博士論文

Security of Quantum Key Distribution with Weak Coherent Pulses

（微弱コヒーレント光を用いた量子鍵配送の安全性証明）

川上　駿

Security of Quantum Key Distribution with Weak Coherent Pulses

A dissertation for the degree of
Doctor of Engineering

by

Shun Kawakami

Department of Applied Physics
Graduate School of Engineering
University of Tokyo

2017

Abstract

Quantum key distribution (QKD) allows two distant parties to share a secret key and realizes a communication with information-theoretic security by combining it with one-time-pad encryption. Since the Bennett-Brassard 1984 (BB84) protocol was proposed, a large number of researches on QKD have been conducted from both aspects of theory and implementations. For implementations of QKD, weak coherent pulses (WCP) are heavily used as optical signals because they are easily generated by typical lasers and attenuators. The security for QKD with WCP has been also studied along the development of the implementations.

In this thesis, the security analysis of the QKD with WCP is considered and further developed from two aspects. First, the security of the differential-quadrature-phase-shift (DQPS) protocol is proved. The DQPS protocol has essentially the same set up as the phase-encoding BB84 (PE-BB84) protocol, which is one of the most frequently demonstrated protocols. Since the known proof techniques for the BB84 protocol is not directly applicable, a modified approach is developed which is suitable for the DQPS protocol. As a result, the advantage of the DQPS protocol in the key generation rate over the PE-BB84 protocol is shown in the asymptotic limit where the size of communication data is assumed to be infinite.

Second, a new method for security analysis with finite-key size is proposed as a suitable method for QKD protocols using WCP. Differently from the current method based on simple random sampling, the proposed method relies on Bernoulli sampling, which is associated with binomial distribution. The security of the BB84 protocol is proved by using the Bernoulli-sampling method, enabling a simpler analysis with a smaller number of parameters to be estimated compared to the method with simple random sampling. The required number of detected signals to generate a secret key is shown to be smaller than 10^4, which is drastic improvement from the number $\sim 10^7$ obtained in the previous result. The proposed method is also applied to the DQPS protocol, and its advantage over the PE-BB84 protocol is certified even in the finite-key regime.

Acknowledgement

This thesis has been written based on much support and advice. In particular, I would like to thank Prof. Masato Koashi, who supervised me throughout my studies in graduate school. He was always ready to listen to student's concerns for both scientific and private matters. His bright insight and accurate advice helped me numerous times. I believe that I have developed an appreciation for science and a logical way of thinking from him.

In addition, I greatly thank my closest collaborator, Dr. Toshihiko Sasaki. It was always a pleasure to work with him and to benefit from his wide range of knowledge. He kindly responded to my research questions, as well as questions about general physics and mathematics. I also thank him for proofreading this thesis. Any remaining errors and omissions are solely my responsibility.

I have been fortunate to have researchers and discussion partners who are sophisticated in various fields. Many practical aspects of this thesis were improved due to comments from Dr. Ken-ichiro Yoshino. Yasunari Suzuki gave me helpful advice on both theoretical and practical aspects. I also had several discussions with Akihiro Mizutani and obtained beneficial ideas from him. The time I spent with them was quite valuable.

I thank Prof. Hoi-Kwong Lo and Prof. Norbert Lütkenhaus for providing me with opportunities to visit their labs and other support. Those experiences broadened my outlook in research. I am also grateful to their group members. In particular, Dr. Feihu Xu and Dr. Patrick Coles spared a lot of time for discussions, which have been utilized to write this thesis.

I have been financially supported by the MERIT program, which gave me precious experiences including interactions with students in other fields. I could enjoy a fruitful student life at the university thanks to its continuous support.

Finally, I thank my family members, Shoko, Junko and in particular, my father, Prof. Norio Kawakami, who gave me academic advice from the standpoint of a researcher in a different field.

Contents

Chapter 1

Introduction

1.1 Background of quantum key distribution

Quantum information theory not only allows us to understand quantum physics deeply through classical information theory but also gives us a brand-new applications to the present information technology. One of the applications with high possibility of realization is quantum cryptography, which is expected to be a part of the future-cryptographic system. While quantum cryptography has information-theoretic security, the security of most cryptography used in these days rely on the computational hardness assumption, in which some mathematical problems are supposed to be difficult to solve in practical time with the present computational resources and algorithms. This indicates that even if important information is strictly protected by the present cryptography, it might be decrypted by strong computational power or a new algorithm in the future. A famous example is Shor's algorithm [1] implemented with quantum computer. It is known to solve the prime-factorization problem in polynomial time to threaten the security of the RSA cryptography, which is widely used in the present communication system. Such an anxiety for the future development of computer science is needless as far as the quantum cryptography is concerned thanks to its security assured by information theory. Quantum cryptography is composed of two elements: secret-key cryptography and quantum key distribution (QKD). For secret-key cryptography, the information-theoretic security is proved if a secret key is used only one time and its length is not shorter than that of the plain text, which is called one-time pad [2]. The problem is to share a secret key between distant parties, and this is the purpose of the quantum key distribution.

The first QKD protocol was proposed by Bennett and Brassard in 1984 and is called the BB84 protocol [3]. Differently from the present cryptography where eavesdropping is generally undetectable, the intervention of an eavesdropper can be detected in the protocol by monitoring bit errors between two parties. In 1988, Bennett *et al.* also proposed the concept of the privacy

amplification [4]. They show that if the amount of eavesdropper's information is bounded, a secure key can be extracted by compressing the shared key by the corresponding amount. This opens the field of security proof of QKD, in which the amount of eavesdropped information is theoretically bounded based on the rules of quantum physics. In 1996, the first security proof of the BB84 protocol is given by Mayers [5], followed by Shor and Preskill [6] based on the ideas of Lo and Chau [7]. On the other hand, these proofs assume ideal situations where Alice sends a single photon and Bob also receives it. Furthermore, the proofs were asymptotic analysis where the key size is assumed to be infinite to eliminate the statistical fluctuation.

For implementations of quantum key distribution, the behaviors of practical devices such as lasers and detectors deviate from the ideal mathematical model. In particular, the effect of light sources emitting multiple photons is serious because there is a photon-number-splitting (PNS) attack [8], in which Eve can obtain the full information of a secret key without disturbing the signal by using a part of multiple photons. The first security proof considering this effect is conducted by Inamori *et al.* in 2001 [9]. Later Gottesmann *et al.* proposed a quite simple concept of "tagging" to treat the multiple-photon emissions [10]. They pointed out that a round where the sender emits multiple photons and a round where she emits a single photon can be in principle classified if the optical phase of each signal is randomized. A round with multiple photons is regarded as tagged and considered to be insecure, while a round with a single photon is regarded as secure by applying the security proofs for the single-photon protocol. By combining the tagging idea with the later security proof which does not require the specific model of the receivers [11, 12, 13], the security of various practical QKD protocols including the BB84 protocols can be proved with simple theory [14, 15, 16, 17].

Another theoretical problem in practical situations is the security proof considering the effect of finite key size. Since the security analysis contains estimations of parameters related to leaked information, statistical fluctuations due to the finiteness must be taken into account, which is called finite-key analysis. Although there appeared security proofs with finite-key analysis based on Mayer's proof [9] and Shor and Preskill's proof [18, 19], these earlier results did not follow the security definition with composability [20, 21], which most of the current security proofs rely on. On the other hand, several proofs [22, 23] with composable security definition used law of large numbers for parameter estimations, which resulted in low key generation rate if the size of exchanged data is limited. It is expected that a simple security analysis with a smaller number of estimated parameters achieves higher key rate due to the small overhead for finite-size effect. Many of the current security proofs [24, 15, 16, 17] with composable finite-key analysis use random sampling theory or Azuma's inequality [25] as the estimation methods.

As theoretical aspects of QKD develop, many implementations of QKD were conducted in laboratories, on fields [26, 27, 28] and even in the space [29, 30, 31]. For the implementations in

laboratories and on fields, a signal light is usually guided by optical fibers, in which the information tends to be encoded on the optical phase of weak coherent pulses (WCP). One of the benefits to use the phase-encoding method is that it can be conducted with simple set up using the current technology. The simplicity is desired not only because of a lower cost and a higher clock rate, but also because complicated systems and procedures tend to impose severe restrictions on the model of the practical apparatus, and to suffer from a large overhead involved in the finite-key analysis. The BB84 protocol with phase encoding (Phase-encoding BB84, PE-BB84 henceforth) [3, 32], which uses four relative phases $\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$ between two neighboring pulses, is one of the simplest QKD implementations among phase-encoding protocols. In the PE-BB84 protocol, the sender and the receiver only need phase modulators and a passive Mach-Zehnder interferometer with two detectors. With its established security [5, 6, 10, 12], a number of demonstrations have so far been reported [33, 34, 35].

For long-distance communication, the laser-based BB84 protocol suffers from PNS attacks. It is often used with decoy-state method [36, 37, 38] to add protection against such attacks, but the decoy-state method sacrifices the simplicity of the PE-BB84 protocol, requiring additional devices as well as severer physical assumptions on the light source. It is common to assume Poissonian statistics of the photon number, and an attempt to relax it into conditions on the general photon number distribution still involves infinite number of inequalities [39]. In contrast, several protocols have been proposed to achieve protection from PNS attacks without decoy states. The differential-phase-shift (DPS) protocol has robustness against PNS attacks while retaining (or even improving) the simplicity of the PE-BB84 protocol, and the demonstration with a high clock rate was conducted [40]. In 2014, the round-robin DPS (RR-DPS) protocol was proposed [41] as a variant of DPS protocol, which is numerically shown to achieve higher key generation rate compared to the decoy-state BB84 protocol, but its implementations [42, 43, 44, 45] are not simple because of an additional element which is required in the receiver's apparatus to measure relative phases of two pulses with various intervals.

1.2 Contributions of this thesis

For the purpose of achieving a higher key generation rate with a simpler protocol, in this thesis two contributions are shown in terms of the security of QKD using practical WCP. The first one is the security proof of the differential-quadrature-phase-shift protocol (DQPS) protocol [46] in asymptotic-key regime. This work was published in [47]. The DQPS protocol was proposed by Iwai and Inoue in 2009 and is regarded as a variant of the DPS protocol as well as the PE-BB84 protocol. It is implemented with essentially the same set up as the PE-BB84 protocol without sacrificing its simplicity. The security of the DQPS protocol is proved by modifying the

tagging idea in this thesis. The result shows that its secure key rate is eight-third as high as that of the PE-BB84 protocol in the asymptotic limit. Practical aspects of the DQPS protocol is also investigated, in which the calibration method for light source is shown to be as simple as that of the PE-BB84 protocol.

The second contribution is the proposition of a new method for finite-key analysis. While most of the finite-key analysis is based on simple random sampling, the proposed method relies on Bernoulli sampling, which is associated to binomial distribution. This work was motivated by the finite-key analysis for the DQPS protocol, but it can be applied to various kinds of protocols, such as the BB84 protocol, the six-state protocol [48], and high-dimensional QKD protocols [49, 50]. In particular, the method enables simpler analysis with less estimation process for the WCP-BB84 protocol compared to the analysis with simple random sampling. The required number of detected signals to generate a secure key reduces to 10^4 from 10^7, which was obtained in the previous work [23]. Furthermore, by applying the analysis to the DQPS protocol, its advantage of the key rate over the PE-BB84 protocol is confirmed also in the finite-key regime.

1.3 Organization of this thesis

This thesis is organized as follows.

In Chapter 2, basic ideas of QKD are introduced. First, we summarize the concepts and notations used in this thesis. Next, various elements of QKD protocol (devices, procedures) are shown along with their assumptions. As an example of a QKD protocol, the BB84 protocol is described. The security definition of QKD is also given in this chapter.

In Chapter 3, the security of the BB84 protocol is proved based on the proof with complementarity [12]. The useful tools for security proof, source replacement, phase error, and a virtual protocol are introduced. By using those tools, we prove the security of the BB84 protocol under the assumption that the number of phase errors are bounded.

In Chapter 4, QKD using WCP are discussed from both theoretical and practical aspects. First, PNS attacks are described. After GLLP's tagging idea is introduced, the dependence of secret-key length on phase errors is derived for WCP-BB84 protocol by using the tagging idea. Based on the resulting key length in the asymptotic limit, we analyze the effect of PNS attacks on the WCP-BB84 protocol. For practical aspects, the PE-BB84 protocol is introduced as a specific form of the WCP-BB84 protocol. Decoy-state method is also discussed with its current practical problems. Finally, the DPS protocol is introduced with its variant, the RR-DPS protocol.

In Chapter 5, the security of the DQPS protocol is proved in the asymptotic limit. After describing the protocol and assumptions, the security proof is conducted with construction of a virtual protocol and an alternative rule of tagging. The result of numerical calculation is shown

to make comparison to the PE-BB84 protocol in terms of key-generation rate. We discuss the generality of the proof and simplicity of the DQPS protocol, and a possible improvement for the proof is suggested.

In Chapter 6, the method for finite-key analysis based on Bernoulli sampling is proposed. First the sampling problems in security analysis are introduced along with their related statistics. The proposed method is applied to the ideal BB84 protocol and WCP-BB84 protocol to make comparison with the conventional method with simple random sampling. The proposed method is also applied to the DQPS protocol to confirm its advantage over the PE-BB84 protocol in the finite-key regime. Finally, the obtained results are summarized and outlooks related to this work are discussed.

In Chapter 7, the summary of my researches and prospects for the future works are presented.

Chapter 2

Basic ideas of quantum key distribution

Quantum cryptography enables communication with information-theoretic security. Although its security depends on the whole system [28] including one-time-pad communication and secret-key management, this thesis focuses on "quantum layer" of quantum cryptography, namely, quantum key distribution (QKD). In this thesis, we treat QKD with two-level system (qubit-based QKD) rather than qudit-based QKD [49, 50] and continuous-variable QKD [51]. This chapter is for introduction of basic ideas used in QKD. Sec. 2.1 represents the tools and notations used throughout this thesis. The typical structure and assumptions of QKD protocols are shown in Sec 2.2. The security definition of QKD protocol is given in Sec 2.3.

2.1 Preliminaries

For later convenience, we introduce several basic concepts and properties in quantum information theory, and summarize notations frequently used in this thesis.

2.1.1 Tools of quantum information theory

Here we introduce several useful tools of quantum information theory: POVM, CPTP map, trace distance, and fidelity.

POVM

POVM (positive operator valued measure) is one of the forms representing quantum measurement. POVM represents a set of positive operators $\{\hat{E}_i\}$ satisfying $\sum_i \hat{E}_i = \hat{\mathbb{1}}$ where $\hat{\mathbb{1}}$ is the identity operator. Each element of the set $\hat{E}_i$ is called POVM element. Any physical measurement can be represented with POVM. For a density operator $\hat{\rho}$, the probability that the outcome

corresponding to $\hat{E}_i$ is obtained is given by $\mathrm{Tr}(\hat{\rho}\hat{E}_i)$.

CPTP map

CPTP map is short for completely-positive and trace-preserving map. A map $\mathcal{E} : \hat{\rho} \mapsto \mathcal{E}(\hat{\rho})$ acting on a density operator $\hat{\rho}$ is called a completely-positive map if

$$(\mathbb{1} \otimes \mathcal{E})(\hat{\rho}') \geq 0 \tag{2.1}$$

holds where $\mathbb{1}$ is the identity map on the auxiliary system and $\hat{\rho}'$ is a density operator on the joint system. The map $\mathcal{E}$ is called a trace-preserving map if

$$\mathrm{Tr}(\mathcal{E}(\hat{\rho})) = 1 \tag{2.2}$$

for any normalized density operator $\hat{\rho}$. Note that any input-output relation which is physically realizable is a CPTP map. A CPTP map can be expressed with operator-sum representation as

$$\mathcal{E}(\hat{\rho}) = \sum_i \hat{K}_i \hat{\rho} \hat{K}_i^\dagger, \tag{2.3}$$

where $\hat{K}_i$ is an operator acting on the same Hilbert space as $\hat{\rho}$, and $\sum_i \hat{K}_i^\dagger \hat{K}_i = \hat{\mathbb{1}}$ with the identity operator $\hat{\mathbb{1}}$.

Trace distance

Trace distance represents distance between two quantum states. We define [*1)] trace distance between two states $\hat{\rho}$ and $\hat{\sigma}$ as $\frac{1}{2}\| \hat{\rho} - \hat{\sigma} \|$ with trace norm $\|A\| := \mathrm{Tr}(\sqrt{AA^\dagger})$. The triangle inequality holds in terms of trace distance:

$$\frac{1}{2}\| \hat{\rho} - \hat{\sigma} \| + \frac{1}{2}\| \hat{\sigma} - \hat{\tau} \| \geq \frac{1}{2}\| \hat{\rho} - \hat{\tau} \|. \tag{2.4}$$

Trace distance has a property of *monotonicity*, that is, for any CPTP map $\mathcal{E}$,

$$\frac{1}{2}\| \mathcal{E}(\hat{\rho}) - \mathcal{E}(\hat{\sigma}) \| \leq \frac{1}{2}\| \hat{\rho} - \hat{\sigma} \| \tag{2.5}$$

is satisfied.

Fidelity

Fidelity is another distance measure for quantum information. We define [*2)] fidelity of two states $\hat{\rho}$ and $\hat{\sigma}$ as

$$F(\hat{\rho}, \hat{\sigma}) := \left\| \sqrt{\hat{\rho}}\sqrt{\hat{\sigma}} \right\|^2. \tag{2.6}$$

[*1)] The definition is not unique, and sometimes $\| \hat{\rho} - \hat{\sigma} \|$ is called trace distance.

[*2)] The definition is not unique, and sometimes $\left\| \sqrt{\hat{\rho}}\sqrt{\hat{\sigma}} \right\|$ is called fidelity.

Uhlmann's theorem [52] holds in terms of fidelity:

$$F(\hat{\rho},\hat{\sigma}) = \max_{|\psi_\sigma\rangle} |\langle\psi_\rho|\psi_\sigma\rangle|^2, \tag{2.7}$$

where $|\psi_\rho\rangle$ and $|\psi_\sigma\rangle$ are purifications of $\hat{\rho}$ and $\hat{\sigma}$, respectively. Fidelity also has a property of monotonicity: For any CPTP map $\mathcal{E}$,

$$F(\mathcal{E}(\hat{\rho}),\mathcal{E}(\hat{\sigma})) \geq F(\hat{\rho},\hat{\sigma}) \tag{2.8}$$

holds. Trace distance is upper-bounded by fidelity as

$$\frac{1}{2}\| \hat{\rho} - \hat{\sigma} \| \leq \sqrt{1 - F(\hat{\rho},\hat{\sigma})}. \tag{2.9}$$

2.1.2 Notations in this thesis

Here, we summarize notations used in this thesis. We adopt an abuse of notation to use the same symbol for a random variable $\tilde{n}$ and its value n, whenever the distinction is obvious. For example, we denote $\Pr(n > 3)$ instead of $\Pr(\tilde{n} > 3)$. We denote by $\Pr(n)$ the probability mass function $\Pr(\tilde{n} = n)$. Similarly, we use $\Pr(n \mid m)$ instead of $\Pr(\tilde{n} = n \mid \tilde{m} = m)$.

