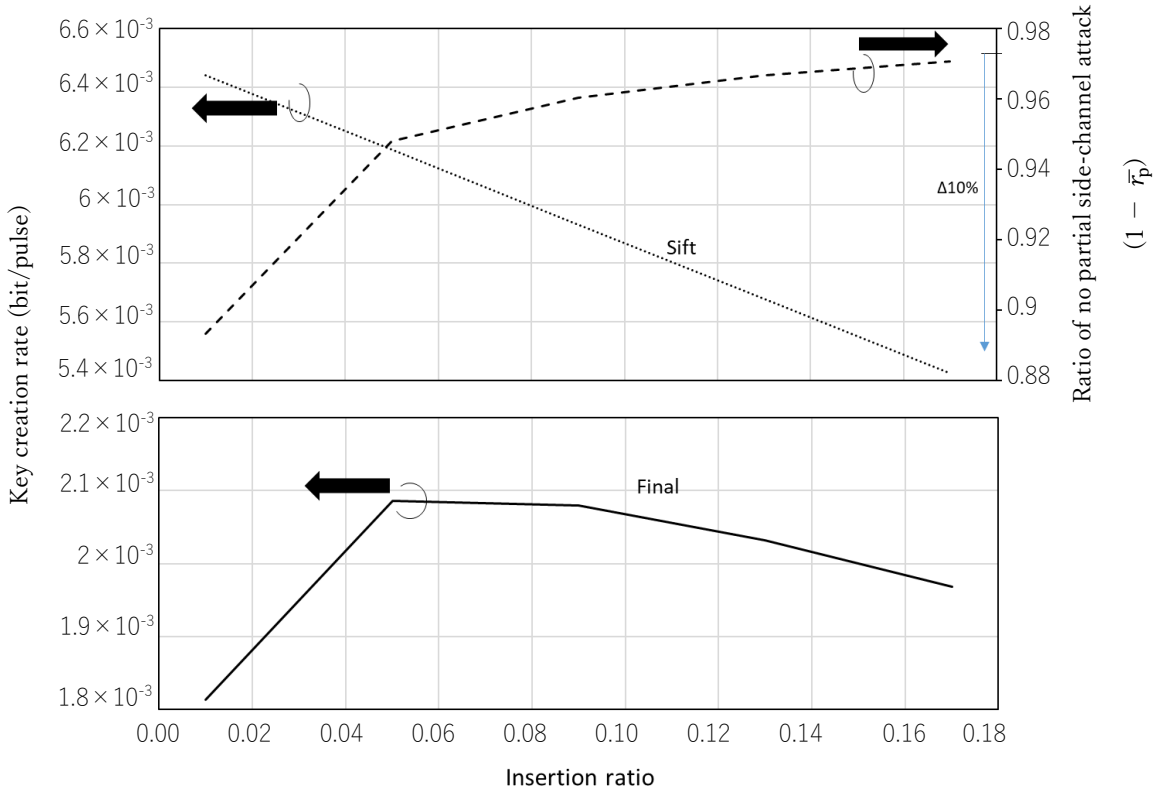

Fig. 6.5. Key creation rate and ratio of no side-channel attack as functions of insertion ratio of attenuated time-slots. The transmission distance is 50 km; the number of pulses is 1×10^6.

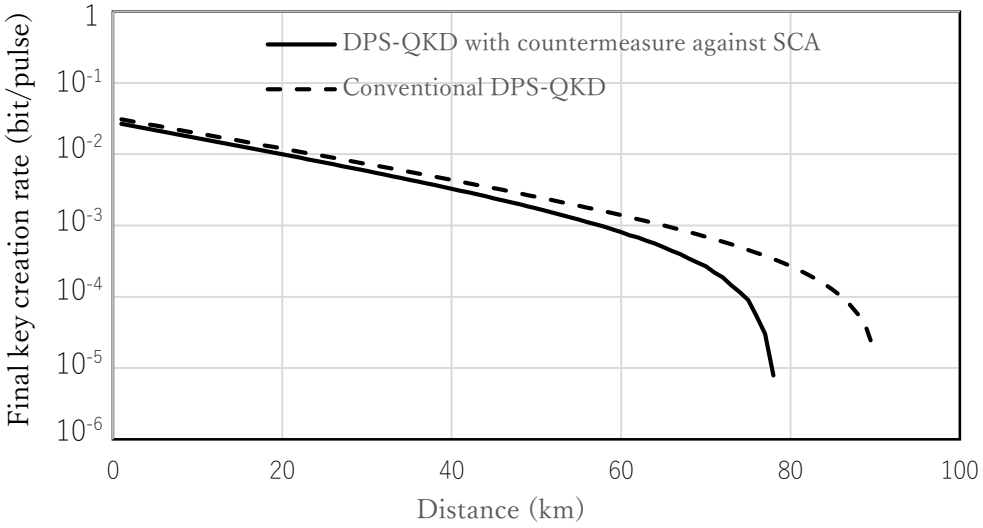

Fig. 6.6. DPS-QKD system performance against side-channel attack (SCA). The insertion ratio of attenuated slots is optimized at each distance. The general individual attack is assumed with following system parameters: Bob's dark count rate = 300 Hz, transmission loss = 0.2 dB/km, error rate in Bob's interferometer = 0.01, Bob's detection efficiency = 10 %, $f(e) = 1.16$, Alice's average photon number $\mu = 0.2$, and the number of pulses is 1×10^6.

In the above calculations, the optimum insertion ratio of attenuated slots is determined under the condition of the total pulse number = 1×10^6. This optimum ratio depends on the total pulse number. Figure 6.7 shows the optimized insertion ratio as a function of the pulse total number. It indicates that the optimized insertion ratio is lower for a larger pulse number. As a result, the system performance is better for a larger pulse number. Figure 6.7 also indicates that the system performance approaches a constant value beyond a certain pulse number, e.g., 5×10^6 in our simulation.

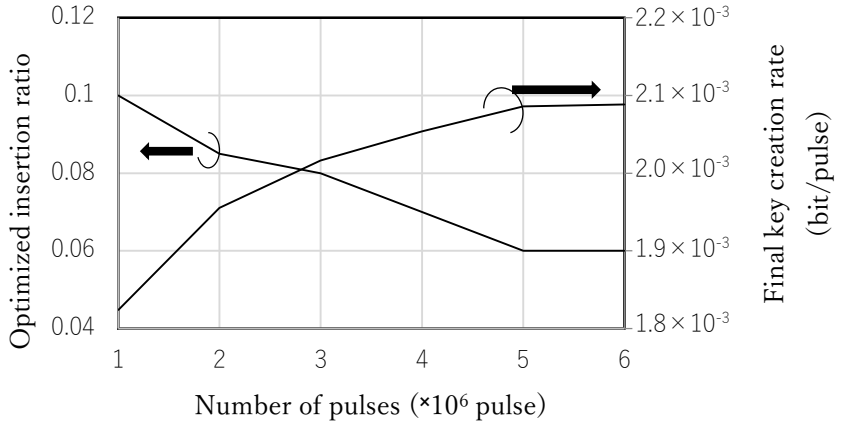

Fig. 6.7. Insertion ratio and final key creation rate as functions of number of pulses. The transmission distance is 50 km.

6.6 Summary

In this chapter, we proposed a countermeasure against the detector blinding and control attack for DPS-QKD using APD-based detectors. It randomly imposes a 6-dB attenuation at the receiver, and finds the attack from change in the photon number statistics during the attenuated time-slots. In contrast to previously reported countermeasures introduced in Section 3.4.2, the proposed scheme is device-independent and provide a general solution to DPS-QKD. The optimum operation condition of the proposed scheme was also discussed, and the performance of the DPS-QKD system with this countermeasure was evaluated.

Chapter 7

Conclusion

In cryptography, the ultimate goal is to achieve a system that is unconditionally unbreakable. The one-time protocol, that uses a secret key of a length equal to a plain text just one time, can reach this goal. However, the main challenge is how to distribute such a key to distant parties in a secret way. Quantum key distribution (QKD) meets this demand.