A bold character, for example $\boldsymbol{V}$, represents a vector of bit strings where addition of two vectors is defined by addition modulo 2 for each element. We use the notation $|\boldsymbol{V}|$ as the length of $\boldsymbol{V}$, and use $\mathrm{wt}(\boldsymbol{V})$ as weight of $\boldsymbol{V}$, namely, the number of 1s contained in $\boldsymbol{V}$. We define the product of two vectors $\boldsymbol{V}\cdot\boldsymbol{W}$ (where $|\boldsymbol{V}| = |\boldsymbol{W}|$) as $\boldsymbol{V}\cdot\boldsymbol{W} = V_1W_1 + V_2W_2 + ...V_{|\boldsymbol{V}|}W_{|\boldsymbol{W}|}$ where the plus sign represents addition modulo 2 (hence $\boldsymbol{V}\cdot\boldsymbol{W} \in \{0,1\}$). For example, for $\boldsymbol{V} = (0,1,0,0,1)$ and $\boldsymbol{W} = (1,0,0,0,1)$, we have $|\boldsymbol{V}| = 5$, $\mathrm{wt}(\boldsymbol{V}) = 2$ and $\boldsymbol{V}\cdot\boldsymbol{W} = 1$.

We define the following increasing function of x defined for $x \geq 0$:

$$h(x) = \begin{cases} -x\log_2 x - (1-x)\log_2(1-x) & (0 \leq x \leq 1/2) \\ 1 & (x > 1/2). \end{cases} \tag{2.10}$$

For $0 \leq x \leq 1/2$, $h(x)$ is identical to the binary-entropy function.

This thesis mainly deals with the BB84 protocol and the DQPS protocol, both of which use two bases, one for generating a secret key (data basis) and the other for monitoring leaked information (check basis). Throughout this thesis except Chapter 5, we assign the Z basis to the data basis, and the X basis to the check basis.

We define $|0_Z\rangle$ and $|1_Z\rangle$ as basis vectors of Z basis on a qubit system, $|0_X\rangle := (|0_Z\rangle + |1_Z\rangle)/\sqrt{2}$ and $|1_X\rangle := (|0_Z\rangle - |1_Z\rangle)/\sqrt{2}$ as those of X basis. When the same notations are used for an optical signal (usually denoted by system S), it should be understood that they refer to the states in the subspace of a single photon contained in two modes, such as polarizations. For simplicity, we

denote $|0\rangle \otimes |0\rangle$ as $|00\rangle$. The ket notation characterized by vector represents $|\boldsymbol{V}\rangle := \bigotimes_{i=1}^{|\boldsymbol{V}|} |V_i\rangle$. The four Bell states are represented by $|\Phi^{\pm}\rangle$ and $|\Psi^{\pm}\rangle$ where

$$|\Phi^{\pm}\rangle := \frac{1}{\sqrt{2}}(|00_Z\rangle \pm |11_Z\rangle), \tag{2.11}$$

$$|\Psi^{\pm}\rangle := \frac{1}{\sqrt{2}}(|01_Z\rangle \pm |10_Z\rangle). \tag{2.12}$$

2.2 QKD protocol

Although there are various types of QKD protocols, they generally have similar components and procedures. In this section we introduce basic components of QKD with their assumptions and the procedures in QKD protocol. We also introduce the BB84 protocol as an example of QKD protocol.

2.2.1 Components and assumptions

We divide QKD components into the sender's devices, the receiver's devices, quantum channel and classical channel to clarify the assumptions usually adopted in QKD protocols. In most QKD protocols, there appear legitimate parties Alice and Bob who want to share secret keys and eavesdropper Eve. Throughout this thesis, we assume that Alice is a signal sender and Bob is a receiver.

Alice's (sender's) devices

Alice's devices are mainly used for preparing quantum states. One of essential devices at Alice's site is a light source. From the viewpoint of simplicity and high repetition rate, an attenuated laser is usually used as a signal source, while QKD with single-photon source has been demonstrated [53] and sophisticated ideas for sources using spontaneous parametric down conversion were proposed [54, 55]. Random number generator is also necessary for basis choice, generating a raw key bit, randomization of optical phase and generating hash functions and so on. Although we assume that perfect (uniform and independent) random numbers can be prepared, practical random number generators have imperfections causing non-uniformity of random numbers and correlations to outside systems. To fill the gap from the practical side, researches on quantum random number generator (QRNG) have been conducted. In these days, QRNG using the randomness of which-path information of photon is commercially available with the rate 4 Mbits/s [56], and faster one with 6 Gbits/s was demonstrated based on quantum-phase fluctuations [57]. As is referred to as "side channel attack" in the current cryptography system, in practice there are

attacks using unintended information leak (such as feeble electromagnetic wave from devices), and hence the appropriate countermeasures are required. On the other hand, in this thesis we assume that internal information of the devices is not leaked outside.

Bob's (receiver's) devices

The role of Bob's devices is to carry out measurement on quantum states to obtain a key bit. A main device at Bob's site is a detector. In practice, threshold detectors, which can tell a single photon or more from vacuum, are often used without sacrificing the security. In several QKD demonstrations with high clock rate [40, 53], superconducting single photon detectors (SSPDs) were used. Recently, SSPDs with high detection efficiency (93 %), low dark count rate (1 c.p.s) and low timing jitter (150 ps) were developed [58]. A random number generator is also necessary if Bob needs basis choice in the protocol. A larger number of side-channel attacks (security loopholes) are known for the receiver's devices [59, 60, 61, 62] than the sender's devices, which leads to the idea of measurement-device-independent (MDI) QKD [63]. In MDI QKD, both Alice and Bob are senders and the receiver's devices are possessed by an untrusted party "Charlie". The protocols dealt in this thesis are based on conventional Alice's state preparation and Bob's measurement. We assume that Bob's devices are also side-channel free similarly to Alice's devices.

Quantum channel

Quantum channel is used for communication with quantum states between Alice and Bob. For practical aspects, optical fibers or free space are suitable as quantum channel for light. Optical fibers are used for most QKD implementations on the ground [26, 27, 28], while the use of free space is expected for implementations involving satellites [29, 30, 31, 64]. We impose no assumption on quantum channel and hence Eve can conduct any physical operation on transmitting signal without constraints on technology. For example, she can use noiseless and lossless channel in principle.

Classical channel

Classical channel is used for all communication between Alice and Bob except the one with quantum channel. While the information on classical channel is publicly open, we assume that the information can not be tampered. This assumption is realized by Wegman-Carter authentication [65], for example, consuming a small number of secret key ($\sim$ logarithm of the communication-data size). Thus, Alice and Bob need to share secret keys in advance, which implies that the role of QKD is not secret-key generation, but secret-key amplification. If we compromise the information-theoretic security, the authentication is conducted by public-key cryptography relying on computational-hardness assumptions, which partially makes sense since

it is sufficient that the authentication succeeds at the present time to make the secret key shared through QKD be secure even in the future.

2.2.2 Procedures

QKD protocols are composed of manipulation of quantum states and classical post processing. In post processing, the procedures are classified as sifting, parameter estimation, error correction and privacy amplification. Here we explain each procedure and introduce several related works.

Quantum manipulations

Quantum manipulations include Alice's preparation of a quantum state, transmission of the state and Bob's measurement. Alice prepares a quantum state based on a random bit and basis choice (if the protocol uses multiple bases) and sends it to Bob through quantum channel. Bob makes measurement on the state to obtain one of outcomes {0, 1, no-detection} and additional information depending on protocols. We name the series of the above procedures for a single state as a "round". Alice and Bob repeat the round many times.

Sifting

In sifting process, Alice and Bob communicate with classical channel to determine whether each round of the protocol is valid or invalid. For example, a round with no detection at Bob's site is invalid, and a round with basis mismatch between Alice and Bob is also regarded as invalid. Some rounds may be chosen as samples for the following parameter estimation process. Alice and Bob obtain bit strings called "sifted key" by concatenating the bits on valid and no-sample rounds. In several works [13, 15, 16], sifting process is conducted at each round of the protocol. On the other hand, Pfister *et al*. have recently pointed out [66] that the conventional security proof based on simple random sampling can not be applied if we disclose the basis choice at each round of the protocol. Thus, if one prefers tight security analysis currently used, sifting process is desired to be conducted after all rounds are over in practical QKD protocols.

Parameter estimation

To certify the security of the protocol, we require parameters which characterizes Eve's intervention on quantum channel. For this, Alice and Bob disclose sample bits through classical channel to obtain the statistics of bit errors. Based on the resulting statistics, Alice and Bob determine whether they proceed to the following steps or abort the protocol. For example, if the number of errors is too large compared to the data size, they abort the protocol.

Error correction

Even if Eve is absent, Bob's sifted key is generally different from Alice's one because of the noise inherent in quantum channel. In error correction process, Alice and Bob correct the obtained keys to make it coincide with each other's one through the communication with classical channel. Based on the estimated bit-error rate on the sifted key, Alice and Bob apply an appropriate error-correcting code. If multiple bases are used in the protocol and bit errors on sifted key do not contribute to the security analysis (e.g. in BB84), the estimation of error rate on the sifted key can be omitted. Instead, they apply an error-correcting code with predetermined communication cost followed by verification process. In verification process, Alice and Bob compare a small number of hash values computed from the sifted keys, and if those values are different between Alice and Bob, they abort the protocol. In practice, the low-density parity-check (LDPC) code [67] is often used for error correction. For fast implementation of LDPC code, the size of a sifted key is desired to be fixed.

Privacy amplification

Privacy amplification is the process to obtain a secret key decoupling from Eve's system. The concept of privacy amplification was proposed and developed by Bennett *et al*. [4, 68] in early days. The idea is that if the amount of information leaked to Eve is upper-bounded, the secret key can be generated by applying an appropriate compressing function on the sifted key, which shortens the key length by the amount corresponding to the leaked information. The bound on leaked information is not directly observed and has to be theoretically determined based on estimated parameters. One of compressing functions established for the privacy amplification is the universal$_2$ hash function [69], and Toeplitz matrix is frequently used in practice due to its small computational complexity. Recently, Hayashi and Tsurumaru constructed another hash functions [70] which belong to a broader class than universal$_2$ hash function. These functions require less random seeds as well as enables us to treat their non-uniformity, which is useful considering the imperfection of random number generators. Although the concept of privacy amplification was proposed mainly for quantum key distribution, recently it has been applied to other fields such as randomness extraction [71] for quantum random number generators.

2.2.3 BB84 protocol

As an example of QKD protocol, we introduce the Bennett-Brassard 1984 (BB84) protocol [3]. In the protocol, Alice and Bob independently chooses two bases (Z basis and X basis) with a biased probability. The final key is generated only from Z-basis data, while X-basis data is used for leak

monitoring to determine the amount for privacy amplification. We say a round is "$Z(X)$-labeled" if both Alice and Bob chose $Z(X)$ basis and photon detections are reported at that round. The number of total rounds is fixed to be $n_{\rm rep}$, and hence the size of the final key is variable.

The protocol proceeds as follows with predetermined parameters $\tilde{p}_Z$, $\tilde{p}_X = 1 - \tilde{p}_Z$ and $n_{\rm rep}$. Following the classification in the previous section, Steps (1)-(4) correspond to quantum manipulations, Steps (5) and (6) represent sifting process and Step (7) is parameter estimation.

(1) Alice chooses Z basis or X basis with probability $\tilde{p}_Z$ and $\tilde{p}_X$, respectively. She chooses a uniformly random bit $\{0, 1\}$.
(2) Alice prepares one of states $\{\hat{\rho}_{Z,0}, \hat{\rho}_{Z,1}, \hat{\rho}_{X,0}, \hat{\rho}_{X,1}\}$ based on the selected basis and bit. She sends the prepared state to Bob over the quantum channel.
(3) Bob chooses Z basis or X basis with probability $\tilde{p}_Z$ and $\tilde{p}_X$, respectively. He measures a received state in chosen basis and obtains the outcome {0, 1, no-detection}.
(4) They repeat the sequence (1) to (3) (which we call a round) by $n_{\rm rep}$ times.
(5) Bob publicly announces whether each round has resulted in a detection or not. Let $n_{\rm det}$ be the number of rounds with detection.
(6) Alice and Bob disclose all of their basis choices. They define sifted keys $\boldsymbol{\kappa}_{A,Z}$ and $\boldsymbol{\kappa}_{B,Z}$ by concatenating the bits for the Z-labeled rounds, and similarly define $\boldsymbol{\kappa}_{A,X}$ and $\boldsymbol{\kappa}_{B,X}$ for the X-labeled rounds. Let their sizes be $n_Z := |\boldsymbol{\kappa}_{A,Z}| = |\boldsymbol{\kappa}_{B,Z}|$ and $n_X := |\boldsymbol{\kappa}_{A,X}| = |\boldsymbol{\kappa}_{B,X}|$.
(7) They disclose and compare $\boldsymbol{\kappa}_{A,X}$ and $\boldsymbol{\kappa}_{B,X}$ to determine the number of bit errors k_X included in them. Let ω represents the following three observed numbers:

$$\omega := (k_X, n_X, n_Z). \tag{2.13}$$

Through public discussion, Alice and Bob determine whether they abort the protocol or not. If the protocol does not abort, they determine the final key size $l(\omega)$ (≥ 0).
(8) Through public discussion, Bob corrects his keys $\boldsymbol{\kappa}_{B,Z}$ to make it coincide with Alice's key $\boldsymbol{\kappa}_{A,Z}$ and obtains $\boldsymbol{\kappa}^{\rm cor}_{B,Z}$ ($|\boldsymbol{\kappa}^{\rm cor}_{B,Z}| = n_Z$).
(9) Alice and Bob conduct privacy amplification by shortening $\boldsymbol{\kappa}_{A,Z}$ and $\boldsymbol{\kappa}^{\rm cor}_{B,Z}$ to obtain final keys $\boldsymbol{\kappa}^{\rm fin}_{A,Z}$ and $\boldsymbol{\kappa}^{\rm fin}_{B,Z}$ of size l.

Intuitively, security of the BB84 protocol is ensured by the uncertainty principle: If Eve attempts to access information for Z basis, then information for X basis is disturbed. Although the BB84 protocol is the first QKD protocol, it is as well the most frequently demonstrated protocol even in the current QKD implementations. A possible reason for the popularity is the simplicity of the protocol, but another remarkable property is that the BB84 protocol also has established security with simple proof, which originates from the symmetry of the Z and X bases. In Chapter 3,

we show the simple security analysis of the BB84 protocol by using the proof of complementarity [12].

2.3 Security definition

Here we introduce the security criteria with "composability" which are currently accepted in the field of QKD. The concept of composable security originates in modern cryptography (not quantum) [72] and was first discussed in the context of QKD by Ben-Or *et al*. [21, 73], followed by Renner *et al*. [20] and Unruh [74]. Roughly speaking, composable security implies that if two protocols are respectively shown to be almost secure, the protocol combining the two protocols is also almost secure. This property is important because secret keys generated from a QKD protocol are used in other protocols, such as one-time pad and authentication of classical channel (see Sec. 2.2.1).

As is adopted in the current security proofs [13, 75, 15, 16, 24, 76, 17], in this thesis we follow the composable security definition represented in Ref. [21]. For a bit strings $\boldsymbol{\kappa} \in \{\emptyset, 0, 1, 00, 01, 10, 11, 000, ...\}$, let us define $\{|\boldsymbol{\kappa}\rangle\}$ as a set of orthogonal bases on the space $\mathcal{H}_0 \oplus \mathcal{H}_1 \oplus \mathcal{H}_2 \oplus .... \oplus \mathcal{H}_{n_{\rm rep}}$ with each dimension of $\mathcal{H}_j$ being 2^j. Let $\hat{\rho}^{\rm fin}_{ABE}$ be a state after finishing the protocol defined on the system A (Alice), B (Bob) and E (Eve), which is written as

$$\hat{\rho}^{\rm fin}_{ABE} := \sum_{\boldsymbol{\kappa}^{\rm fin}_{A,Z}, \boldsymbol{\kappa}^{\rm fin}_{B,Z}} \Pr(\boldsymbol{\kappa}^{\rm fin}_{A,Z}, \boldsymbol{\kappa}^{\rm fin}_{B,Z}) \, |\boldsymbol{\kappa}^{\rm fin}_{A,Z}, \boldsymbol{\kappa}^{\rm fin}_{B,Z}\rangle \langle \boldsymbol{\kappa}^{\rm fin}_{A,Z}, \boldsymbol{\kappa}^{\rm fin}_{B,Z}|_{AB} \otimes \hat{\rho}^{\rm fin}_{E}(\boldsymbol{\kappa}^{\rm fin}_{A,Z}, \boldsymbol{\kappa}^{\rm fin}_{B,Z}), \tag{2.14}$$

where $\Pr(\boldsymbol{\kappa}^{\rm fin}_{A,Z}, \boldsymbol{\kappa}^{\rm fin}_{B,Z})$ represents the probability that Alice and Bob obtain the final key $\boldsymbol{\kappa}^{\rm fin}_{A,Z}$ and $\boldsymbol{\kappa}^{\rm fin}_{B,Z}$, respectively, and $|\boldsymbol{\kappa}^{\rm fin}_{A,Z}, \boldsymbol{\kappa}^{\rm fin}_{B,Z}\rangle_{AB} := |\boldsymbol{\kappa}^{\rm fin}_{A,Z}\rangle_A \, |\boldsymbol{\kappa}^{\rm fin}_{B,Z}\rangle_B$. Let $\hat{\rho}^{\rm ideal}_{AE}$ be an ideal state where Alice's and Bob's final keys are uniform and independent of Eve's system (except final-key size l):

$$\hat{\rho}^{\rm ideal}_{ABE} := \sum_{l} \sum_{\boldsymbol{\kappa}:\ |\boldsymbol{\kappa}|=l} \Pr(l) \, \frac{1}{2^l} \, |\boldsymbol{\kappa}, \boldsymbol{\kappa}\rangle \langle \boldsymbol{\kappa}, \boldsymbol{\kappa}|_{AB} \otimes \hat{\rho}^{\rm fin}_{E}(l), \tag{2.15}$$

where $\Pr(l)$ represents the probability to obtain the final key of size l and $\hat{\rho}^{\rm fin}_{E}(l)$ is Eve's state conditioned on l, which are related to the parameters in the protocol as

$$\Pr(l) = \sum_{\boldsymbol{\kappa}^{\rm fin}_{A,Z}, \boldsymbol{\kappa}^{\rm fin}_{B,Z}:\ |\boldsymbol{\kappa}^{\rm fin}_{A,Z}|=|\boldsymbol{\kappa}^{\rm fin}_{B,Z}|=l} \Pr(\boldsymbol{\kappa}^{\rm fin}_{A,Z}, \boldsymbol{\kappa}^{\rm fin}_{B,Z}), \tag{2.16}$$

$$\hat{\rho}^{\rm fin}_{E}(l) := \frac{1}{\Pr(l)} \sum_{\boldsymbol{\kappa}^{\rm fin}_{A,Z}, \boldsymbol{\kappa}^{\rm fin}_{B,Z}:\ |\boldsymbol{\kappa}^{\rm fin}_{A,Z}|=|\boldsymbol{\kappa}^{\rm fin}_{B,Z}|=l} \Pr(\boldsymbol{\kappa}^{\rm fin}_{A,Z}, \boldsymbol{\kappa}^{\rm fin}_{B,Z}) \hat{\rho}^{\rm fin}_{E}(\boldsymbol{\kappa}^{\rm fin}_{A,Z}, \boldsymbol{\kappa}^{\rm fin}_{B,Z}). \tag{2.17}$$

Since it is practically impossible to obtain the final state as in the ideal form Eq. (2.15), we allow the small probability $\epsilon_{\rm sec}$ that the protocol is insecure. Such a concept is called $\epsilon_{\rm sec}$-security, and

its exact definition is described as follows.