QKD systems are proved to be ultimately secure in theory. In practice, however, they have security loopholes arising from operation characteristics of actual devices, which are outside the theoretical framework. Several eavesdropping strategies taking advantage of such a loophole, which is called side-channel attack, have been proposed and demonstrated, and countermeasures against them have been studied and developed. However, conventional countermeasures are not easy to implement, costly, or device-dependent.

In order to counter side-channel attacks in a simple way, this thesis proposed countermeasures featuring simplicity, and evaluated their performances. QKD experiments were also conducted, demonstrating the feasibility of the proposed scheme, where a novel receiver setup was employed.

The summaries of what this thesis performed are as follows.

A. Countermeasure against side-channel attack in four-states QKD protocol

In four-states QKD protocols, a transmitter (Alice) and a receiver (Bob) randomly choose basis in her modulation and his measurement, respectively, where their choice of basis is mismatched with a 50% probability. Conventionally, these basis-mismatched events are simply discarded. We propose to utilize these events for a countermeasure against the side-channel attack.

In practical QKD systems, Alice uses a weak coherent light as an information carrier. Such light has a finite probability of including more than two photons, even when strongly attenuated, and then occasionally causes coincident counts in Bob's basis-mismatched measurement. On the other

hand, the detector blinding and control attack, that is the strongest side-channel attack, causes no coincident click in basis-mismatched measurement. This thesis proposes to utilize this discrepancy in the coincident count rate to find the eavesdropping.

The number of coincident counts depends on system conditions such as the transmission loss, Bob's detector efficiency, and the mean photon number sent from Alice. We estimate expected coincident counts considering the above system conditions, and carry out an experiment to confirm the estimation. The results show that the proposed countermeasure is feasible in practice.

B. Countermeasure against side-channel attack in DPS QKD protocol

In DPS-QKD, Alice sends a train of weak coherent pulses to Bob. We propose to implement a variable attenuator in front of Bob's measurement system as a countermeasure against the detector blinding and control attack in DPS-QKD. Bob randomly and occasionally imposes a 6-dB attenuation on the attenuator. In the normal condition with no eavesdropping, Bob has a number of clicks according to the 6-dB attenuation in the attenuated time-slots. However, the detector blinding and control attack does not cause any click in the attenuated time-slots, from which eavesdropping is reveled. We study the performance of the proposed countermeasure, where the insertion ratio of the attenuated time-slots is optimized, and the QKD performance (the key rate and the transmission distance) is evaluated with optimized insertion ratios. The result indicates its feasibility at a sacrifice of a 10% of the transmission distance.

C. QKD experiments of four-states protocols

In order to demonstrate the proposed countermeasure for four-state QKD protocol, we conduct experiments for four-states QKD protocols. A novel receiver setup featuring polarization insensitive and stable operation is also proposed and demonstrated. The experiment setup runs two QKD protocols, BB84 and DQPS, where Alice prepares two pulses and a train of pulses for BB84 and DQPS, respectively. For the polarization-insensitive operation, we introduced a polarization diversity scheme consisting of polarization beam splitters for splitting and recombining two orthogonal polarization components, between which phase modulators are inserted for each polarization component. This setup achieves stable phase-modulation as the

input of each phase modulator has an aligned polarization state irrespective of the polarization state of transmitted signal. The above phase-modulation circuit is placed in front of a waveguide interferometer, owing to which stable measurement with active basis selection is achieved. We conduct QKD experiments with the above setup, while varying the polarization state input into the receiver to examine the polarization dependency, and also recording coincident counts as a countermeasure against the detector blinding and control attack. The results show that we can obtain coincident count in practical system condition, confirming the feasibility of countermeasure as well as the polarization-insensitive operation of our receiver setup.

In this thesis, we proposed two novel schemes to counter the side-channel attacks in two different QKD systems, i.e., four-states and DPS-QKD. Proposed schemes feature simplicity and practicality, and provide a general solution independent of device characteristics.

This thesis contributes to construct practical QKD systems robust against the most powerful side-channel attack with a simple setup.

References

[1] C. H. Bennett, F. Bessette, L. Salvail, G. Brassard, and J. Smolin, "Experimental quantum cryptography," *Journal of Cryptology*, vol. 5, 3–28 (1992).

[2] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, "Quantum cryptography, or unforgeable subway tokens," *Advances in Cryptology: Proceedings of Crypto' 82*, 267-275, August 1982, Plenum, New York.

[3] S. Wiesner, "Conjugate coding," manuscript written circa 1970, unpublished until it appeared in *Sigact News*, vol. 15, 78-88 (1983).

[4] C. H. Bennett, G, Brassard, and S. Breidbart, Quantum Cryptography II: How to re-use a one-time pad safely even if P=NP," *Natural Computing*, vol. 13, 453–458 (2014).

[5] C. H. Bennett and G. Brassard, "An update on quantum cryptography," Advances *in Cryptology: Proceedings of Crypto' 84*, p.p. 475-480, August 1984, Springer-Verlag, New York.

[6] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Proceedings of *IEEE International Conference on Computers, Systems, and Signal Processing*, pp. 175-179, December 1984, Bangalore, India.

[7] C. H. Bennett, G. Brassard, C. Crepeau, and M.-H. Skubiszewska, "Practical quantum oblivious transfer", *Advances in Cryptology: Proceedings of Crypto' 91*, p.p. 351-366, August 1991, California.

[8] G. Brassard and C. Crrpeau, "Quantum bit commitment and coin tossing protocols", *Advances in Cryptology: Proceedings of Crypto '90*, 49-61, August 1990, California.

[9] A. Ekert, "Quantum cryptography based on Bell's theorem", *Physical Review Letters*, vol. 67, 661-663 (1991).

[10] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?," *Physical Review*, vol. 47, 777–780 (1935).

[11] C. H. Bennett, "Quantum cryptography using any 2 nonorthogonal states," *Physical Review Letters*, vol. 68, 3121–3124 (1992).

[12] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution," *Physical Review Letters*, vol. 89, 037902 (2002).

[13] A. Muller, H. Zbinden, and N. Gisin, “Quantum cryptography over 23 km in installed under-lake telecom fibre,” *Euro Physics Letters*, vol. 33, 335–339 (1996).

[14] D. Stucki, N.Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, “High rate, long-distance quantum key distribution over 250 km of ultra-low loss fibres,” *New Journal of Physics*, vol. 11, 075003 (2009).

[15] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, “Entanglement-based quantum communication over 144 km,” *Nature Physics*, vol. 3, 481–486 (2007).

[16] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, “Generalized privacy amplification,” *IEEE Transactions on Information Theory*, vol. 41, 1915–1923 (1995).

[17] D. Mayers, “Advances in cryptology,” *Proceedings of Crypto’96*, vol. 1109, edited by N. Koblitz, 343–357, Springer, New York, 1996.

[18] H.-K. Lo and H. F. Chau, “Unconditional security of quantum key distribution over arbitrarily long distances,” *Science*, vol. 283, 2050–2056 (1999).

[19] P. W. Shor and J. Preskill, “Simple proof of security of the BB84 quantum key distribution protocol,” *Physical Review Letters*, vol. 85, 441–444 (2000).

[20] D. Mayers, “Unconditional security in quantum cryptography,” *Journal of the ACM*, vol. 48, 351–406 (2001).

[21] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, “Security of quantum key distribution with imperfect devices,” *Quantum Information & Computation*, vol. 4, 325–360 (2004).

[22] H. Inamori, N. Lütkenhaus, and D. Mayers, “Unconditional security of practical quantum key distribution,” *European Physical Journal D*, vol. 41, 599–627 (2007).

[23] M. Koashi and J. Preskill, “Secure quantum key distribution with an uncharacterized source,” *Physical Review Letters*, vol. 90, 057902 (2003).

[24] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, “Limitations on practical quantum cryptography,” *Physical Review Letters*, vol. 85, 1330–1333 (2000).

[25] N. Lütkenhaus, “Security against individual attacks for realistic quantum key distribution,” *Physical Review A*, vol. 61, 052304 (2000).