Definition of $\epsilon_{\rm sec}$-security
The protocol is $\epsilon_{\rm sec}$-secure if and only if the trace distance between $\hat{\rho}^{\rm fin}_{ABE}$ and $\hat{\rho}^{\rm ideal}_{ABE}$ is no larger than $\epsilon_{\rm sec}$:

$$\frac{1}{2}\| \hat{\rho}^{\rm fin}_{ABE} - \hat{\rho}^{\rm ideal}_{ABE} \| \leq \epsilon_{\rm sec}. \tag{2.18}$$

Typically the value of $\epsilon_{\rm sec}$ is set to $\epsilon_{\rm sec} \sim 10^{-10}$.

For the convenience of security proof, $\epsilon_{\rm sec}$-security is usually divided into $\epsilon_{\rm c}$-correctness and $\epsilon_{\rm s}$-secrecy [77]. The protocol is called $\epsilon_{\rm c}$-correct if and only if

$$\Pr(\boldsymbol{\kappa}^{\rm fin}_{A,Z} \neq \boldsymbol{\kappa}^{\rm fin}_{B,Z}) \leq \epsilon_{\rm c}. \tag{2.19}$$

Define $\hat{\rho}^{\rm fin}_{AE}$ and $\hat{\rho}^{\rm ideal}_{AE}$ as

$$\hat{\rho}^{\rm fin}_{AE} := {\rm Tr}_B(\hat{\rho}^{\rm fin}_{ABE}) = \sum_{\boldsymbol{\kappa}^{\rm fin}_{A,Z}} \Pr(\boldsymbol{\kappa}^{\rm fin}_{A,Z}) \, |\boldsymbol{\kappa}^{\rm fin}_{A,Z}\rangle \langle \boldsymbol{\kappa}^{\rm fin}_{A,Z}|_A \otimes \hat{\rho}^{\rm fin}_E(\boldsymbol{\kappa}^{\rm fin}_{A,Z}) \tag{2.20}$$

$$\hat{\rho}^{\rm ideal}_{AE} := {\rm Tr}_B(\hat{\rho}^{\rm ideal}_{ABE}) = \sum_{l} \sum_{\boldsymbol{\kappa}:\ |\boldsymbol{\kappa}|=l} \Pr(l) \, \frac{1}{2^l} \, |\boldsymbol{\kappa}\rangle \langle \boldsymbol{\kappa}|_A \otimes \hat{\rho}^{\rm fin}_E(l). \tag{2.21}$$

The protocol is called $\epsilon_{\rm s}$-secret if and only if

$$\frac{1}{2}\| \hat{\rho}^{\rm fin}_{AE} - \hat{\rho}^{\rm ideal}_{AE} \| \leq \epsilon_{\rm s}. \tag{2.22}$$

By using the triangle inequality Eq. (2.4) in terms of trace distance, one can show that if the protocol is $\epsilon_{\rm c}$-correct and $\epsilon_{\rm s}$-secret, the protocol is also $\epsilon_{\rm sec}$-secure with $\epsilon_{\rm sec} = \epsilon_{\rm c} + \epsilon_{\rm s}$ (see Ref. [12], for example). It is useful to quantify $\epsilon_{\rm c}$-correctness and $\epsilon_{\rm s}$-secrecy separately. Since $\epsilon_{\rm c}$-correctness is ensured in the protocol through the verification process or estimation of bit errors, the target of security proof is to ensure $\epsilon_{\rm s}$-secrecy of the protocol.

Until the concept of composable security was generally accepted, the security of QKD was typically evaluated by Shannon mutual information $I(\boldsymbol{\kappa}^{\rm fin}_{A,Z}; K_E)$ [78] between Alice's final key $\boldsymbol{\kappa}^{\rm fin}_{A,Z}$ and Eve's classical strings K_E obtained by measurement on her system [9, 18, 19]. However, small $I(\boldsymbol{\kappa}^{\rm fin}_{A,Z}; K_E)$ does not necessarily means $\epsilon_{\rm s}$-secrecy with small $\epsilon_{\rm s}$. Ref. [21] shows that $\epsilon_{\rm s}$-secrecy is satisfied if

$$I(\boldsymbol{\kappa}^{\rm fin}_{A,Z}; K_E) \leq 2^{-(l+2)} \epsilon_{\rm s}^2, \tag{2.23}$$

where we fixed the value of $l = |\boldsymbol{\kappa}^{\rm fin}_{A,Z}|$ for simplicity. Later, the exponential dependence of the mutual information on the final key size as in Eq. (2.23) was shown [79] to be necessary as well as sufficient for $\epsilon_{\rm s}$-secrecy, which implies that the mutual information is not suitable as security definition.

Chapter 3

Security proof of the BB84 protocol

So far a large number of security proofs are given for various protocols, but the number of the security proofs for the BB84 protocol is outstanding compared to those for others. The reason is supposed to be that it has a beautiful symmetry of two conjugate observables, which enables a simple proof. Many security proofs for other protocols also use the property of two conjugate observables and they are regarded as a variant of the proof for the BB84 protocol. Thus, understanding the security proof for the BB84 protocol might be essential to address the security of general QKD protocols. The first security proof for the BB84 protocol was given by Mayers [5] although it was complicated. The simple proof using quantum error correction was proposed by Shor and Preskill in 2000 [6]. Later, the other simple proofs are suggested by Koashi in 2005 [11] and by Tomamichel *et al*. in 2012 [13]. In this chapter, the security of the BB84 protocol is shown with a method based on complementarity proposed by Koashi [11, 12]. The proofs includes finite-key analysis and satisfies the composable security definition [20, 21]. As a preliminary, three methods (mentioned above except Mayers') of security proofs currently used are introduced and compared in Sec 3.1. In Sec. 3.2, tools for security proof are introduced to use the proof with complementarity, containing replacement of state preparation, phase error and virtual protocol. By using those tools, the security of the BB84 protocol is shown based on the proof with complementarity in Sec. 3.3. The result of this chapter is applied to Chapter 5 and 6.

3.1 Three types of security proof

As far as the qubit-based protocols (*c f*. continuous variable QKD [51]) including the BB84 protocol are concerned, the security proofs which are valid for Eve's general attack are mainly classified into three types: the proof with entanglement distillation protocol (EDP) [7, 6], the proof with complementarity [11, 12] and the proof with entropic uncertainty principle [13]. We briefly

introduce those three proofs focusing on what concepts are used and what physical assumptions on devices are required.

Security proof with EDP

The security proof with EDP was originally proposed by Lo and Chau in 1999 [7]. They prove the security of the BBM92 protocol [80], in which an entangled photon pair is separately distributed to Alice and Bob, by using the ideas of entanglement distillation protocol [81, 82, 83]. Later in 2000, Shor and Preskill show that the security of the BB84 protocol is reduced to the proof of the BBM92 protocol [6]. The proof is based on simple CSS quantum error correction code [84, 85] and the security is evaluated how good both bit errors and phase errors (mentioned in Sec. 3.2.2) are corrected. On the other hand, it requires an assumption that Alice and Bob make ideal qubit measurements. The proof with EDP is used not only for the above two protocols but also for B92 protocol [86, 87], six-state protocol [48, 88], DPS protocol [89, 90] and so on.

Security proof with complementarity

The security proof with complementarity was proposed by Koashi in 2005 [11]. It follows the spirit of the first proof for the BB84 protocol given by Mayers [5], in which the security is analyzed with uncertainty principle at Alice's system. While it adopts the similar proof with EDP by using the idea of phase error correction, the bit error correction is separated from the security analysis and the security is evaluated how good phase errors are corrected. Compared to the proof with EDP, the physical assumption at receiver's devices is relaxed as follows:
Condition of the receiver ($*$): *The probability that a signal is detected at the receiver is independent of the basis choice.*
The proof with complementarity is applied to the BB84 protocol [14], round-robin DPS protocol [41] and so on.

Security proof with entropic uncertainty relation

The security proof with entropic uncertainty relation was proposed by Tomamichel *et al*. in 2012 [13]. Differently from the previous two proofs considering phase error correction, the security proof is denoted in terms of smooth min-entropy. Smooth min-entropy quantifies the amount of uniform randomness that can be extracted from the quantum system of finite size and it directly bounds the eavesdropped information in finite-key regime. The security proof is composed of the uncertainty relation of smooth entropies [91] and quantum leftover hashing lemma [92], which were also shown by Tomamichel *et al*.. The assumption for source and receiver is identical to that of the proof with complementarity. The proof is applied to the BB84 protocol [13, 15], MDI protocol [63, 16] and continuous-variable QKD [75].

3.2 Tools of security proof

Here three theoretical tools are introduced to use the security proof with complementarity in Sec. 3.3. The replacement of state preparation is the idea to assume an auxiliary qubit at Alice's site, which is commonly used for the three proofs in the previous section. Phase error and virtual protocol are used in the proof with EDP and that with complementarity although their meanings are slightly different between the two proofs.

3.2.1 Replacement of state preparation

Most protocols of QKD including the BB84 protocol belong to "prepare-and-measure (PM)" type, in which Alice prepares a quantum state based on a selecting bit and sends to Bob, and he makes measurement on the state to obtain a key bit. Another type of QKD protocol is called entanglement-based protocol, in which an entanglement state is distributed to Alice and Bob and they make measurement to share key bits. While the PM-type protocol is easier to implement in general, it is convenient for the security proof to convert the PM-type protocol to entanglement-based protocol where Alice generates an entanglement state and sends a part of it while keeping the other part. Suppose that in the PM-type protocol, Alice selects a bit 0,1 with probability 1/2 and that she prepares $\hat{\rho}_{Z,0}$ and $\hat{\rho}_{Z,1}$ on the system S based on her selecting bit 0 and 1, respectively. The state preparation of $\hat{\rho}_{Z,0}$ and $\hat{\rho}_{Z,1}$ is replaced by the procedure that Alice prepares $\hat{\chi}_{AS}$ on the system AS satisfying

$$\mathrm{Tr}\left(|a_Z\rangle\langle a_Z|_A \hat{\chi}_{AS}\right) = \frac{1}{2}\hat{\rho}_{Z,a} \qquad (a \in \{0,1\}), \tag{3.1}$$

followed by making measurement on the system A with Z basis $\{|0_Z\rangle_A, |1_Z\rangle_A\}$. The state on the system ASE after Eve's interruption does not depend on the timing of Alice's measurement on the system A because the system A is protected from Eve. With $\mathcal{E}_{SE}$ representing Eve's interaction between the accessible system S and her system E, this property is roughly sketched by

$$|a_Z\rangle\langle a_Z|_A \mathcal{E}_{SE}(\hat{\chi}_{AS} \otimes \hat{\rho}_E)|a_Z\rangle\langle a_Z|_A \tag{3.2}$$

$$= \mathcal{E}_{SE}\left(\mathrm{Tr}_A\left(|a_Z\rangle\langle a_Z|_A (\hat{\chi}_{AS} \otimes \hat{\rho}_E)\right)\right) \tag{3.3}$$

$$= \mathcal{E}_{SE}\left(\frac{1}{2}\hat{\rho}_{Z,a} \otimes \hat{\rho}_E\right). \tag{3.4}$$

The form of Eq. (3.2) represents the state (not normalized) on the system ASE where the measurement on the system A is conducted after Eve's intervention and the form of Eq. (3.4) represents the state where the measurement is conducted before her intervention. Although the above argument is limited to a single round of the protocol, it can be extended to total rounds where $\mathcal{E}_{SE}$ includes Eve's coherent interaction among different rounds.

3.2.2 Phase error

Phase error is a convenient concept to express the amount of eavesdropped information, which is adopted in the security proof with EDP and complementarity. In contrast to the fact that an observed error in the protocol is called as "bit error", a phase error is defined through the virtual process which is not conducted in the protocol. Let $\hat{\chi}_{AS}^{\text{int}}$ be a state which is changed from $\hat{\chi}_{AS}$ in Eq. (3.1) after Eve's intervention on the system S. A phase error is defined as a virtual error occurring when Alice and Bob make X-basis measurement on $\hat{\chi}_{AS}^{\text{int}}$ on a Z-labeled round. Here, in the proof with complementarity, Alice's measurement is an ideal X-basis $\{|0_X\rangle_A, |1_X\rangle_A\}$ measurement on the system A while Bob's X-basis measurement on the system S is not limited if the detection probability is identical to that of Z-basis measurement (In BB84, we use the actual X-basis measurement which is conducted in the protocol). In the proof with EDP, both Alice and Bob's measurements are ideal X-basis measurements, which implies that a phase error is obtained by the projective measurement to obtain the result of $|01_X\rangle_{AS}$ or $|10_X\rangle_{AS}$. This corresponds to another definition of phase error in the proof with EDP, in which a phase error occurs by Bell-basis measurement to obtain the result $|\Phi^-\rangle_{AS}$ or $|\Psi^-\rangle_{AS}$ (Notations of Bell states are shown in Sec. 2.1.2). This is because we have the relation

$$|\Phi^-\rangle\langle\Phi^-|_{AB} + |\Psi^-\rangle\langle\Psi^-|_{AB} = |01_X\rangle\langle 01_X|_{AB} + |10_X\rangle\langle 10_X|_{AB}. \tag{3.5}$$

Intuitively, Eve's strong interaction to read Z-basis information leads to a large number of phase errors because of the uncertainty principle. In the proof with EDP and complementarity, the security is evaluated how good phase errors (also bit errors for EDP) are corrected through the virtual protocol which is shown in the following.

3.2.3 Virtual protocol

The definition of the virtual protocol is not uniquely determined, but roughly speaking, it is regarded as a tool for security proof satisfying the following property: If the virtual protocol is secure, then the actual protocol is also secure. Although the concept of the virtual protocol appears in both proofs with EDP and with complementarity, the requirement for the virtual protocol is different from each other. For the proof with complementarity, Alice and Bob do not need to share final keys in the virtual protocol but the goal is to generate a secure key at Alice's site. The only condition for the virtual protocol is given as follows.

Condition for virtual protocol:
For any Eve's attack in the actual protocol, the final state of Alice and Eve in the virtual protocol

is identical to that of the actual protocol which is written as Eq. (2.20).

This condition means that if the virtual protocol is ϵ_s-secret for any attack in the actual protocol, the actual protocol is also ϵ_s-secret. In the virtual protocol, we only need to consider the attack conducted in the actual protocol. Thus, the use of additional public information is allowed in the virtual protocol while the public information announced in the actual protocol has to be disclosed in the virtual protocol. For the proof with complementarity, the virtual protocol includes phase error correction to obtain a number of X-basis eigenstate $|0_X\rangle_A$ at Alice's site, followed by making Z-basis $\{|0_Z\rangle, |1_Z\rangle\}$ measurement on the Alice's system. Since $|0_X\rangle_A$ is a separable state as well as causes the outcome 0,1 with even probability by making Z-basis measurement, the final state is expected to be close to the ideal state Eq. (2.21) if the success probability of phase error correction is high.

For comparison, let us mention the proof with EDP. In the proof with EDP, the virtual protocol is the EDP followed by ideal Z-basis $\{|0_Z\rangle, |1_Z\rangle\}$ measurement by Alice and Bob. The goal of the EDP is to generate maximally entangled state $|\Phi^+\rangle_{AB}$ between Alice and Bob by correcting bit errors and phase errors simultaneously (with CSS code, for example). This requires the ideal qubit measurements at Bob's site (affecting the definition of phase error) and prevents us to decouple the analysis of phase error correction from the bit error correction. In practical case where Bob receives multiple photons, the EDP is incorporated to the squash operation [93, 94], in which the measurement of the multiple photons is replaced by the equivalent single-photon measurement. Differently from the proof with complementarity, the final state of the virtual protocol has to be that of the actual protocol in terms of the whole system of Alice, Bob and Eve.

3.3 Security proof of the BB84 protocol with complementarity

Here, the security of the BB84 protocol is proved based on the proof with complementarity [12]. We assume that Alice's and Bob's apparatuses are ideal, namely, Alice sends a single photon in the states $\{\hat{\rho}_{W,a} = |a_W\rangle\langle a_W|_S\}$ ($W \in \{Z, X\}, a \in \{0, 1\}$) in Step (2) of the protocol shown in Sec. 2.2.3 and Bob conducts ideal measurement with unit efficiency described by POVM $\{|0_W\rangle\langle 0_W|_S, |1_W\rangle\langle 1_W|_S, \hat{\mathbb{1}}_S - |0_W\rangle\langle 0_W|_S - |1_W\rangle\langle 1_W|_S\}$ in Step (3) corresponding to the outcome {0,1,no-detection}. In this case, Bob's measurement satisfies the condition $(*)$ in Sec. 3.1.

In Sec. 3.3.1, the actual protocol is described with the replacement of state preparation. After the main theorem denoting the ϵ_s-secrecy of the actual protocol is given in Sec. 3.3.2, the virtual protocol satisfying the condition in 3.2.3 is constructed in Sec. 3.3.3. Finally the main theorem is proved in Sec. 3.3.4. Since the statement about the fidelity extension in the original paper (Eq. (18) in Ref. [12]) is not correct from the perspective of composable security definition, it is

replaced by the lemma 1 in Sec. 3.3.4.

3.3.1 Description of the actual protocol

Here we describe the ideal BB84 protocol in Sec. 2.2.3 in the alternative form based on the replacement idea introduced in Sec. 3.2.1. In the ideal BB84 protocol, $\hat{\chi}_{AS} = |\Phi^+\rangle\langle\Phi^+|_{AS}$ satisfies Eq. (3.1) as well as

$$\mathrm{Tr}\left(|a_X\rangle\langle a_X|_A \hat{\chi}_{AS}\right) = \frac{1}{2}\hat{\rho}_{X,a} \qquad (a \in \{0,1\}). \tag{3.6}$$

This means that the state preparation for both Z basis and X basis are replaced by preparation of $\hat{\chi}_{AS}$ followed by the measurement on the system A with the corresponding basis. Bob's measurement on the system S is also replaced by a filtering operation to make sure a single photon is received and transfer its state to a qubit B, followed by the orthogonal measurement of B on $\{|0_W\rangle\langle 0_W|_B, |1_W\rangle\langle 1_W|_B\}$ depending on the chosen basis to determine the outcome 0 or 1. Let us call it a "valid-detection" when the filtering succeeds, namely, when the outcome is not "no-detection". The above replacement implies that the basis choices by Alice and Bob can be postponed after valid-detection/no-detection is declared by Bob.