[26] Ø. Marøy, L. Lydersen, and J. Skaar, "Security of quantum key distribution with arbitrary individual imperfections," *Physical Review A*, vol. 82, 032337 (2010).

[27] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Physical Review Letters*, vol. 92, 057901 (2004).

[28] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Physical Review Letters*, vol. 91, 057901 (2003).

[29] A. Becir, A. Messikh, and M. R. B. Wahiddin, "Improvement of secure communication with continuous variable entanglement of squeezed coherent states via heterodyne detection," *Journal of Physics B: Atomic, Molecular and Optical Physics*, vol. 44, 069801 (2011).

[30] C. Kurtsiefer, P. Zarda, S. Mayer, and H. Weinfurter, "The breakdown flash of silicon avalanche photodiodes-back door for eavesdropper attacks?" *Journal of Modern Optics*, vol. 48, 2039–2047 (2001).

[31] A. Vakhitov, V. Makarov, and D. R. Hjelme, "Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography," *Journal of Modern Optics*, vol. 48, 2023–2038 (2001).

[32] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, "Trojan-horse attacks on quantum-key-distribution systems," *Physical Review A*, vol.73, 022320 (2006).

[33] V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems," *Physical Review A*, vol. 74, 022313 (2006); Erratum ibid. vol. 78, 019905 (2008).

[34] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, "Time-shift attack in practical quantum cryptosystems," *Quantum Information & Computation*, vol. 7, 73–82 (2007).

[35] A. Lamas-Linares and C. Kurtsiefer, "Breaking a quantum key distribution system through a timing side channel," *Optics Express*, vol. 15, 9388–9393 (2007).

[36] C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, "Phase-remapping attack in practical quantum-key-distribution systems," *Physical Review A*, vol. 75, 032314 (2007).

[37] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum key- distribution systems," *Physical Review A*, vol.78, 042333 (2008).

[38] S. Nauerth, M. Fürst, T. Schmitt-Manderbach, H. Weier, and H. Weinfurter, "Information leakage via side channels in free space BB84 quantum cryptography," *New Journal of Physics*, vol. 11, 065001 (2009).

[39] V. Makarov, "Controlling passively quenched single photon detectors by bright light," *New Journal of Physics*, vol. 11, 065003 (2009).

[40] F. Xu, B. Qi, and H.-K. Lo, "Experimental demonstration of phase remapping attack in a practical quantum key distribution system," *New Journal of Physics*, vol. 12, 113026 (2010).

[41] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nature Photonics*, vol. 4, 686–689 (2010).

[42] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, "Full-field implementation of a perfect eavesdropper on a quantum cryptography system," *Nature Communications*, vol. 2, 1349 (2011).

[43] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, "Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors," *New Journal of Physics*, vol. 13, 073024 (2011).

[44] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device independent security of quantum cryptography against collective attacks," *Physical Review Letters*, vol. 98, 230501 (2007).

[45] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Physical Review Letters*, vol. 108, 130503 (2012).

[46] M. Koashi and N. Imoto, "Quantum cryptography based on split transmission of one-bit information in two setps," *Physical Review Letters*, vol. 79, 2383–2386 (1997).

[47] B. Huttner, N. Imoto, N. Gisin, and T. Mor, "Quantum cryptography with coherent states," *Physical Review A*, vol. 51, 1863–1869 (1995).

[48] C. H. Bennett, G. Brassard, and N. Mermin, “Quantum cryptography without Bell’s theorem,” *Physical Review Letters*, vol. 68, 557–559 (1992).

[49] D. Welsh, “Codes and cryptography,” Clarendon Press, Oxford, UK (1998).

[50] G. Brassard and L. Salvail, “Secret-key reconciliation by public discussion,” *in Advances in Cryptology-EUROCRYPT’93* (T. Helleseth, ed.), vol. 765 of Lecture Notes in Computer Science, 410–423 (Springer-Verlag, Berlin, 1994).

[51] N. Lütkenhaus, “Estimates for practical quantum cryptography,” *Physical Review A*, vol. 59, 3301–3319 (1999).

[52] A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres, “Eavesdropping on quantum-cryptographical systems,” *Physical Review A*, vol. 50, 1047–1056 (1994).

[53] B. Huttner and A. K. Ekert, “Information gain in quantum eavesdropping,” *Journal of Modern Optics*, vol. 41, 2455–2466 (1994).

[54] N. Lütkenhaus, “Security against individual attacks for realistic quantum key distribution,” *Physical Review A*, vol. 61, 052304 (2000).

[55] 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,” *Physical Review A*, vol. 56, 1163–1172 (1997).

[56] B. A. Slutsky, R. Rao, P. C. Sun, and Y. Fainman, “Security of quantum cryptography against individual attacks,” *Physical Review A*, vol. 57, 2383–2398 (1998).

[57] E. Biham and T. Mor, “Security of quantum cryptography against collective attacks,” *Physical Review Letters*, vol. 78, 2256–2259 (1997).

[58] X.-B. Wang, “Beating the photon-number-splitting attack in practical quantum cryptography,” *Physical Review Letters*, vol. 94, 230503 (2005).

[59] H.-K. Lo, X. Ma, and K. Chen, “Decoy state quantum key distribution,” *Physical Review Letters*, vol. 94, 230504 (2005).

[60] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, “Practical decoy state for quantum key distribution,” *Physical Review A*, vol. 72, 012326 (2005).

[61] 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," *Physical Review Letters*, vol. 98, 010504 (2007).

[62] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, "Entanglement-based quantum communication over 144 km," *Nature Physics*, vol. 3, 481–486 (2007).

[63] M. Koashi, "Efficient quantum key distribution with practical sources and detectors," arXiv:quant-ph/0609180v1.

[64] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Continuous operation of high bit rate quantum key distribution," *Applied Physics Letters*, vol. 96, 161102 (2010).

[65] K. Inoue, "Differential phase-shift quantum key distribution systems," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, 6600207 (2015).

[66] K. Inoue and Y. Iwai, "Differential-quadrature-phase-shift quantum key distribution," *Physical Review A*, vol. 79, 022319 (2009).

[67] S. Kawakami, T. Sasaki, and M. Koashi, "Security of the differential-quadrature-phase-shift quantum key distribution," *Physical Review A*, vol. 94, 022332 (2016).

[68] M. Hillery, "Quantum cryptography with squeezed states," *Physical Review A*, vol. 61, 022309 (2000).

[69] N. J. Cerf, M. Levy, and G. Van Assche, "Quantum distribution of Gaussian keys using squeezed states," *Physical Review A*, vol. 63, 052311 (2001).

[70] V. Makarov and D. R. Hjelme, "Faked states attack on quantum cryptosystems," *Journal of Modern Optics*, vol. 52, 691-705 (2005).

[71] L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov, "Controlling a superconducting nanowire single-photon detector using tailored bright illumination," *New Journal of Physics*, vol. 13, 113042 (2011).

[72] L. Lydersen, N. Jain, C. Wittmann, Ø. Marøy, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, " Superlinear threshold detectors in quantum cryptography," *Physical Review A*, vol. 84, 032320 (2011).

[73]N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, “Device calibration impacts security of quantum key distribution,” *Physical Review Letters*, vol. 107, 110501 (2011).

[74] H. W. Li, S. Wang, J. Z. Huang, W. Chen, Z. Q. Yin, F.Y. Li, Z. Zhou, D. Liu, Y. Zhang, G. C. Guo, W. S. Bao, and Z. F. Han, “Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multi-wavelength sources,” *Physical Review A*, vol. 84, 062308 (2011).

[75] Y. L. Tang, H. L. Yin, X. Ma, C. H. F. Fung, Y. Liu, H. L. Yong, T. Y. Chen, C. Z. Peng, Z. B. Chen, and J. W. Pan, “ Source attack of decoy-state quantum key distribution using phase information,” *Physical Review A*, vol. 88, 022308 (2013).

[76] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, “Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution,” *Physical Review A*, vol. 87, 062313 (2013).

[77] M. S. Jiang, S. H. Sun, G. Z. Tang, X. C. Ma, C. Y. Li, and L. M. Liang, “Intrinsic imperfection of self-differencing single-photon detectors harms the security of high-speed quantum cryptography systems,” *Physical Review A*, vol. 88, 062335 (2013).