For simplicity, we assume that there is an error-correction scheme which ensures ϵ_c-correctness of the protocol, and denote the total cost for the error correction by λ_{EC}. We also assume that the communication for error correction is encrypted by consuming secret key shared in advance, which allows us to assume that no public information is announced for error correction. Furthermore, Bob corrects his key to agree on Alice's one while Alice's key is unchanged. Then we see that the error correction scheme is no longer necessary for the virtual protocol to fulfill the condition in Sec. 3.2.3. The actual protocol to prove the security is described as follows.

Actual Protocol.
(1') Alice prepares $|\Phi^+\rangle_{AS}$.
(2') Alice sends the part of the state (system S) to Bob over quantum channel.
(3') Bob receives the signal and confirms whether it causes a valid-detection or not. If there is a valid-detection, he keeps the qubit B without measurement.
(4') They repeat (1') to (3') by n_{rep} times.
(5') Bob publicly announces whether each round has resulted in a valid-detection or not. Let n_{det} be the number of rounds with valid-detections.
(6') For the n_{det} rounds, Alice and Bob choose Z basis or X basis with probability $\tilde{p}_Z$ and $\tilde{p}_X$, respectively. They disclose all of their basis choices and discard the rounds where their choice is not identical. Let the number of Z-labeled and X-labeled rounds be n_Z and n_X, respectively. Alice and Bob make X-basis measurement on the system A and B, respectively, on the X-labeled

rounds to obtain bit strings $\boldsymbol{\kappa}_{A,X}$ and $\boldsymbol{\kappa}_{B,X}$.
(7') They disclose and compare $\boldsymbol{\kappa}_{A,X}$ and $\boldsymbol{\kappa}_{B,X}$ to determine the number of bit errors k_X contained in the X-labeled rounds. Let ω represents the following three observed numbers:

$$\omega := (k_X, n_X, n_Z). \tag{3.7}$$

Alice and Bob determine the amount of privacy amplification $m(\omega)$ based on ω and the cost of error correction λ_{EC} through public discussion[*1)]. If $n_Z - m(\omega) \leq \lambda_{\mathrm{EC}}$, the protocol aborts. If it is not, they determine the final key length as $l(\omega) := n_Z - m(\omega)$. For privacy amplification, they randomly select $l(\omega)$ binary vectors $\boldsymbol{V}_1, \boldsymbol{V}_2, ...\boldsymbol{V}_{l(\omega)}$ of size n_Z such that each vector is linearly independent.
(8') Alice and Bob make Z-basis measurement on the system A and B, respectively, on Z-labeled rounds to obtain bit strings $\boldsymbol{\kappa}_{A,Z}$ and $\boldsymbol{\kappa}_{B,Z}$ as sifted keys.
(9') Through public discussion, Bob corrects his key $\boldsymbol{\kappa}_{B,Z}$ to make it coincide with Alice's key $\boldsymbol{\kappa}_{A,Z}$ and obtains $\boldsymbol{\kappa}_{B,Z}^{\mathrm{cor}}$ ($|\boldsymbol{\kappa}_{B,Z}^{\mathrm{cor}}| = n_Z$).
(10') With $\boldsymbol{\kappa}_{A,Z}$ and $\{\boldsymbol{V}_k\}$, final key of size $l(\omega)$ is calculated by $\boldsymbol{\kappa}_{A,Z}^{\mathrm{fin}} = (\boldsymbol{\kappa}_{A,Z} \cdot \boldsymbol{V}_1,\ \boldsymbol{\kappa}_{A,Z} \cdot \boldsymbol{V}_2, ..., \boldsymbol{\kappa}_{A,Z} \cdot \boldsymbol{V}_{l(\omega)})$.

We define Ω as all public information after step (7'), including ω, λ_{EC} and $\{\boldsymbol{V}_k\}$. Here, ω and Ω are not fixed and treated as random variables. Define T_{pass} as the set of Ω such that the protocol does not abort. Let

$$p_{\mathrm{abort}} := 1 - \sum_{\Omega \in T_{\mathrm{pass}}} \Pr(\Omega) \tag{3.8}$$

be the probability that the protocol aborts, and

$$\hat{\rho}_{ABE}^{\mathrm{abort}} := |\emptyset\rangle\langle\emptyset|_{AB} \otimes \hat{\rho}_E^{\mathrm{fin}}(\emptyset) \tag{3.9}$$

be the state under the condition that the protocol aborts. Since Eve can use the information Ω freely, we assume that Eve has a state $|\Omega\rangle\langle\Omega|$ depending on Ω where $\langle\Omega|\Omega'\rangle = \delta_{\Omega,\Omega'}$ with $\delta_{i,j}$ being Kronecker delta. The state on the system ABE after step (7') is described as

$$\hat{\rho}_{ABE} := \sum_{\Omega \in T_{\mathrm{pass}}} \Pr(\Omega) \hat{\rho}_{ABE}^{(\Omega)} + p_{\mathrm{abort}}\, \hat{\rho}_{ABE}^{\mathrm{abort}}, \tag{3.10}$$

where $\hat{\rho}_{ABE}^{(\Omega)}$ has a form of

$$\hat{\rho}_{ABE}^{(\Omega)} = \hat{\rho}_{ABE'}^{(\Omega)} \otimes |\Omega\rangle\langle\Omega|. \tag{3.11}$$

[*1)] One of methods to determine the cost for error correction is sampling a small portion of bits on Z-labeled rounds at random. In this case, Step (7') contains measurement and announcement of the sampled bits, and the sifted keys $\boldsymbol{\kappa}_{A,Z}$ and $\boldsymbol{\kappa}_{B,Z}$ are defined as bit strings on Z rounds in which the sampled bits are removed.

For later convenience, define the following partial states:

$$\hat{\rho}_E^{(\Omega)} := \mathrm{Tr}_{AB}(\hat{\rho}_{ABE}^{(\Omega)}) \tag{3.12}$$

$$\hat{\rho}_{AB}^{(\Omega)} := \mathrm{Tr}_{E}(\hat{\rho}_{ABE}^{(\Omega)}). \tag{3.13}$$

We define $\hat{\rho}_{AE}^{(\Omega)}$, $\hat{\rho}_{BE}^{(\Omega)}$ and $\hat{\rho}_{AE}^{\mathrm{abort}}$ in the same manner. The state $\hat{\rho}_{ABE}$ is changed to $\hat{\rho}_{ABE}^{\mathrm{fin}}$ after Step (10'), which has a form of Eq. (2.14).

3.3.2 Main theorem

Since ϵ_{c}-correctness of the protocol is assumed, it is sufficient to prove that the protocol is ϵ_{s}-secret to certify the ϵ_{sec} $(= \epsilon_{\mathrm{c}} + \epsilon_{\mathrm{s}})$ -security (see Sec. 2.3). Let $\hat{\rho}_{AE}^{\mathrm{fin}}$ and $\hat{\rho}_{AE}^{\mathrm{ideal}}$ be the final state and the ideal state of the protocol written as in Eq. (2.20) and Eq. (2.21), respectively. The main theorem is given as follows.

Theorem:
Suppose that the following inequality holds regardless of Eve's strategy:

$$\Pr(k_{\mathrm{ph}} > f(\omega)) \leq \epsilon_{\mathrm{PE}}, \tag{3.14}$$

where k_{ph} is the number of phase errors. If the amount of privacy amplification is set to $m(\omega) = \left\lceil n_Z h(\frac{f(\omega)}{n_Z}) + \log_2 \frac{1}{\epsilon_{\mathrm{PA}}} \right\rceil$, then we have

$$\frac{1}{2} \left\| \hat{\rho}_{AE}^{\mathrm{fin}} - \hat{\rho}_{AE}^{\mathrm{ideal}} \right\| \leq \sqrt{2}\sqrt{\epsilon_{\mathrm{PE}} + \epsilon_{\mathrm{PA}}}, \tag{3.15}$$

where $\lceil\ \rceil$ represents ceiling function.

The theorem ensures ($\sqrt{2}\sqrt{\epsilon_{\mathrm{PE}} + \epsilon_{\mathrm{PA}}}$)-secrecy of the protocol. Although a function $f(\omega)$ satisfying Eq. (3.14) is not obvious here, it is obtained by classical sampling theory, which is treated in Chapter 6.

3.3.3 Construction of virtual protocol

Here we show an example of the virtual protocol satisfying the condition in Sec. 3.2.3. A virtual protocol is not uniquely determined and convenient one can be chosen. Define the following operators on the system A:

$$\hat{\zeta}_Z(\boldsymbol{C}) := \bigotimes_{i=1}^{n_Z} \hat{\sigma}_Z^{C_i}, \quad \hat{\zeta}_X(\boldsymbol{C}) := \bigotimes_{i=1}^{n_Z} \hat{\sigma}_X^{C_i}, \tag{3.16}$$

where $\hat{\sigma}_Z$ and $\hat{\sigma}_X$ are Pauli operators (bit flip operators on X basis and Z basis, respectively) and $C_i \in \{0,1\}$ is the i-th element of a vector $\boldsymbol{C}$ of size n_Z. We see that calculating $\boldsymbol{\kappa}_{A,Z} \cdot \boldsymbol{V_k}$ after the Z-basis measurement is equivalent to obtain the measurement outcome of the observable $\hat{\zeta}_Z(\boldsymbol{V}_k)$. Let $\mathcal{E}^{(\omega)}_{\rm act}$ be an operation defined on Alice's system, which is equivalent to Alice's Z-basis measurement followed by calculating $\{\boldsymbol{\kappa}_{A,Z} \cdot \boldsymbol{V_k}\}$ in step (8'), (9') and (10') of the actual protocol.

Operation $\mathcal{E}^{(\omega)}_{\rm act}$: Alice measures $l(\omega)$ observables $\{\hat{\zeta}_Z(\boldsymbol{V}_k)\}_{1\le k\le l(\omega)}$ on the system A and register obtained results as $\boldsymbol{\kappa}^{\rm fin}_{A,Z}$.

The operation $\mathcal{E}^{(\omega)}_{\rm act} \otimes \mathbb{1}_{BE}$ on the system ABE satisfies [*2)]

$$\sum_{\Omega\in T_{\rm pass}} \Pr(\Omega)\, {\rm Tr}_B \left(\mathcal{E}^{(\omega)}_{\rm act} \otimes \mathbb{1}_{BE}(\hat{\rho}^{(\Omega)}_{ABE})\right) + p_{\rm abort}\, \hat{\rho}^{\rm abort}_{AE} = \hat{\rho}^{\rm fin}_{AE} \tag{3.17}$$

$$\sum_{\Omega\in T_{\rm pass}} \Pr(\Omega)\, {\rm Tr}_B \left(\mathcal{E}^{(\omega)}_{\rm act} \otimes \mathbb{1}_{BE}(|\boldsymbol{0}_X\rangle\langle\boldsymbol{0}_X|_A \otimes \hat{\rho}^{(\Omega)}_{BE})\right) + p_{\rm abort}\, \hat{\rho}^{\rm abort}_{AE} = \hat{\rho}^{\rm ideal}_{AE}, \tag{3.18}$$

where $|\boldsymbol{0}_X\rangle_A := \bigotimes_{i=1}^{n_Z} |0_X\rangle_{A,i}$ is an eigenstate of the X basis.

Next we consider the following virtual operation on Alice's and Bob's system which is not included in the actual protocol.

Operation $\mathcal{E}^{(\omega)}_{\rm vir}$: Bob makes measurement on his system with X basis and obtain the outcome $\boldsymbol{X}_B \in \{0,1\}^{n_Z}$. He sends $\boldsymbol{X}_B$ to Alice through the public channel. Alice randomly chooses $m(\omega)$ binary vectors $\boldsymbol{W}_1, \boldsymbol{W}_2, ...\boldsymbol{W}_{m(\omega)}$ such that $\boldsymbol{V}_k \cdot \boldsymbol{W}_j = 0$ holds for all (j,k). She measures $m(\omega)$ observables $\{\hat{\zeta}_X(\boldsymbol{W}_j)\}$ on the system A. Based on the measurement outcomes and the classical information $(\omega, \boldsymbol{X}_B)$, she determines "error vector" $\boldsymbol{E}_{\rm est}$ of size n_Z and applies X-flip operation $\hat{\zeta}_Z(\boldsymbol{E}_{\rm est})$.

The goal of operation $\mathcal{E}^{(\omega)}_{\rm vir}$ is to obtain the eigenstate on X basis $|\boldsymbol{0}_X\rangle_A$ in order to use the relation Eq. (3.18). In practice, there is a failure probability to obtain $|\boldsymbol{0}_X\rangle_A$, which is analyzed in the next section. By simple calculation, we see that the condition $\boldsymbol{V}_k \cdot \boldsymbol{W}_j = 0$ leads to $\left[\hat{\zeta}_Z(\boldsymbol{V}_k), \hat{\zeta}_X(\boldsymbol{W}_j)\right] = 0$, which means that the measurement of $\hat{\zeta}_Z(\boldsymbol{V}_k)$ and $\hat{\zeta}_X(\boldsymbol{W}_j)$ commutes. In addition, the X-flip operation $\hat{\zeta}_Z(\boldsymbol{E}_{\rm est})$ does not change the measurement outcomes on Z basis and commutes with the measurement of $\hat{\zeta}_Z(\boldsymbol{V}_k)$. Thus, the final state on the system AE is not changed even if the

[*2)] Assuming the identity map on Eve's system in Eq. (3.17) and Eq. (3.18) does not lose generality of the security proof since all public information is disclosed by Step (7') and any Eve's operation after Step (7') only reduces the trace distance in Eq. (3.28).

operation $\mathcal{E}^{(\omega)}_{\rm vir}$ is conducted before the actual operation:

$$\mathrm{Tr}_B\left(\mathcal{E}^{(\omega)}_{\rm act}\otimes\mathbb{1}_{BE}\left(\mathcal{E}^{(\omega)}_{\rm vir}\otimes\mathbb{1}_E(\hat{\rho}^{(\Omega)}_{ABE})\right)\right)=\mathrm{Tr}_B\left(\mathcal{E}^{(\omega)}_{\rm act}\otimes\mathbb{1}_{BE}(\hat{\rho}^{(\Omega)}_{ABE})\right). \tag{3.19}$$

For later convenience, let us define $\mathcal{E}^{(\omega,\boldsymbol{X}_B)}_{A,\rm vir}$ as Alice's operation in $\mathcal{E}^{(\omega)}_{\rm vir}$ conditioned on $\boldsymbol{X}_B$. With this notation, the state on the system AB after the operation $\mathcal{E}^{(\omega)}_{\rm vir}$ is described as

$$\mathcal{E}^{(\omega)}_{\rm vir}(\hat{\rho}^{(\Omega)}_{AB})=\sum_{\boldsymbol{X}_B}\mathcal{E}^{(\omega,\boldsymbol{X}_B)}_{A,\rm vir}\left({}_B\langle(\boldsymbol{X}_B)_X|\hat{\rho}^{(\Omega)}_{AB}|(\boldsymbol{X}_B)_X\rangle_B\right)\otimes|(\boldsymbol{X}_B)_X\rangle\langle(\boldsymbol{X}_B)_X|_B \tag{3.20}$$

$$=\sum_{\boldsymbol{X}_B}\Pr(\boldsymbol{X}_B)\,\mathcal{E}^{(\omega,\boldsymbol{X}_B)}_{A,\rm vir}\left(\hat{\sigma}^{(\Omega,\boldsymbol{X}_B)}_A\right)\otimes|(\boldsymbol{X}_B)_X\rangle\langle(\boldsymbol{X}_B)_X|_B\,, \tag{3.21}$$

where

$$\Pr(\boldsymbol{X}_B)=\mathrm{Tr}_A\left({}_B\langle(\boldsymbol{X}_B)_X|\hat{\rho}^{(\Omega)}_{AB}|(\boldsymbol{X}_B)_X\rangle_B\right),\quad \hat{\sigma}^{(\Omega,\boldsymbol{X}_B)}_A:=\frac{{}_B\langle(\boldsymbol{X}_B)_X|\hat{\rho}^{(\Omega)}_{AB}|(\boldsymbol{X}_B)_X\rangle_B}{\Pr(\boldsymbol{X}_B)}. \tag{3.22}$$

Since $\mathcal{E}^{(\omega,\boldsymbol{X}_B)}_{A,\rm vir}$ is only composed of the measurement of $\{\hat{\zeta}_X(\boldsymbol{W}_j)\}$ and the flip operation on X basis,

$${}_A\langle\boldsymbol{0}_X|\,\mathcal{E}^{(\omega,\boldsymbol{X}_B)}_{A,\rm vir}(\hat{\sigma}^{(\Omega,\boldsymbol{X}_B)}_A)\,|\boldsymbol{0}_X\rangle_A={}_A\langle\boldsymbol{0}_X|\,\mathcal{E}^{(\omega,\boldsymbol{X}_B)}_{A,\rm vir}(D_X(\hat{\sigma}^{(\Omega,\boldsymbol{X}_B)}_A))\,|\boldsymbol{0}_X\rangle_A \tag{3.23}$$

holds where D_X is an operation which preserves diagonal element on X basis but changes non-diagonal element to 0. We see that applying $\mathcal{E}^{(\omega,\boldsymbol{X}_B)}_{A,\rm vir}$ on $D_X(\hat{\sigma}^{(\Omega,\boldsymbol{X}_B)}_A)$ is identical to a classical parity check and bit flip on a n_Z bit sequence, i.e. classical error correction. This implies that the fidelity in Eq. (3.23) is given by the success probability of classical error correction which corresponds to the operation $\mathcal{E}^{(\omega,\boldsymbol{X}_B)}_{A,\rm vir}$.

By using $\mathcal{E}^{(\omega)}_{\rm act}$ and $\mathcal{E}^{(\omega)}_{\rm vir}$, we define the virtual protocol as follows.

Virtual protocol. Alice and Bob conduct steps (1′) ∼ (7′) of the actual protocol to obtain $\hat{\rho}^{(\Omega)}_{AB}$. They operate $\mathcal{E}^{(\omega)}_{\rm vir}$ on the system AB followed by operating $\mathcal{E}^{(\omega)}_{\rm act}$.

From Eq. (3.17) and the Eq. (3.19), the final state on the system AE of the virtual protocol is given by

$$\sum_{\Omega\in T_{\rm pass}}\Pr(\Omega)\,\mathrm{Tr}_B\left(\mathcal{E}^{(\omega)}_{\rm act}\otimes\mathbb{1}_{BE}(\mathcal{E}^{(\omega)}_{\rm vir}\otimes\mathbb{1}_E(\hat{\rho}^{(\Omega)}_{ABE}))\right)+p_{\rm abort}\,\hat{\rho}^{\rm abort}_{AE} \tag{3.24}$$

$$=\sum_{\Omega\in T_{\rm pass}}\Pr(\Omega)\,\mathrm{Tr}_B\left(\mathcal{E}^{(\omega)}_{\rm act}\otimes\mathbb{1}_{BE}(\hat{\rho}^{(\Omega)}_{ABE})\right)+p_{\rm abort}\,\hat{\rho}^{\rm abort}_{AE} \tag{3.25}$$

$$=\hat{\rho}^{\rm fin}_{AE}, \tag{3.26}$$

which satisfies the condition for the virtual protocol in Sec. 3.2.3.