[78] A. N. Bugge, S. Sauge, A. M. M. Ghazali, J. Skaar, L. Lydersen, and V. Makarov, “Laser damage helps the eavesdropper in quantum cryptography,” *Physical Review Letters*, vol. 112, 070503 (2014).

[79] Z. L. Yuan, J. F. Dynes, and A. J. Shields, “Avoiding the blinding attack in QKD,” *Nature Photonics*, vol. 4, 800-801 (2010).

[80] L. Lydersen, V. Makarov, and J. Skaar, “Secure gated detection scheme for quantum cryptography,” *Physical Review A*, vol. 83, 032306 (2011).

[81] T. Honjo, M. Fujiwara, K. Shimizu, and K. Tamaki,” Countermeasure against tailored bright illumination attack for DPS-QKD,” *Optics Express*, vol. 21, 2667-2673 (2013).

[82] M. Alhussein, K. Inoue, and T. Honjo, “Monitoring coincident clicks in differential-quadrature-phase shift QKD to reveal detector blinding and control attacks,” *Japanese Journal of Applied Physics*, vol. 58, 012006 (2019).

[83] A. R. Dixon, J. F. Dynes, M. Lucamarini, B. Fröhlich, A. W. Sharpe, A. Plews, W. Tam, Z. L. Yuan, Y. Tanizawa, H. Sato, S. Kawamura, M. Fujiwara, M. Sasaki, and A. J. Shields, "Quantum key distribution with hacking countermeasures and long term field trial," *Scientific Report,* vol. 7, 1978-1-9 (2017).

[84] V. Makarov, Quantum cryptography and quantum cryptanalysis, Doctoral thesis, Norwegian University of Science and Technology (2007).

[85] R. H. Hadfield, "Single-photon detectors for optical quantum information applications," *Nature Photonics,* vol. 3, 696–705(2009).

[86] N. Namekata, S. Adachi, and S. Inoue, "1.5 GHz single-photon detection at telecommunication wavelengths using sinusoidally gated InGaAs/InP avalanche photodiode," *Optics Express,* vol. 17, 6275–6282 (2009).

[87] J. Zhang, R. Thew, C. Barreiro, and H. Zbinden, "Practical fast gate rate InGaAs/InP single-photon avalanche photodiodes," *Applied Physics Letters,* vol. 95, 091103 (2009).

[88] Z. L. Yuan, A. W. Sharpe, J. F. Dynes, A. R. Dixon, and A. J. Shields, "Multi-gigahertz operation of photon counting InGaAs avalanche photodiodes," *Applied Physics Letters,* vol. 96, 071101 (2010).

[89] J. Zhang, P. Eraerds, N. Walenta, C. Barreiro, R. Thew, and H. Zbinden, "2.23 GHz gating InGaAs/InP single-photon avalanche diode for quantum key distribution," *in Proceedings of the SPIE - The International Society for Optical Engineering*, vol. 7681, 76810Z (2010). (edited by M. A. Itzler and J. C. Campbell).

[90] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Review of Modern Physics,* vol. 81, 1301-1352 (2009).

[91] V. Scarani and C. Kurtsiefer, "The black paper of quantum cryptography: real implementation problems," arXiv:0906.4547v1 [quant-ph].

[92] V. Makarov and J. Skaar, "Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols," *Quantum Information & Computation*, vol. 8, 622–635 (2008).

[93] L. Lydersen and J. Skaar, “Security of quantum key distribution with bit and basis dependent detector flaws,” *Quantum Information & Computation*, vol. 10, 60–76 (2010).

[94] P. M. Nielsen, C. Schori, J. L. Sørensen, L. Salvail, I. Damgård, and E. Polzik, “Experimental quantum key distribution with proven security against realistic attacks,” *Journal of Modern Optics*, vol. 48, 1921–1942 (2001).

[95] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, “Security proof of quantum key distribution with detection efficiency mismatch,” *Quantum Information & Computation*, vol. 9, 131–165 (2009).

[96] V. Makarov, “Controlling passively quenched single photon detectors by bright light,” *New Journal of Physics*, vol. 11, 065003 (2009).

[97] S. Sauge, L. Lydersen, A. Anisimov, J. Skaar, and V. Makarov, “Controlling an actively-quenched single photon detector with bright light,” arXiv:0809.3408 [quant-ph].

[98] L. Lydersen, J. Skaar, and V. Makarov, “Tailored bright illumination attack on distributed-phase-reference protocols,” *Journal of Modern Optics*, vol. 58, 680–685 (2011).

[99] Z. L. Yuana, J. F. Dynes, and A. J. Shields, “Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography,” *Applied Physics Letters*, vol. 98, 231104 (2011).

[100] Z. L. Yuan, J. F. Dynes, and A. J. Shields, “Avoiding the blinding attack in QKD,” *Nature Photonics*, vol. 4, 800-801 (2010).

[101] J. Wang, H. Wang, X. Qin, Z. Wei, and Z. Zhang, “The countermeasures against the blinding attack in quantum key distribution,” *The European Physical Journal D*, vol.70, 5 (2016).

[102] M. Alhussein, K. Inoue, and T. Honjo, “BB84 and DQPS-QKD experiments using one polarization-insensitive measurement setup with a countermeasure against detector blinding and control attacks,” *Conference on Lasers and Electro-Optics (CLEO)*, paper JTu2A.28, USA (2019).

[103] M. Alhussein and K. Inoue,” Differential phase shift quantum key distribution with variable loss revealing blinding and control side-channel attacks,” *Japanese Journal of Applied Physics*, vol. 58, 102001 (2019).

[104] E. Waks, H. Takesue, and Y. Yamamoto, “Security of differential-phase-shift quantum key distribution against individual attacks,” *Physical Review A*, vol. 73, 012344 (2006).

Publication list

Journal Publications

1) Muataz Alhussein, Kyo Inoue, and Toshimori Honjo, "Monitoring coincident clicks in differential-quadrature-phase shift QKD to reveal detector blinding and control attacks," Japanese Journal of Applied Physics, vol. 58, 012006 (2019). (Chap. 4)

2) Muataz Alhussein, and Kyo Inoue, "Differential phase shift quantum key distribution with variable loss revealing blinding and control side-channel attacks," Japanese Journal of Applied Physics, vol. 58, 102001 (2019). (Chap. 6)

International conference (refereed)

1) Muataz Alhussein and Kyo Inoue, "Encrypting-deviced QKD working as measurement device independent system," International Conference on Quantum Communication, Measurement and Computing (QCMC), paper 42, USA, March 2018.

2) Muataz Alhussein and Kyo Inoue, "MDI-DPS-QKD utilizing QSS setup," 7th International Conference on Quantum Cryptography (QCrypt), paper We458, UK, September 2017.

3) Muataz Alhussein and Kyo Inoue, Toshimori Honjo, "BB84 and DQPS-QKD experiments using one polarization-insensitive measurement setup with a countermeasure against detector blinding and control attacks," Conference on Lasers and Electro-Optics (CLEO), paper JTu2A.28, USA, May 2019. (Chap. 5)

Domestic conference (not refereed)

1) Muataz Alhussein and Kyo Inoue, “MDI-DPS-QKD with no joint measurement,” Japanese Society of Applied Physics (JSAP), 5p-A414-4, Japan, September 2017.

2) Muataz Alhussein and Kyo Inoue, “Encrypting-device QKD working as a measurement device independent system,” Japanese Society of Applied Physics (JSAP), 19a-A302-9, Japan, March 2018.

3) Muataz Alhussein and Kyo Inoue, “Monitoring coincident click in DQPS-QKD to prevent side-channel attacks manipulating single-photon detectors,” Japanese Society of Applied Physics (JSAP), 18a-438-5, Japan, September 2018.

4) Muataz Alhussein and Kyo Inoue, Toshimori Honjo, “BB84 experiment using one polarization-insensitive measurement setup with a countermeasure against blinding and controlling attack,” Japanese Society of Applied Physics (JSAP), 10p-S422-10, Japan, March 2019.