3.3.4 Proof of the main theorem

Here we prove the main theorem in Sec. 3.3.2. Since the state on the system E is orthogonal for different Ω (see Eq. (3.11)), Eq. (3.18) and Eq. (3.26) lead to

$$\frac{1}{2}\left\| \hat{\rho}_{AE}^{\text{fin}} - \hat{\rho}_{AE}^{\text{ideal}} \right\| \tag{3.27}$$

$$= \frac{1}{2} \sum_{\Omega \in T_{\text{pass}}} \Pr(\Omega) \left\| \text{Tr}_B \left(\mathcal{E}_{\text{act}}^{(\omega)} \otimes \mathbb{1}_{BE} \left(\mathcal{E}_{\text{vir}}^{(\omega)} \otimes \mathbb{1}_E (\hat{\rho}_{ABE}^{(\Omega)}) - |\mathbf{0}_X\rangle\langle\mathbf{0}_X|_A \otimes \hat{\rho}_{BE}^{(\Omega)} \right) \right) \right\| \tag{3.28}$$

$$\leq \frac{1}{2} \sum_{\Omega \in T_{\text{pass}}} \Pr(\Omega) \left\| \text{Tr}_B \left(\mathcal{E}_{\text{vir}}^{(\omega)} \otimes \mathbb{1}_E (\hat{\rho}_{ABE}^{(\Omega)}) \right) - |\mathbf{0}_X\rangle\langle\mathbf{0}_X|_A \otimes \hat{\rho}_E^{(\Omega)} \right\| \tag{3.29}$$

$$\leq \sum_{\Omega \in T_{\text{pass}}} \Pr(\Omega) \sqrt{1 - F\left(\text{Tr}_B \left(\mathcal{E}_{\text{vir}}^{(\omega)} \otimes \mathbb{1}_E (\hat{\rho}_{ABE}^{(\Omega)}) \right), \ |\mathbf{0}_X\rangle\langle\mathbf{0}_X|_A \otimes \hat{\rho}_E^{(\Omega)} \right)}, \tag{3.30}$$

where Eq. (3.29) is obtained by monotonicity of trace distance Eq. (2.5), and Eq. (3.30) is obtained by the relation between trace distance and fidelity Eq. (2.9). The reason that the trace distance is replaced by the fidelity is because we want to use the following lemma which connects the fidelity of the system AE with system A.

lemma1:
For any state $\hat{\tau}_{AE}$ on the system AE and any pure state $|\tilde{0}\rangle\langle\tilde{0}|_A$ on the system A ,

$$F(\hat{\tau}_{AE}, \ |\tilde{0}\rangle\langle\tilde{0}|_A \otimes \hat{\tau}_E) \geq \left(F(\hat{\tau}_A, \ |\tilde{0}\rangle\langle\tilde{0}|_A) \right)^2 \tag{3.31}$$

holds where $\hat{\tau}_E := \text{Tr}_A(\hat{\tau}_{AE})$ and $\hat{\tau}_A := \text{Tr}_E(\hat{\tau}_{AE})$.

The proof is shown in Appendix A. Since

$$\text{Tr}_A \left(\text{Tr}_B \left(\mathcal{E}_{\text{vir}}^{(\omega)} \otimes \mathbb{1}_E (\hat{\rho}_{ABE}^{(\Omega)}) \right) \right) = \text{Tr}_{AB}(\hat{\rho}_{ABE}^{(\Omega)}) = \hat{\rho}_E^{(\Omega)} \tag{3.32}$$

holds, lemma1 lead to

$$F\left(\text{Tr}_B \left(\mathcal{E}_{\text{vir}}^{(\omega)} \otimes \mathbb{1}_E (\hat{\rho}_{ABE}^{(\Omega)}) \right), \ |\mathbf{0}_X\rangle\langle\mathbf{0}_X|_A \otimes \hat{\rho}_E^{(\Omega)} \right) \geq \left(F\left(\text{Tr}_B \left(\mathcal{E}_{\text{vir}}^{(\omega)} (\hat{\rho}_{AB}^{(\Omega)}) \right), \ |\mathbf{0}_X\rangle\langle\mathbf{0}_X|_A \right) \right)^2. \tag{3.33}$$

Eq. (3.30) is replaced by

$$\frac{1}{2}\left\| \hat{\rho}_{AE}^{\text{fin}} - \hat{\rho}_{AE}^{\text{ideal}} \right\| \tag{3.34}$$

$$\leq \sum_{\Omega \in T_{\text{pass}}} \Pr(\Omega) \sqrt{1 - \left(F\left(\text{Tr}_B \left(\mathcal{E}_{\text{vir}}^{(\omega)} (\hat{\rho}_{AB}^{(\Omega)}) \right), \ |\mathbf{0}_X\rangle\langle\mathbf{0}_X|_A \right) \right)^2}. \tag{3.35}$$

Thus, we only need to evaluate the fidelity of the two states in the system A. From Eq. (3.21), we have

$$F\left(\mathrm{Tr}_B\left(\mathcal{E}_{\mathrm{vir}}^{(\omega)}(\hat{\rho}_{AB}^{(\Omega)})\right),\ |\mathbf{0}_X\rangle\langle\mathbf{0}_X|_A\right) = \sum_{\boldsymbol{X}_B} \Pr(\boldsymbol{X}_B)_A\langle\mathbf{0}_X|\,\mathcal{E}_{A,\mathrm{vir}}^{(\omega,\boldsymbol{X}_B)}\left(\hat{\sigma}_A^{(\Omega,\boldsymbol{X}_B)}\right)|\mathbf{0}_X\rangle_A\,. \tag{3.36}$$

Next we evaluate each term of the right-hand side of Eq. (3.36). For convenience, define $\hat{P}_{f(\omega),\boldsymbol{X}_B}$ as a projector on the subspace which can be corrected to $|\mathbf{0}_X\rangle\langle\mathbf{0}_X|_A$ (except small probability) through $\mathcal{E}_{A,\mathrm{vir}}^{(\omega,\boldsymbol{X}_B)}$ based on a given phase-error bound $f(\omega)$ and Bob's measurement outcomes $\boldsymbol{X}_B$. In mathematical expression,

$$\hat{P}_{f(\omega),\boldsymbol{X}_B} := \sum_{\boldsymbol{A}\in S_{f(\omega),\boldsymbol{X}_B}} |\boldsymbol{A}_X\rangle\langle\boldsymbol{A}_X|_A \tag{3.37}$$

$$S_{f(\omega),\boldsymbol{X}_B} := \{\boldsymbol{A}\in\{0,1\}^{n_Z} \mid \mathrm{wt}(\boldsymbol{A}+\boldsymbol{X}_B)\le f(\omega)\}, \tag{3.38}$$

where $\mathrm{wt}(\boldsymbol{X})$ is weight of a vector $\boldsymbol{X}$. Recalling that a phase error is defined as a bit error where Alice and Bob make virtual X-basis measurement on Z-labeled incidents, the state $|\boldsymbol{A}'_X\rangle\langle\boldsymbol{A}'_X|_A$ satisfying $\mathrm{wt}(\boldsymbol{A}'+\boldsymbol{X}_B)=k$ causes k phase errors if it is measured on X basis. Thus, the projector $\hat{P}_{f(\omega),\boldsymbol{X}_B}$ is interpreted as a projector onto a subspace which causes no more than $f(\omega)$ phase errors. Thus, the probability that the number of phase errors k_{ph} is more than $f(\omega)$ is written with the random variables k_{ph}, ω, Ω and $\boldsymbol{X}_B$ as follows:

$$\Pr(k_{\mathrm{ph}} > f(\omega)) = \sum_{\Omega}\sum_{\boldsymbol{X}_B} \Pr(\Omega)\Pr(\boldsymbol{X}_B)\,\mathrm{Tr}\left((\hat{\mathbb{1}}_A - \hat{P}_{f(\omega),\boldsymbol{X}_B})\hat{\sigma}_A^{(\Omega,\boldsymbol{X}_B)}\right), \tag{3.39}$$

where the summation is over all Ω regardless of abort or pass of the protocol. With $\hat{P}_{f(\omega),\boldsymbol{X}_B}$, we evaluate how closely $\hat{\sigma}_A^{(\Omega,\boldsymbol{X}_B)}$ is corrected to $|\mathbf{0}_X\rangle\langle\mathbf{0}_X|_A$ through $\mathcal{E}_{A,\mathrm{vir}}^{(\omega,\boldsymbol{X}_B)}$:

$$\begin{aligned}
&{}_A\langle\mathbf{0}_X|\,\mathcal{E}_{A,\mathrm{vir}}^{(\omega,\boldsymbol{X}_B)}(\hat{\sigma}_A^{(\Omega,\boldsymbol{X}_B)})\,|\mathbf{0}_X\rangle_A && (3.40)\\
&= {}_A\langle\mathbf{0}_X|\,\mathcal{E}_{A,\mathrm{vir}}^{(\omega,\boldsymbol{X}_B)}\left(D_X(\hat{\sigma}_A^{(\Omega,\boldsymbol{X}_B)})\right)|\mathbf{0}_X\rangle_A && (3.41)\\
&= {}_A\langle\mathbf{0}_X|\,\mathcal{E}_{A,\mathrm{vir}}^{(\omega,\boldsymbol{X}_B)}\left(D_X\Big((\hat{P}_{f(\omega),\boldsymbol{X}_B}+\hat{\mathbb{1}}-\hat{P}_{f(\omega),\boldsymbol{X}_B})\hat{\sigma}_A^{(\Omega,\boldsymbol{X}_B)}(\hat{P}_{f(\omega),\boldsymbol{X}_B}+\hat{\mathbb{1}}-\hat{P}_{f(\omega),\boldsymbol{X}_B})\Big)\right)|\mathbf{0}_X\rangle_A && (3.42)\\
&= {}_A\langle\mathbf{0}_X|\,\mathcal{E}_{A,\mathrm{vir}}^{(\omega,\boldsymbol{X}_B)}\left(D_X(\hat{P}_{f(\omega),\boldsymbol{X}_B}\hat{\sigma}_A^{(\Omega,\boldsymbol{X}_B)}\hat{P}_{f(\omega),\boldsymbol{X}_B})\right)|\mathbf{0}_X\rangle_A\\
&\quad + {}_A\langle\mathbf{0}_X|\,\mathcal{E}_{A,\mathrm{vir}}^{(\omega,\boldsymbol{X}_B)}\left(D_X\left((\hat{\mathbb{1}}-\hat{P}_{f(\omega),\boldsymbol{X}_B})\hat{\sigma}_A^{(\Omega,\boldsymbol{X}_B)}(\hat{\mathbb{1}}-\hat{P}_{f(\omega),\boldsymbol{X}_B})\right)\right)|\mathbf{0}_X\rangle_A && (3.43)\\
&\ge \mathrm{Tr}(\hat{P}_{f(\omega),\boldsymbol{X}_B}\hat{\sigma}_A^{(\Omega,\boldsymbol{X}_B)})\,{}_A\langle\mathbf{0}_X|\,\mathcal{E}_{A,\mathrm{vir}}^{(\omega,\boldsymbol{X}_B)}\left(D_X\left(\hat{\chi}_A^{(\Omega,\boldsymbol{X}_B,f(\omega))}\right)\right)|\mathbf{0}_X\rangle_A\,, && (3.44)
\end{aligned}$$

where we used Eq. (3.23) in Eq. (3.41) and used complete positivity of $\mathcal{E}_{A,\mathrm{vir}}^{(\omega,\boldsymbol{X}_B)}$ (see Eq. (2.1)) in Eq. (3.44). We defined $\hat{\chi}_A^{(\Omega,\boldsymbol{X}_B,f(\omega))}$ in Eq. (3.44) as a normalized state

$$\hat{\chi}_A^{(\Omega,\boldsymbol{X}_B,f(\omega))} := \frac{\hat{P}_{f(\omega),\boldsymbol{X}_B}\hat{\sigma}_A^{(\Omega,\boldsymbol{X}_B)}\hat{P}_{f(\omega),\boldsymbol{X}_B}}{\mathrm{Tr}(\hat{P}_{f(\omega),\boldsymbol{X}_B}\hat{\sigma}_A^{(\Omega,\boldsymbol{X}_B)})}. \tag{3.45}$$

From what was mentioned after Eq. (3.23) about the operation $\mathcal{E}_{A,\mathrm{vir}}^{(\omega,\boldsymbol{X}_B)}$,

$$ {}_A\langle \boldsymbol{0}_X | \mathcal{E}_{A,\mathrm{vir}}^{(\omega,\boldsymbol{X}_B)} \left(D_X \left(\hat{\chi}_A^{(\Omega,\boldsymbol{X}_B,f(\omega))} \right) \right) | \boldsymbol{0}_X \rangle_A \tag{3.46} $$

in Eq. (3.44) is regarded as the success probability of classical error correction. Furthermore, this time the error correction is conducted for the confined set $S_{f(\omega),\boldsymbol{X}_B}$. There the syndrome of a vector $\boldsymbol{A} \in S_{f(\omega),\boldsymbol{X}_B}$ is obtained by calculating $(\boldsymbol{A}\cdot\boldsymbol{W}_1, \boldsymbol{A}\cdot\boldsymbol{W}_2, ..., \boldsymbol{A}\cdot\boldsymbol{W}_{m(\omega)})$ followed by applying bit flip to make $\boldsymbol{A}$ coincide $(0, 0, 0...., 0)$. From the classical code theory, we introduce the following two lemmas.

lemma 2 (classical):
With $k, n \in \mathbb{N}$ satisfying $k/n \leq 1/2$, $\left|\left\{\boldsymbol{E} \in \{0,1\}^n \mid \mathrm{wt}(\boldsymbol{E}) \leq k\right\}\right| \leq 2^{nh(k/n)}$ holds.

The lemma means that the number of the vector patterns is bounded if its weight has an upper bound. The proof is equivalent to show ${}_nC_k \leq 2^{nh(k/n)}$, which can be seen in *Example* 12.1.3 in Ref. [78], for instance.

lemma 3 (classical):
Suppose m random binary vectors $(\boldsymbol{M}_1, \boldsymbol{M}_2, ..., \boldsymbol{M}_m)$ of size n. For all $\boldsymbol{E} \in S \subset \{0,1\}^n$, the probability that there is $\boldsymbol{E}' \in S$ such that $\boldsymbol{M}_i \cdot \boldsymbol{E} = \boldsymbol{M}_i \cdot \boldsymbol{E}'$ (for any i) and $\boldsymbol{E} \neq \boldsymbol{E}'$ is no more than $2^{-m}|S|$.

The similar argument to lemma 3 can be seen in the hashing method of EDP [83]. Let $e_{\mathrm{cor}}^{(\boldsymbol{E},S)}$ be the probability to fail the error correction for a given set S and vector $\boldsymbol{E} \in S$, which equals to the failure probability to uniquely identify the original vector $\boldsymbol{E}$ in the confined set S based on the obtained syndrome $\{\boldsymbol{M}_i \cdot \boldsymbol{E}\}$. The lemma 3 indicates $e_{\mathrm{cor}}^{(\boldsymbol{E},S)} \leq 2^{-m}|S|$.

From lemma 2, we have

$$ \left|\left\{\boldsymbol{A} + \boldsymbol{X}_B \in \{0,1\}^{n_Z} \mid \mathrm{wt}(\boldsymbol{A} + \boldsymbol{X}_B) \leq f(\omega)\right\}\right| \leq 2^{n_Z h(f(\omega)/n_Z)}. \tag{3.47} $$

Since $\boldsymbol{X}_B$ is known in the virtual protocol,

$$ \left|\left\{\boldsymbol{A} \in \{0,1\}^{n_Z} \mid \mathrm{wt}(\boldsymbol{A} + \boldsymbol{X}_B) \leq f(\omega)\right\}\right| \leq 2^{n_Z h(f(\omega)/n_Z)}, \tag{3.48} $$

which leads to

$$ |S_{f(\omega),\boldsymbol{X}_B}| \leq 2^{n_Z h(f(\omega)/n_Z)} \tag{3.49} $$

from Eq. (3.38). From lemma 3, we have

$$ e_{\mathrm{cor}}^{(\boldsymbol{A},S_{f(\omega),\boldsymbol{X}_B})} \leq 2^{-m(\omega)}|S_{f(\omega),\boldsymbol{X}_B}|. \tag{3.50} $$

for arbitrary $\boldsymbol{A} \in S_{f(\omega),\boldsymbol{X}_B}$. Combining Eq. (3.49) with Eq. (3.50),

$$e_{\rm cor}^{(\boldsymbol{A},S_{f(\omega),\boldsymbol{X}_B})} \leq 2^{n_Z h(f(\omega)/n_Z)-m(\omega)} \tag{3.51}$$

holds. Therefore, if we set

$$m(\omega) = \left\lceil n_Z h\left(\frac{f(\omega)}{n_Z}\right) + \log_2 \frac{1}{\epsilon_{\rm PA}} \right\rceil, \tag{3.52}$$

the failure probability of error correction in $S_{f(\omega),\boldsymbol{X}_B}$ is not larger than $\epsilon_{\rm PA}$, which leads to

$${}_A\langle \boldsymbol{0}_X| \mathcal{E}_{A,\rm vir}^{(\omega,\boldsymbol{X}_B)} \left(D_X \left(\hat{\chi}_A^{(\Omega,\boldsymbol{X}_B,f(\omega))} \right) \right) |\boldsymbol{0}_X\rangle_A \geq 1-\epsilon_{\rm PA}. \tag{3.53}$$

Now we obtained all elements to bound Eq. (3.35). From Eq. (3.44) and Eq. (3.53), we have

$${}_A\langle \boldsymbol{0}_X| \mathcal{E}_{A,\rm vir}^{(\omega,\boldsymbol{X}_B)}(\hat{\sigma}_A^{(\Omega,\boldsymbol{X}_B)}) |\boldsymbol{0}_X\rangle_A \geq (1-\epsilon_{\rm PA}) {\rm Tr}(\hat{P}_{f(\omega),\boldsymbol{X}_B} \hat{\sigma}_A^{(\Omega,\boldsymbol{X}_B)}) \tag{3.54}$$

for all $\boldsymbol{X}_B$. Combining this with Eq. (3.36),

$$F\left({\rm Tr}_B \left(\mathcal{E}_{\rm vir}^{(\omega)}(\hat{\rho}_{AB}^{(\Omega)}) \right), \ |\boldsymbol{0}_X\rangle\langle \boldsymbol{0}_X|_A \right) \geq (1-\epsilon_{\rm PA}) \left(\sum_{\boldsymbol{X}_B} {\rm Pr}(\boldsymbol{X}_B) {\rm Tr}(\hat{P}_{f(\omega),\boldsymbol{X}_B} \hat{\sigma}_A^{(\Omega,\boldsymbol{X}_B)}) \right), \tag{3.55}$$

which leads to

$$\begin{aligned}
&1 - \left(F\left({\rm Tr}_B \left(\mathcal{E}_{\rm vir}^{(\omega)}(\hat{\rho}_{AB}^{(\Omega)}) \right), \ |\boldsymbol{0}_X\rangle\langle \boldsymbol{0}_X|_A \right) \right)^2 && (3.56)\\
&\leq 2\left(1 - F\left({\rm Tr}_B \left(\mathcal{E}_{\rm vir}^{(\omega)}(\hat{\rho}_{AB}^{(\Omega)}) \right), \ |\boldsymbol{0}_X\rangle\langle \boldsymbol{0}_X|_A \right)\right) && (3.57)\\
&\leq 2\left(1 - (1-\epsilon_{\rm PA}) \left(\sum_{\boldsymbol{X}_B} {\rm Pr}(\boldsymbol{X}_B) {\rm Tr}(\hat{P}_{f(\omega),\boldsymbol{X}_B} \hat{\sigma}_A^{(\Omega,\boldsymbol{X}_B)}) \right)\right) && (3.58)\\
&= 2\left(1 - (1-\epsilon_{\rm PA}) \left(\sum_{\boldsymbol{X}_B} {\rm Pr}(\boldsymbol{X}_B) \left(1 - {\rm Tr}\left((\hat{\mathbb{1}}_A - \hat{P}_{f(\omega),\boldsymbol{X}_B}) \hat{\sigma}_A^{(\Omega,\boldsymbol{X}_B)} \right) \right) \right)\right) && (3.59)\\
&= 2\left(1 - (1-\epsilon_{\rm PA}) \left(1 - \sum_{\boldsymbol{X}_B} {\rm Pr}(\boldsymbol{X}_B) {\rm Tr}\left((\hat{\mathbb{1}}_A - \hat{P}_{f(\omega),\boldsymbol{X}_B}) \hat{\sigma}_A^{(\Omega,\boldsymbol{X}_B)} \right) \right)\right) && (3.60)\\
&\leq 2\epsilon_{\rm PA} + 2 \sum_{\boldsymbol{X}_B} {\rm Pr}(\boldsymbol{X}_B) {\rm Tr}\left((\hat{\mathbb{1}}_A - \hat{P}_{f(\omega),\boldsymbol{X}_B}) \hat{\sigma}_A^{(\Omega,\boldsymbol{X}_B)} \right). && (3.61)
\end{aligned}$$

By combining this with Eq. (3.35), we have

$$\begin{aligned}
&\frac{1}{2} \left\| \hat{\rho}_{AE}^{\rm fin} - \hat{\rho}_{AE}^{\rm ideal} \right\| && (3.62)\\
&\leq \sum_{\Omega \in T_{\rm pass}} {\rm Pr}(\Omega) \sqrt{2\epsilon_{\rm PA} + 2 \sum_{\boldsymbol{X}_B} {\rm Pr}(\boldsymbol{X}_B) \ {\rm Tr}\left((\hat{\mathbb{1}}_A - \hat{P}_{f(\omega),\boldsymbol{X}_B}) \hat{\sigma}_A^{(\Omega,\boldsymbol{X}_B)} \right)} && (3.63)\\
&\leq \sqrt{2\epsilon_{\rm PA} + 2 \sum_{\Omega \in T_{\rm pass}} \sum_{\boldsymbol{X}_B} {\rm Pr}(\Omega) \ {\rm Pr}(\boldsymbol{X}_B) \ {\rm Tr}\left((\hat{\mathbb{1}}_A - \hat{P}_{f(\omega),\boldsymbol{X}_B}) \hat{\sigma}_A^{(\Omega,\boldsymbol{X}_B)} \right)} && (3.64)\\
&\leq \sqrt{2} \sqrt{\epsilon_{\rm PA} + {\rm Pr}(k_{\rm ph} > f(\omega))}, && (3.65)
\end{aligned}$$

where we used the concavity of square root function in Eq. (3.64) and used Eq. (3.39) in Eq. (3.65). From the assumption of the main theorem $\Pr(k_{\rm ph} \geq f(\omega)) \leq \epsilon_{\rm PE}$, we have

$$\frac{1}{2}\left\| \hat{\rho}_{AE}^{\rm fin} - \hat{\rho}_{AE}^{\rm ideal} \right\| \leq \sqrt{2}\sqrt{\epsilon_{\rm PA} + \epsilon_{\rm PE}}. \tag{3.66}$$

3.3.5 Discussion

Although the proof shown in the previous section basically followed the one in Ref. [12], lemma 1 did not appear there. In Ref. [12], the similar argument is used to connect two fidelities where Eve's state of the ideal state (ρ_E in Eq. (4) in Ref. [12]) is not related to the actual protocol and chosen freely to satisfy Eq. (18) in Ref. [12]. However, this might not satisfy the security criteria with composability. Suppose that a protocol $\mathcal{P}$ is conducted before the QKD protocol $\mathcal{Q}$ (to prove the security) where $\mathcal{Q}$ uses secret keys generated by $\mathcal{P}$. In general, Eve's state ρ_E defined on $\mathcal{Q}$ depends on the information obtained in $\mathcal{P}$, which includes Alice and Bob's set up for $\mathcal{P}$. Thus, ρ_E should not be chosen freely for ideal states and in this case we are not sure that composable security is satisfied.

In the proof discussed in the previous section, we assumed the protocol where the final-key length $l(\omega)$ is not fixed and the condition for aborting the protocol is given by $n_Z - m(\omega) \leq \lambda_{\rm EC}$. On the other hand, the proof is also applicable to the protocols with fixed final-key length, which is seen in Ref. [13], for example. The fixed-key-length protocol, in which the data size n_Z and n_X have threshold $\bar{n}_Z$ and $\bar{n}_X$, is finished whenever $n_Z \geq \bar{n}_Z$ and $n_X \geq \bar{n}_X$ are satisfied. (To realize it, a basis choice is assumed to be disclosed at each round.) If $n_Z > \bar{n}_Z$ or $n_X > \bar{n}_X$, the surplus $n_Z - \bar{n}_Z$ bits or $n_X - \bar{n}_X$ bits are randomly discarded. For the number of bit errors k'_X contained in the $\bar{n}_X$ rounds, the protocol also has a threshold $\bar{k}_X$, namely, the protocol aborts when $k'_X > \bar{k}_X$. With these thresholds, $f(\omega)$ is fixed to be the predetermined value $f(\bar{\omega})$ where $\bar{\omega} = (\bar{k}_X, \bar{n}_Z, \bar{n}_X)$, and the amount of privacy amplification is also fixed to $m(\bar{\omega}) = \lceil \bar{n}_Z h(f(\bar{\omega})/\bar{n}_Z) + \log_2(1/\epsilon_{\rm PA}) \rceil$ if the protocol does not abort. The theorem in the previous section is still valid in this case as long as Eq. (3.14) is satisfied for $f(\bar{\omega})$.

Chapter 4

QKD with weak coherent pulses

After the security of the ideal BB84 protocol was proved by Mayers [5] and Shor and Preskill [6], the focus on the security proof was shifted to the practical case using conventional lasers and threshold detectors which can only tell single photon or more from vacuum. In particular, the security proof for QKD using weak coherent pulses (WCP) was a crucial issue not only because a single-photon source with high repetition rate is technically hard to realize, but also because there is a strong attack using multiple photons called photon number splitting (PNS) attack. Although the proof for the BB84 protocol with WCP (WCP-BB84) was given by Inamori *et al*. in 2001 [9], it uses the modified proof of Mayers [5] and inherits its complexity. On the other hand, Gottesman, Lo, Lütkenhaus and Preskill (GLLP) proposed a simple idea which can be incorporated to various proof techniques for ideal QKD assuming single-photon emission. They proposed the concept of "tagging", in which a round with multiple-photon emission is classified as "tagged" (insecure) while a round with single-photon emission is classified as "untagged" (secure). If the tagging idea is combined with the security proof based on complementarity [12] or entropic uncertainty relation [13], uncharacterized receiver can be assumed as long as the condition $(*)$ in Sec. 3.1 is satisfied. The security of QKD protocols with general source flaws (e.g. modulation of polarization, optical phase and intensity) were also proved in sophisticated ways [95, 17, 96, 97], but in this thesis we focus on the practical effect of multiple-photon emission.

This chapter is organized as follows. In Sec. 4.1, PNS attack is introduced. Sec 4.2 briefly shows the GLLP's tagging idea and derive the key length of WCP-BB84 protocol in terms of phase errors on untagged rounds. In Sec. 4.3, we focus on practical aspects of the WCP-BB84 protocol by introducing the phase-encoding BB84 (PE-BB84) protocol which is suitable for implementation with optical fibers, and also by introducing the decoy-state method, a countermeasure against PNS attacks. In Sec. 4.4, the DPS protocol is shown as a simple protocol with robustness against PNS attacks.

4.1 Photon number splitting attack

Photon number splitting (PNS) attack is an Eve's strong strategy where she exploits full information of the signal with multiple-photon emission without causing any disturbance. It was pointed out by Brassard *et al*. in 2000 [8]. The details of PNS attack are as follows. Suppose the protocol where bit information is encoded on polarization of light. After receiving the signal emitted from the source, Eve projects the signal state onto the subspaces characterized by the total photon number m. This projective measurement is regarded as quantum-non-demolition (QND) measurement which does not disturb the signal's polarization. Next she performs splitting operation preserving polarization where $n-1$ photons are kept at her system and only one photon is sent to Bob. After Eve learns the basis choices of Alice and Bob which is disclosed on the classical channel, she makes measurement on the preserved photons with the corresponding basis. Since the $n-1$ extracted photons have the same polarization as the other single photon which is sent to Bob, signal information with multiple-photon emissions is totally leaked without any disturbance.

For later convenience, let us denote PNS attack in a mathematical way. We define the following parameters. Let Q represents the detection rate of the protocol (=rounds with detections / total rounds) and e_X represents the bit-error rate on the X-labeled rounds. Let $p^{(m)}$ be the probability that the state emitted from the source was projected to m-photon subspace by Eve. Let Y_m represents the probability that the signal projected to m-photon subspace causes detection at Bob's site, and $e_{X,m}$ represents the error rate on the X-labeled rounds where the signal is projected to m-photon subspace. If Eve conducts PNS attack in the above manner, we have the following equations in the asymptotic limit:

$$Q = \sum_{m\geq 0} p^{(m)} Y_m \tag{4.1}$$

$$Qe_X = \sum_{m\geq 0} p^{(m)} Y_m \, e_{X,m}. \tag{4.2}$$

The parameters Q and e_X are observed values in the protocol, and the parameter $p^{(m)}$ is determined by the property of the source and known through its calibration. Here we consider Eve's strategy to change Y_m and $e_{X,m}$ under the fixed values of Q, e_X and $p^{(m)}$. Eve's optimal attack is to make multi-photon signals detected perfectly, and use allowed errors to eavesdrop single-photon signal as much as possible. If we assume that Eve has no technical limit and she can use lossless and noiseless channel, the optimal choice is

$$Y_m = 1, \;\; e_{X,m} = 0 \quad \text{for} \;\; m \geq 2, \tag{4.3}$$

which leads to

$$p^{(0)}Y_0 + p^{(1)}Y_1 = Q - \sum_{m\geq 2} p^{(m)} \tag{4.4}$$

$$p^{(0)}Y_0\, e_{X,0} + p^{(1)}Y_1\, e_{X,1} = e_X. \tag{4.5}$$

Eq. (4.4) implies that if $Q \leq \sum_{m\geq 2} p^{(m)}$, no secure key can be extracted.

4.2 GLLP's tagging idea

The tagging idea (called "tagged signal" in the original paper [10]) is a quite useful method to prove the security of QKD using WCP, which was proposed by Gottesman, Lo, Lütkenhaus and Preskill (GLLP). In their idea, a round with multiple-photon emission is regarded as tagged and that with single-photon emission is regarded as untagged. The tagged rounds are considered to be totally insecure (considering PNS attack) and they show that the security of the WCP protocol only depends on the security of the untagged rounds even if Alice and Bob do not know which rounds are tagged in the actual protocol. This allows various security proofs for the ideal single-photon protocols to be applied to the practical QKD protocols with WCP. By using this idea, GLLP showed the asymptotic key rate of the WCP-BB84 protocol, which is slightly better than that obtained in the previous work of Inamori *et al*. [9]. In this section, first we introduce the phase-randomizing operation, which allows us to use the tagging idea. Next the key length of the WCP-BB84 protocol is derived in terms of phase errors on untagged rounds by applying the proof in Sec. 3.3. Finally, we evaluate the effect of PNS attacks on the WCP-BB84 protocol by using the asymptotic key rate.

4.2.1 Phase-randomizing operation

In this subsection, we introduce a sufficient condition for the light source to use the tagging idea and show that it is satisfied by the randomizing operation on the optical phase. Suppose that at each round of the protocol, Alice prepares an i.i.d state $\hat{\rho}_{W,a}$ on the system S depending on her basis choice W ($\in \{Z, X\}$ for BB84 protocol) and a selected bit $a \in 0, 1$. The condition to use the tagging idea is that $\hat{\rho}_{W,a}$ is expressed as

$$\hat{\rho}_{W,a} = (1 - r_{\text{tag}})\hat{\rho}_{W,a,\text{unt}} \oplus r_{\text{tag}}\hat{\rho}_{W,a,\text{tag}}, \tag{4.6}$$

which indicates that each round is in principle classified to tagged or untagged. In the following, we show that this condition is satisfied if the optical phase of each signal is randomized, and if

the probability that the state before phase randomization $\hat{\sigma}_{W,a}$ has two or more photons is given by

$$\sum_{m\geq 2} \mathrm{Tr}(\hat{N}_m \hat{\sigma}_{W,a}) = r_{\mathrm{tag}}, \tag{4.7}$$

where we defined $\hat{N}_m$ as the projector onto the subspace with m photons. Suppose that the phase-shift operator $\hat{J}(\theta) := \exp(i\theta \sum_m m\hat{N}_m)$ is acting on $\hat{\sigma}_{W,a}$. By defining phase-randomizing operation as $\mathcal{E}_{\mathrm{PR}}$, we have

$$\begin{aligned}
\hat{\rho}_{W,a} &= \mathcal{E}_{\mathrm{PR}}(\hat{\sigma}_{W,a}) && (4.8)\\
&= \frac{1}{2\pi}\int_0^{2\pi} \hat{J}(\theta)\, \hat{\sigma}_{W,a}\, \hat{J}(\theta)^\dagger d\theta && (4.9)\\
&= \frac{1}{2\pi}\sum_{m,m'}\int_0^{2\pi} e^{i\theta(m-m')} \hat{N}_m \hat{\sigma}_{W,a} \hat{N}_{m'} d\theta && (4.10)\\
&= \sum_m \hat{N}_m \hat{\sigma}_{W,a} \hat{N}_m. && (4.11)
\end{aligned}$$

Thus, any optical state is regarded as a classical mixture of photon-number state by randomizing its optical phase. By reformulating Eq. (4.11),

$$\hat{\rho}_{W,a} = \sum_{m=0,1} (1 - r_{\mathrm{tag}}) \frac{\hat{N}_m \hat{\sigma}_{W,a} \hat{N}_m}{1 - r_{\mathrm{tag}}} + \sum_{m\geq 2} r_{\mathrm{tag}} \frac{\hat{N}_m \hat{\sigma}_{W,a} \hat{N}_m}{r_{\mathrm{tag}}} \tag{4.12}$$

holds. Eq. (4.6) is satisfied by taking

$$\begin{aligned}
\hat{\rho}_{W,a,\mathrm{unt}} &= \sum_{m=0,1} \frac{\hat{N}_m \hat{\sigma}_{W,a} \hat{N}_m}{1 - r_{\mathrm{tag}}}\\
\hat{\rho}_{W,a,\mathrm{tag}} &= \sum_{m\geq 2} \frac{\hat{N}_m \hat{\sigma}_{W,a} \hat{N}_m}{r_{\mathrm{tag}}}.
\end{aligned} \tag{4.13}$$

It is instructive to learn the negative effect on WCP protocols caused by imperfection of phase randomization because most of QKD protocols these days adopt phase-randomizing operation to use the tagging idea for their security proofs [98, 90]. At least for the WCP-BB84 protocol, the achievable key rate of the protocol without phase randomization is shown to be lower than that with phase randomization [99], which implies that there is an Eve's attack to use the coherence between different photon numbers. In practice, randomizing the optical phase in continuous range $[0, 2\pi)$ as in Eq. (4.9) can be difficult if the resource of random numbers is limited. Recently Cao *et al*. [100] have shown the security of QKD with discrete-phase randomization where the optical phase is randomly chosen from $\{2\pi/n \mid 1 \leq n \leq \bar{n}\}$ with finite $\bar{n}$. Although many QKD demonstrations realize the random phases by switching on and off a laser repeatedly under the assumption that the optical phase is randomized once the laser is switched off, it is controversial whether the phase is truly independent of that of the previous pulse or not [101].

4.2.2 Security analysis of WCP-BB84 with tagging idea

Here we derive the secure key length of the WCP-BB84 protocol in terms of phase errors by combining the tagging idea with the complementarity proof introduced in Sec. 3.3. If the bound of phase errors on untagged rounds is known (derived in Sec. 6), this subsection gives a complete security proof for the WCP-BB84 protocol. Similarly to the ideal qubit-based protocol, the WCP-BB84 protocol also follows the procedures described in Sec. 2.2.3, but the latter assumes more general light sources and measurement apparatuses.

For Alice's state preparation, we assume that the state prepared by Alice has a form of Eq. (4.6) and that there is a basis-independent state $\hat{\chi}_{\rm unt}$ on the system AS satisfying

$$\mathrm{tr}_A\left((|a_W\rangle\langle a_W|_A \otimes \hat{\mathbb{1}}_S)\hat{\chi}_{\rm unt}\right) = \frac{1}{2}\hat{\rho}_{W,a,\rm unt}, \tag{4.14}$$

which corresponds to Eq. (3.1) and Eq. (3.6) in the ideal BB84 protocol. Those assumptions allow Alice's basis choice to be postponed after Eve's intervention as far as untagged rounds are concerned. Eqs. (4.6) and (4.14) are realized, for example, if Alice uses a laser emitting an ideally polarized coherent state

$$|\alpha_{W,a}\rangle_S := \sum_m e^{-\frac{|\alpha|^2}{2}} \frac{\alpha^m}{\sqrt{m!}} |m_{W,a}\rangle_S \,, \tag{4.15}$$

where α is a complex number and $|m_{W,a}\rangle_S$ is a photon-number state on the system S with a basis W and a bit a, and if its optical phase is randomized. From Eq. (4.11), the state after phase-randomizing operation is

$$\mathcal{E}_{\rm PR}(|\alpha_{W,a}\rangle\langle\alpha_{W,a}|_S) = \sum_m e^{-\mu}\frac{\mu^m}{m!} |m_{W,a}\rangle\langle m_{W,a}|_S \,, \tag{4.16}$$

where we defined a parameter $\mu := |\alpha|^2$ as mean photon number of the coherent light. From Eq. (4.13), $\hat{\rho}_{W,a,\rm unt}$ and $\hat{\rho}_{W,a,\rm tag}$ in Eq. (4.6) are written as

$$(1 - r_{\rm tag})\hat{\rho}_{W,a,\rm unt} = e^{-\mu}|0_{W,a}\rangle\langle 0_{W,a}| + \mu e^{-\mu}|1_{W,a}\rangle\langle 1_{W,a}| \tag{4.17}$$

$$r_{\rm tag}\hat{\rho}_{W,a,\rm tag} = e^{-\mu}\sum_{m=2}^{\infty}\frac{\mu^m}{m!}|m_{W,a}\rangle\langle m_{W,a}| \tag{4.18}$$

with

$$r_{\rm tag} = 1 - e^{-\mu} - \mu e^{-\mu}. \tag{4.19}$$

For Bob's measurement apparatus, we impose either of the following two assumptions.
(i) The probability of detecting a signal at Bob's receiver is independent of his basis choice.
(ii) The measurement of an input signal on the system S is replaced by an ideal single-photon

measurement on the system B preceding by a squashing operation [93, 94].
The condition (ii), which is stronger than the condition (i), validates the use of the security proof with entanglement distillation. The proof with complementarity works under the weaker condition (i), because it essentially validates the argument given in Sec. 3.3.1. Under the condition (i), Bob's measurement on the system S can be replaced by a filtering operation to make sure a valid-detection and to transfer its state to a system B (not necessarily a qubit), followed by a measurement on B depending on the chosen basis to determine the outcome 0 or 1. Hence, as in Sec. 3.3.1, Bob's choice of basis can be postponed until he declares valid-detection/no-detection. For the WCP-BB84 protocol, both conditions are satisfied if we assume the following model for Bob's apparatus: Bob actively chooses the basis, and uses two threshold detectors corresponding to the measurement result "0" and "1" after a polarization beam splitter. He assigns random bit if both detectors report their detections. In addition, the inefficiency and dark countings of the detectors are allowed as long as they are equivalently represented by an absorber and a stray photon source placed in front of Bob's apparatus.

For the WCP-BB84 protocol, the preparation of the state Eq. (4.6) on basis W is replaced by that of basis-dependent state on the system AS

$$\hat{\chi}_W := (1 - r_{\rm tag})\hat{\chi}_{\rm unt} \oplus r_{\rm tag}\hat{\chi}_{W,{\rm tag}}, \tag{4.20}$$

followed by the W-basis measurement on the system A, in which $\hat{\chi}_{W,{\rm tag}}$ is a basis-dependent state satisfying

$$\mathrm{tr}_A\left((|a_W\rangle\langle a_W|_A \otimes \hat{\mathbb{I}}_S)\hat{\chi}_{W,{\rm tag}}\right) = \frac{1}{2}\hat{\rho}_{W,a,{\rm tag}}. \tag{4.21}$$

This implies that Alice's state preparation is described as follows. At each round, Alice determines whether it is tagged or not with probabilities $r_{\rm tag}$ and $1 - r_{\rm tag}$. If the round is tagged, she selects a basis and prepares $\hat{\chi}_{W,{\rm tag}}$ based on her basis choice, and if not, she prepares the basis-independent state $\hat{\chi}_{\rm unt}$ without selecting a basis.

Similarly to the protocol in Sec. 3.3.1, we assume that $\epsilon_{\rm c}$-correctness of the protocol is ensured by an error-correction method with encryption consuming $\lambda_{\rm EC}$ pre-obtained secret keys. The description of the protocol with the replacement of state preparation (which corresponds to the actual protocol in Sec. 3.3.1) is given as follows.

(1') Alice determines whether a round is tagged or untagged with probabilities $r_{\rm tag}$ and $1 - r_{\rm tag}$. For a tagged round, she selects Z basis or X basis with probability $\tilde{p}_Z$ and $\tilde{p}_X$, respectively, and prepares $\hat{\chi}_{W,{\rm tag}}$ based on her basis choice. For an untagged round, she prepares $\hat{\chi}_{\rm unt}$ without selecting a basis.
(2') Alice sends the part of the state (system S) to Bob over quantum channel.

(3') Bob receives the signal and confirms whether it causes a valid-detection or not. If there is a valid-detection, he keeps system B without measurement.
(4') They repeat (1') to (3') by $n_{\rm rep}$ times.
(5') Bob publicly announces whether each round has resulted in a valid-detection or not. Let $n_{\rm det}$ be the number of rounds with valid-detections. Let $n_{\rm tot,unt}$ be the number of untagged rounds with valid-detections.
(6') For the $n_{\rm tot,unt}$ rounds, Alice chooses Z basis or X basis with probability $\tilde{p}_Z$ and $\tilde{p}_X$, respectively. For the $n_{\rm det}$ rounds, Bob chooses Z basis or X basis with probability $\tilde{p}_Z$ and $\tilde{p}_X$, respectively. They disclose all of their basis choice and discard the rounds where their choice is not identical. Let the number of Z-labeled and X-labeled rounds be n_Z and n_X, respectively. They make X-basis measurement on the X-labeled rounds to obtain bit strings $\boldsymbol{\kappa}_{A,X}$ and $\boldsymbol{\kappa}_{B,X}$. Alice publicly announces which rounds are untagged.
(7') They disclose and compare $\boldsymbol{\kappa}_{A,X}$ and $\boldsymbol{\kappa}_{B,X}$ to determine the number of bit errors k_X contained in the X-labeled rounds. Let ω represents the following three observed numbers:

$$\omega := (k_X, n_X, n_Z). \tag{4.22}$$

Alice and Bob determine the amount of privacy amplification $m(\omega)$ based on ω and the cost of error correction $\lambda_{\rm EC}$ through public discussion. If $n_Z - m(\omega) \leq \lambda_{\rm EC}$, the protocol aborts. If it is not, they determine the final key length as $l(\omega) := n_Z - m(\omega)$. For privacy amplification, they randomly select $l(\omega)$ binary vectors $\boldsymbol{V}_1, \boldsymbol{V}_2, ...\boldsymbol{V}_{l(\omega)}$ of size n_Z such that each vector is linearly independent.
(8') Alice and Bob make Z-basis measurement on system A and B, respectively, on Z-labeled rounds to obtain bit strings $\boldsymbol{\kappa}_{A,Z}$ and $\boldsymbol{\kappa}_{B,Z}$ as sifted keys.
(9') Through public discussion, Bob corrects his keys $\boldsymbol{\kappa}_{B,Z}$ to make it coincide with Alice's key $\boldsymbol{\kappa}_{A,Z}$ and obtains $\boldsymbol{\kappa}^{\rm cor}_{B,Z}$ ($|\boldsymbol{\kappa}^{\rm cor}_{B,Z}| = n_Z$).
(10') With $\boldsymbol{\kappa}_{A,Z}$ and $\{\boldsymbol{V}_k\}$, final key of size $l(\omega)$ is calculated by $\boldsymbol{\kappa}^{\rm fin}_{A,Z} = (\boldsymbol{\kappa}_{A,Z} \cdot \boldsymbol{V}_1,\ \boldsymbol{\kappa}_{A,Z} \cdot \boldsymbol{V}_2, ..., \boldsymbol{\kappa}_{A,Z} \cdot \boldsymbol{V}_{l(\omega)})$.

The number of untagged rounds $n_{\rm tot,unt}$ defined in Step (5') is not an observed parameter in practice, but only an "observable-in-principle" parameter. Similarly to this parameter, let $n_{Z,\rm unt}$ and $n_{Z,\rm tag}$ ($:= n_Z - n_{Z,\rm unt}$) be the number of Z-labeled untagged rounds and tagged rounds, respectively, which are in principle observed in Step (6'). We also define

$$\tilde{\omega} = (k_X, n_X, n_Z, n_{Z,\rm unt}). \tag{4.23}$$

Let $n_{X,\rm unt}$ and $n_{X,\rm tag}$ ($:= n_X - n_{X,\rm unt}$) be the number of X-labeled untagged rounds and tagged rounds, respectively. Then $n_{Z,\rm unt} + n_{X,\rm unt} = n_{\rm tot,unt}$ is satisfied. We also define $k_{X,\rm unt}$ and $k_{X,\rm tag}$ as the number

of bit errors on X-labeled untagged rounds and tagged rounds, respectively, which are in principle determined in Step (7').

Based on those parameters, the theorem similar to the one in Sec. 3.3.2 is given as follows.

Theorem:
Suppose that the following inequality holds regardless of Eve's strategy:

$$\Pr(k_{\mathrm{ph,unt}} > f(\tilde{\omega})) \leq \epsilon_{\mathrm{PE}} \tag{4.24}$$

$$\Pr(n_{Z,\mathrm{unt}} < \underline{n}_{Z,\mathrm{unt}}) \leq \epsilon_{Z,\mathrm{unt}}, \tag{4.25}$$

where $k_{\mathrm{ph,unt}}$ is the number of phase errors on untagged rounds. If the final key length $l(\omega)$ satisfies

$$l(\omega) \leq \min_{n_{Z,\mathrm{unt}} \geq \underline{n}_{Z,\mathrm{unt}}} \left\{ n_{Z,\mathrm{unt}}(1 - h\left(\frac{f(\tilde{\omega})}{n_{Z,\mathrm{unt}}}\right)) \right\} - \log_2 \frac{2}{\epsilon_{\mathrm{PA}}}, \tag{4.26}$$

the protocol is ϵ_s-secret with

$$\epsilon_{\mathrm{s}} = \sqrt{2}\sqrt{\epsilon_{\mathrm{PE}} + \epsilon_{\mathrm{PA}}} + \epsilon_{Z,\mathrm{unt}}. \tag{4.27}$$

Although the bounds $f(\tilde{\omega})$ and $\underline{n}_{Z,\mathrm{unt}}$ are not obvious here, they are derived in Chapter 6.

The proof of the theorem is quite similar to that in Sec. 3.3.4 but with several modifications. We assume that the observable-in-principle parameters are also disclosed to Eve in the previous protocol. Let $\tilde{\Omega}$ be all disclosed information including $\tilde{\omega}$. Eq. (3.29) is replaced by

$$\frac{1}{2}\left\| \hat{\rho}_{AE}^{\mathrm{fin}} - \hat{\rho}_{AE}^{\mathrm{ideal}} \right\| \tag{4.28}$$

$$\leq \frac{1}{2} \sum_{\tilde{\Omega} \in \tilde{T}_{\mathrm{pass}}} \Pr(\tilde{\Omega}) \left\| \mathrm{Tr}_B \left(\mathcal{E}_{\mathrm{vir}}^{(\tilde{\omega})} \otimes \mathbb{1}_E(\hat{\rho}_{ABE}^{(\tilde{\Omega})}) \right) - |\mathbf{0}_X\rangle\langle\mathbf{0}_X|_A \otimes \hat{\rho}_E^{(\tilde{\Omega})} \right\|, \tag{4.29}$$

where $\tilde{T}_{\mathrm{pass}}$ is a set of $\tilde{\Omega}$ such that the protocol does not abort. For simplicity, we define

$$\gamma^{(\tilde{\Omega})} := \frac{1}{2}\left\| \mathrm{Tr}_B \left(\mathcal{E}_{\mathrm{vir}}^{(\tilde{\omega})} \otimes \mathbb{1}_E(\hat{\rho}_{ABE}^{(\tilde{\Omega})}) \right) - |\mathbf{0}_X\rangle\langle\mathbf{0}_X|_A \otimes \hat{\rho}_E^{(\tilde{\Omega})} \right\|. \tag{4.30}$$

By reformulating Eq. (4.29),

$$\frac{1}{2}\left\| \hat{\rho}_{AE}^{\text{fin}} - \hat{\rho}_{AE}^{\text{ideal}} \right\| \tag{4.31}$$

$$\leq \sum_{\tilde{\Omega}\in\tilde{T}_{\text{pass}}} \Pr(\tilde{\Omega})\, \gamma^{(\tilde{\Omega})} \tag{4.32}$$

$$= \sum_{\substack{\tilde{\Omega}\in\tilde{T}_{\text{pass}}:\\ n_{Z,\text{unt}}\geq \underline{n}_{Z,\text{unt}}}} \Pr(\tilde{\Omega})\, \gamma^{(\tilde{\Omega})} \;+\; \sum_{\substack{\tilde{\Omega}\in\tilde{T}_{\text{pass}}:\\ n_{Z,\text{unt}}< \underline{n}_{Z,\text{unt}}}} \Pr(\tilde{\Omega})\, \gamma^{(\tilde{\Omega})} \tag{4.33}$$

$$\leq \Pr(n_{Z,\text{unt}} \geq \underline{n}_{Z,\text{unt}}) \sum_{\substack{\tilde{\Omega}\in\tilde{T}_{\text{pass}}:\\ n_{Z,\text{unt}}\geq \underline{n}_{Z,\text{unt}}}} \frac{\Pr(\tilde{\Omega})}{\Pr(n_{Z,\text{unt}} \geq \underline{n}_{Z,\text{unt}})}\, \gamma^{(\tilde{\Omega})} + \Pr(n_{Z,\text{unt}} < \underline{n}_{Z,\text{unt}}) \tag{4.34}$$

$$\leq (1-\epsilon_{Z,\text{unt}}) \sum_{\substack{\tilde{\Omega}\in\tilde{T}_{\text{pass}}:\\ n_{Z,\text{unt}}\geq \underline{n}_{Z,\text{unt}}}} p(\tilde{\Omega})\; \gamma^{(\tilde{\Omega})} \;+\; \epsilon_{Z,\text{unt}}, \tag{4.35}$$

where the summations are over $\tilde{\Omega}$ such that $\tilde{\Omega} \in \tilde{T}_{\text{pass}}$ and $n_{Z,\text{unt}} \geq \underline{n}_{Z,\text{unt}}$ (or $n_{Z,\text{unt}} < \underline{n}_{Z,\text{unt}}$), and we defined

$$p(\tilde{\Omega}) := \frac{\Pr(\tilde{\Omega})}{\Pr(n_{Z,\text{unt}} \geq \underline{n}_{Z,\text{unt}})} \qquad s.t. \qquad \sum_{\substack{\tilde{\Omega}\in\tilde{T}_{\text{pass}}:\\ n_{Z,\text{unt}}\geq \underline{n}_{Z,\text{unt}}}} p(\tilde{\Omega}) = 1. \tag{4.36}$$

We used $\gamma^{(\tilde{\Omega})} \leq 1$ in Eq. (4.34) and also used Eq. (4.25) in Eq. (4.35). Define $\Gamma^{(\tilde{\Omega})}$ as

$$\Gamma^{(\tilde{\Omega})} := \sqrt{1 - F\left(\text{Tr}_B\left(\mathcal{E}_{\text{vir}}^{(\tilde{\omega})} \otimes \mathbb{1}_E(\hat{\rho}_{ABE}^{(\tilde{\Omega})})\right),\ |\mathbf{0}_X\rangle\langle\mathbf{0}_X|_A \otimes \hat{\rho}_E^{(\tilde{\Omega})}\right)}. \tag{4.37}$$

From the relation between the trace distance and the fidelity Eq. (2.9), we have

$$\gamma^{(\tilde{\Omega})} \leq \Gamma^{(\tilde{\Omega})}. \tag{4.38}$$

Eq. (4.35) is replaced by

$$\frac{1}{2}\left\| \hat{\rho}_{AE}^{\text{fin}} - \hat{\rho}_{AE}^{\text{ideal}} \right\| \tag{4.39}$$

$$\leq (1-\epsilon_{Z,\text{unt}}) \sum_{\substack{\tilde{\Omega}\in\tilde{T}_{\text{pass}}:\\ n_{Z,\text{unt}}\geq \underline{n}_{Z,\text{unt}}}} p(\tilde{\Omega})\; \Gamma^{(\tilde{\Omega})} \;+\; \epsilon_{Z,\text{unt}}. \tag{4.40}$$

The evaluation of $\Gamma^{(\tilde{\Omega})}$ is quite similar to that in Sec. 3.3.4. The difference is that a set of vectors $S_{f(\omega),\boldsymbol{x}_B}$ in Eq. (3.38) is replaced by another one. Since Alice and Bob tell tagged rounds from untagged rounds in principle, we divide a vector $\boldsymbol{A}$ of size n_Z into untagged part of size $n_{Z,\text{unt}}$ and tagged part of size $n_{Z,\text{tag}}$:

$$\boldsymbol{A} = \boldsymbol{A}_{\text{unt}} \oplus \boldsymbol{A}_{\text{tag}}. \tag{4.41}$$

With this notation, we define

$$\tilde{S}_{f(\tilde{\omega}),\boldsymbol{X}_B} := \{\boldsymbol{A} \in \{0,1\}^{n_Z} \mid \mathrm{wt}(\boldsymbol{A}_{\mathrm{unt}} + \boldsymbol{X}_{B,\mathrm{unt}}) \leq f(\tilde{\omega})\}, \tag{4.42}$$

where the plus sign represents addition modulo 2 of each element. Eq. (4.42) implies that the vector patterns for the tagged rounds are totally unknown, which corresponds to the assumption that the information of tagged rounds is fully leaked to Eve. In order to use lemma 3 and to obtain Eq. (3.50), we require $|\tilde{S}_{f(\tilde{\omega}),\boldsymbol{X}_B}|$. For untagged rounds,

$$\left|\left\{\boldsymbol{A}_{\mathrm{unt}}\middle|\mathrm{wt}(\boldsymbol{A}_{\mathrm{unt}} + \boldsymbol{X}_{B,\mathrm{unt}}) \leq f(\tilde{\omega})\right\}\right| \leq 2^{n_{Z,\mathrm{unt}} h(f(\tilde{\omega})/n_{Z,\mathrm{unt}})} \tag{4.43}$$

is satisfied from lemma 2. Thus, we have

$$\left|\tilde{S}_{f(\tilde{\omega}),\boldsymbol{X}_B}\right| \leq 2^{n_{Z,\mathrm{unt}} h(f(\tilde{\omega})/n_{Z,\mathrm{unt}})} 2^{n_{Z,\mathrm{tag}}}. \tag{4.44}$$

By using the argument from Eq. (3.50) to Eq. (3.53), if the amount of privacy amplification $m(\omega)$ satisfies

$$m(\omega) = \max_{n_{Z,\mathrm{unt}} \geq \underline{n}_{Z,\mathrm{unt}}} \left\lceil n_{Z,\mathrm{unt}} h(f(\tilde{\omega})/n_{Z,\mathrm{unt}}) + n_{Z,\mathrm{tag}} + \log_2 \frac{1}{\epsilon_{\mathrm{PA}}} \right\rceil, \tag{4.45}$$

we have

$${}_A\langle \boldsymbol{0}_X| \mathcal{E}_{A,\mathrm{vir}}^{(\tilde{\omega},\boldsymbol{X}_B)} \left(D_X \left(\hat{\chi}_A^{(\tilde{\Omega},\boldsymbol{X}_B,f(\tilde{\omega}))} \right) \right) |\boldsymbol{0}_X\rangle_A \geq 1 - \epsilon_{\mathrm{PA}} \tag{4.46}$$

for $\tilde{\Omega}$ satisfying $\tilde{\Omega} \in \tilde{T}_{\mathrm{pass}}$ and $n_{Z,\mathrm{unt}} \geq \underline{n}_{Z,\mathrm{unt}}$. By combining this with Eqs. (3.33), (3.36), (3.44) and (3.61), we have

$$\Gamma^{(\tilde{\Omega})} \leq \sqrt{2\epsilon_{\mathrm{PA}} + 2 \sum_{\boldsymbol{X}_B} \Pr(\boldsymbol{X}_B) \mathrm{Tr}\left((\hat{\mathbb{I}}_A - \hat{P}_{f(\tilde{\omega}),\boldsymbol{X}_B}) \hat{\sigma}_A^{(\tilde{\Omega},\boldsymbol{X}_B)} \right)}. \tag{4.47}$$

Recall that the evaluation of $\Gamma^{(\tilde{\Omega})}$ in Eq. (4.40) is limited to $\{\tilde{\Omega}\}$ satisfying $\tilde{\Omega} \in \tilde{T}_{\mathrm{pass}}$ and $n_{Z,\mathrm{unt}} \geq \underline{n}_{Z,\mathrm{unt}}$. From Eq. (4.24) and Eq. (4.25), we have

$$\Pr(k_{\mathrm{ph,unt}} > f(\tilde{\omega}) \mid n_{Z,\mathrm{unt}} \geq \underline{n}_{Z,\mathrm{unt}}) \leq \frac{\epsilon_{\mathrm{PE}}}{1 - \epsilon_{Z,\mathrm{unt}}}. \tag{4.48}$$

Let us write down the left-hand side of Eq. (4.48) explicitly. Define $\hat{\tilde{P}}_{f(\tilde{\omega}),\boldsymbol{X}_B}$ based on $\tilde{S}_{f(\tilde{\omega}),\boldsymbol{X}_B}$:

$$\hat{\tilde{P}}_{f(\tilde{\omega}),\boldsymbol{X}_B} := \sum_{\boldsymbol{A} \in \tilde{S}_{f(\tilde{\omega}),\boldsymbol{X}_B}} |\boldsymbol{A}_X\rangle\langle \boldsymbol{A}_X|_A \,. \tag{4.49}$$

Similarly to Eq. (3.39), we have

$$\Pr(k_{\mathrm{ph,unt}} > f(\tilde{\omega})) = \sum_{\tilde{\Omega}} \sum_{\boldsymbol{X}_B} \Pr(\tilde{\Omega}) \Pr(\boldsymbol{X}_B) \, \mathrm{Tr}\left((\hat{\mathbb{I}} - \hat{P}_{f(\tilde{\omega}),\boldsymbol{X}_B}) \hat{\sigma}_A^{(\tilde{\Omega},\boldsymbol{X}_B)} \right), \tag{4.50}$$

which leads to

$$\Pr(k_{\mathrm{ph,unt}} > f(\tilde{\omega}) \mid n_{Z,\mathrm{unt}} \geq \underline{n}_{Z,\mathrm{unt}}) = \sum_{\tilde{\Omega}: n_{Z,\mathrm{unt}} \geq \underline{n}_{Z,\mathrm{unt}}} \sum_{\boldsymbol{X}_B} p(\tilde{\Omega}) \Pr(\boldsymbol{X}_B) \operatorname{Tr}\left((\hat{\mathbb{1}} - \hat{P}_{f(\tilde{\omega}),\boldsymbol{X}_B}) \hat{\sigma}_A^{(\tilde{\Omega},\boldsymbol{X}_B)} \right), \quad (4.51)$$

where the summation in Eq. (4.51) is over $\tilde{\Omega}$ satisfying $n_{Z,\mathrm{unt}} \geq \underline{n}_{Z,\mathrm{unt}}$ regardless of whether $\tilde{\Omega} \in \tilde{T}_{\mathrm{pass}}$ or not, and $p(\tilde{\Omega})$ is defined in Eq. (4.36). Since each summand of Eq. (4.51) is non-negative, the right-hand side does not increase if the summation is further limited to $\tilde{\Omega} \in \tilde{T}_{\mathrm{pass}}$. Thus, Eq. (4.48) and Eq. (4.51) lead to

$$\sum_{\substack{\tilde{\Omega} \in \tilde{T}_{\mathrm{pass}}: \\ n_{Z,\mathrm{unt}} \geq \underline{n}_{Z,\mathrm{unt}}}} \sum_{\boldsymbol{X}_B} p(\tilde{\Omega}) \Pr(\boldsymbol{X}_B) \operatorname{Tr}\left((\hat{\mathbb{1}} - \hat{P}_{f(\tilde{\omega}),\boldsymbol{X}_B}) \hat{\sigma}_A^{(\tilde{\Omega},\boldsymbol{X}_B)} \right) \leq \frac{\epsilon_{\mathrm{PE}}}{1 - \epsilon_{Z,\mathrm{unt}}}. \quad (4.52)$$

From Eqs. (4.40), (4.47) and (4.52), we have

$$\frac{1}{2} \left\| \hat{\rho}_{AE}^{\mathrm{fin}} - \hat{\rho}_{AE}^{\mathrm{ideal}} \right\| \quad (4.53)$$

$$\leq (1 - \epsilon_{Z,\mathrm{unt}}) \sum_{\substack{\tilde{\Omega} \in \tilde{T}_{\mathrm{pass}}: \\ n_{Z,\mathrm{unt}} \geq \underline{n}_{Z,\mathrm{unt}}}} p(\tilde{\Omega}) \sqrt{2\epsilon_{\mathrm{PA}} + 2 \sum_{\boldsymbol{X}_B} \Pr(\boldsymbol{X}_B) \operatorname{Tr}\left((\hat{\mathbb{1}}_A - \hat{P}_{f(\tilde{\omega}),\boldsymbol{X}_B}) \hat{\sigma}_A^{(\tilde{\Omega},\boldsymbol{X}_B)} \right)} + \epsilon_{Z,\mathrm{unt}} \quad (4.54)$$

$$\leq (1 - \epsilon_{Z,\mathrm{unt}}) \sqrt{2\epsilon_{\mathrm{PA}} + 2 \sum_{\substack{\tilde{\Omega} \in \tilde{T}_{\mathrm{pass}}: \\ n_{Z,\mathrm{unt}} \geq \underline{n}_{Z,\mathrm{unt}}}} \sum_{\boldsymbol{X}_B} p(\tilde{\Omega}) \Pr(\boldsymbol{X}_B) \operatorname{Tr}\left((\hat{\mathbb{1}}_A - \hat{P}_{f(\tilde{\omega}),\boldsymbol{X}_B}) \hat{\sigma}_A^{(\tilde{\Omega},\boldsymbol{X}_B)} \right)} + \epsilon_{Z,\mathrm{unt}} \quad (4.55)$$

$$\leq (1 - \epsilon_{Z,\mathrm{unt}}) \sqrt{2\epsilon_{\mathrm{PA}} + \frac{\epsilon_{\mathrm{PE}}}{1 - \epsilon_{Z,\mathrm{unt}}}} + \epsilon_{Z,\mathrm{unt}} \quad (4.56)$$

$$\leq \sqrt{2} \sqrt{\epsilon_{\mathrm{PA}} + \epsilon_{\mathrm{PE}}} + \epsilon_{Z,\mathrm{unt}}. \quad (4.57)$$

By using Eq. (4.45) and $m(\omega) = n_Z - l(\omega)$, the protocol is ϵ_{s}-secret with $\epsilon_{\mathrm{s}} = \sqrt{2} \sqrt{\epsilon_{\mathrm{PA}} + \epsilon_{\mathrm{PE}}} + \epsilon_{Z,\mathrm{unt}}$ if the final-key length $l(\omega)$ satisfies

$$l(\omega) = n_Z - \max_{n_{Z,\mathrm{unt}} \geq \underline{n}_{Z,\mathrm{unt}}} \left\lceil n_{Z,\mathrm{unt}} h\left(\frac{f(\tilde{\omega})}{n_{Z,\mathrm{unt}}} \right) + n_{Z,\mathrm{tag}} + \log_2 \frac{1}{\epsilon_{\mathrm{PA}}} \right\rceil \quad (4.58)$$

$$\leq \min_{n_{Z,\mathrm{unt}} \geq \underline{n}_{Z,\mathrm{unt}}} \left\{ n_{Z,\mathrm{unt}} (1 - h\left(\frac{f(\tilde{\omega})}{n_{Z,\mathrm{unt}}} \right)) \right\} - \log_2 \frac{2}{\epsilon_{\mathrm{PA}}}. \quad (4.59)$$

4.2.3 PNS attack vs. WCP-BB84 protocol

In this section, we derive the asymptotic key rate of the WCP-BB84 protocol with tagging idea as in Ref. [10], and show that the protocol is vulnerable to PNS attack in long-distance communication. Consider the asymptotic limit $n_{\mathrm{rep}} \to \infty$ while the parameters

$$\Delta := \frac{n_{Z,\mathrm{tag}}}{n_Z}, \quad Q := \frac{n_Z}{n_{\mathrm{rep}} \tilde{p}_Z^2}, \quad e_X := \frac{k_X}{n_X} \quad (4.60)$$

are fixed. By using the result of finite-key analysis Eq. (4.59), the asymptotic key rate per round is given by

$$R_{\mathrm{asy}}^{(\Delta,e_{X,\mathrm{unt}})} := \tilde{p}_Z^2 Q\,(1-\Delta)(1-h\,(e_{X,\mathrm{unt}})), \tag{4.61}$$

where $e_{X,\mathrm{unt}} := k_{X,\mathrm{unt}}/n_{X,\mathrm{unt}}$ and Δ are unknown parameters. Since $n_{X,\mathrm{unt}}/n_X \to 1-\Delta$ holds in the asymptotic limit, $k_{X,\mathrm{unt}} \leq k_X$ leads to

$$(1-\Delta)e_{X,\mathrm{unt}} \leq e_X. \tag{4.62}$$

Then we have

$$R_{\mathrm{asy}}^{(\Delta,e_{X,\mathrm{unt}})} \geq \tilde{p}_Z^2 Q\,(1-\Delta)(1-h\left(\frac{e_X}{1-\Delta}\right)) \tag{4.63}$$

$$=: R_{\mathrm{asy}}^{(\Delta)}. \tag{4.64}$$

To bound $R_{\mathrm{asy}}^{(\Delta)}$ with known parameters, we use the inequality

$$\Delta \leq \frac{r_{\mathrm{tag}}}{Q}, \tag{4.65}$$

which is obtained from Eq. (4.6) and Eq. (4.60). This leads to

$$R_{\mathrm{asy}}^{(\Delta)} \geq \tilde{p}_Z^2 Q\,(1-\frac{r_{\mathrm{tag}}}{Q})(1-h\left(\frac{e}{1-\frac{r_{\mathrm{tag}}}{Q}}\right)) \tag{4.66}$$

$$=: R_{\mathrm{asy}}. \tag{4.67}$$

Note that R_{asy} is the optimal key rate in the form of Eq. (4.61), namely, Eve can in principle choose parameters which satisfy $R_{\mathrm{asy}} = R_{\mathrm{asy}}^{(\Delta,e_{X,\mathrm{unt}})}$. Moreover, those parameters are realized by PNS attacks introduced in Sec. 4.1. To confirm these, it is sufficient to check the equality of Eq. (4.62) and Eq. (4.65). With $e_{X,\mathrm{tag}} := k_{X,\mathrm{tag}}/n_{X,\mathrm{tag}}$, we see that

$$(1-\Delta)e_{X,\mathrm{unt}} = e_X \;\leftrightarrow\; e_{X,\mathrm{tag}} = 0 \;\leftrightarrow\; e_{X,m} = 0 \;\;(\text{for } m \geq 2). \tag{4.68}$$

Let $p^{(m)}$ be the probability that the source emits m photons (assuming phase randomization). Let $Y^{(m)}$ be the probability that a signal emitted with m-photons causes a detection at Bob's receiver. Those parameters have identical meaning to those in Sec. 4.1. Since $r_{\mathrm{tag}} = \sum_{m\geq 2} p^{(m)}$ holds from Eq. (4.13), we have

$$Q\Delta = r_{\mathrm{tag}} \;\leftrightarrow\; \sum_{m\geq 2} p^{(m)} Y_m = \sum_{m\geq 2} p^{(m)} \;\leftrightarrow\; Y_m = 1 \;\;(\text{for } m \geq 2) \tag{4.69}$$

in the asymptotic limit. Both Eq. (4.68) and Eq. (4.69) are satisfied by Eq. (4.3) with PNS attack.

To evaluate the effect of PNS attacks on the BB84 protocol, we assume the specific value of r_{tag} by adopting the model that Alice uses a coherent light source, in which r_{tag} is given by Eq. (4.19). We derive the dependence of R_{asy} on total transmittance η (including detector efficiency) in the limit of $\eta \to 0$. From Eq. (4.67), the value of r_{tag}/Q has to be kept smaller than 1 to ensure $R_{\mathrm{asy}} > 0$. Since Q decreases as η approaches to 0, $\mu \to 0$ is required to keep R_{asy} positive. Thus, Q and r_{tag} are expressed as

$$Q = \eta(\mu + O(\mu^2)) \tag{4.70}$$

$$r_{\mathrm{tag}} = \frac{\mu^2}{2} + O(\mu^3). \tag{4.71}$$

Eq. (4.70) and Eq. (4.71) lead to

$$\frac{r_{\mathrm{tag}}}{Q} = \frac{1}{2\eta}(\mu + O(\mu^2)). \tag{4.72}$$

If r_{tag}/Q is held fixed as η gets small, the value of μ is changed as $\mu = O(\eta)$. Then the overall key generation rate R_{asy} has square dependence on η:

$$R_{\mathrm{asy}} = O(\eta^2). \tag{4.73}$$

This implies that the BB84 protocol is vulnerable to PNS attacks in the long distance communication.

4.3 Practical aspects of WCP-BB84 protocol

In this subsection, we focus on the practical aspects of the WCP-BB84 protocol. For implementation of QKD protocols, its simplicity is crucial for several reasons. The first one is straightforward, that is, we have to reduce the cost of QKD for its commercialization [56]. Another reason is that practical devices have security loopholes [59, 60, 61, 62, 102], which violates the assumptions of the security proof. This means that if complicated devices are used, we have to consider many countermeasures (from both theoretical and practical sides) against possible attacks. The BB84 protocol with phase-encoding (PE-BB84) is a specific form of the WCP-BB84 protocol which can be implemented with simple devices. Since PE-BB84 protocol is vulnerable to PNS attacks in the long distance, it is often used with the decoy-state method. Although it enables long distance communication and many demonstrations have already been conducted, several practical problems still remain. In the following, we introduce the PE-BB84 protocol and the decoy-state method, and discuss their advantages and problems.

4.3.1 Phase-encoding BB84 protocol

When QKD is implemented, we typically use free space or optical fibers as quantum channel. While some simulations and demonstrations of free-space QKD (e.g. satellite QKD) are conducted [64, 29, 30, 31], most of high-speed QKD implementations use the optical fibers to guide signals stably [26, 27, 28]. In fiber-based QKD, a bit 0,1 tends to be encoded on optical phase rather than polarization of photons because polarization is less stabler than optical phase in optical fibers due to their birefringence. Another advantage of phase-encoding method is that the fast encoding and reading are possible with current techniques (e.g. 1 GHz pulse-repetition rate with phase modulation in Ref. [35] and 10 GHz in Ref [40]).

Phase-encoding BB84 protocol (PE-BB84 protocol) is composed of simple devices, such as a typical laser, a phase modulator and a passive Mach-Zehnder interferometer (see also Fig. 4.1). With established security (the proof for the PE-BB84 is identical to the WCP-BB84), a number of demonstrations are conducted [33, 34, 35]. In the protocol, double pulses with interval $\Delta\tau$ are generated at Alice's site, followed by phase modulation which includes randomization of the global phase as well as changing the relative phase to encode a bit. At Bob's site, each pulse is fed to a delayed interferometer with its delay being equal to $\Delta\tau$. The longer arm of the interferometer passes through a phase modulator which incurs phase shift $\theta_B = 0$ or $\frac{\pi}{2}$. After the interferometer, the pulses are measured by two photon detectors corresponding to bit values "0" and "1". If there is a detection from the superposition of the double pulses, we call it as valid detection (see Fig. 4.2). The description of the PE-BB84 protocol is identical to that in Sec. 2.2.3 except that Step (1)-(3) have more concrete expressions.
(1) Alice chooses Z basis or X basis with probability $\tilde{p}_Z$ and $\tilde{p}_X$, respectively. She chooses a uniformly random bit $\{0, 1\}$.
(2) Alice generates double pulses and modulates the relative phase between those pulses as $0, \pi, \pi/2, 3\pi/2$ if her basis and bit are $(Z, 0)$, $(Z, 1)$, $(X, 0)$, $(X, 1)$, respectively. She also changes the global phase of the double pulses at random.
(3) Bob chooses Z basis or X basis with probability $\tilde{p}_Z$ and $\tilde{p}_X$, respectively. He sets the phase shift $\theta_B = 0$ and $\theta_B = \pi/2$ if he selects Z basis and X basis, respectively. If an invalid detection occurs, Bob declares no-detection. If both detectors have detections at a valid timing, Bob randomly generates a bit 0 or 1. He obtains the outcome {0, 1, no-detection}.

Bob's random-bit assignment in Step 3 is for the sake of satisfying the receiver's condition $(*)$ in Sec. 3.1. Since a valid detection occurs only when the first pulse in the long arm and the second pulse in the short arm have interference, there are invalid detections with probability 1/2 due to the use of the passive interferometer (see Fig. 4.2). Although invalid detections can be reduced by using an optical switch, it typically has insertion loss larger than 1/2 (e.g. 4 dB loss

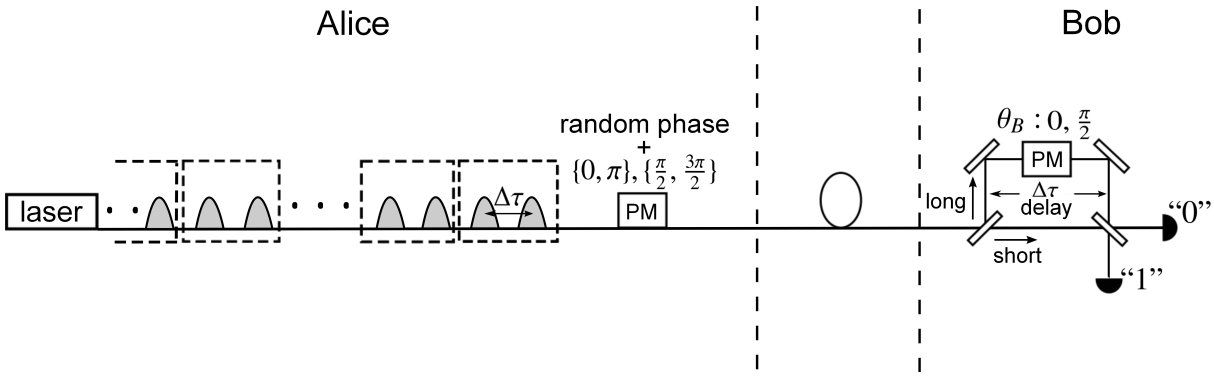

Figure 4.1: Set up of the BB84 protocol. Alice generates double pulses (in a dashed block in the figure) and modulates the global phase at random and also modulate the relative phase based on her basis and bit. Bob changes the phase shift θ_B based on his basis choice. The delay in the long arm equals to the interval of the double pulse $\Delta\tau$, which enables neighboring pulses to interfere each other. A detection from the interference between double pulses in a block is regarded as valid, and outcomes from other detections are invalid.

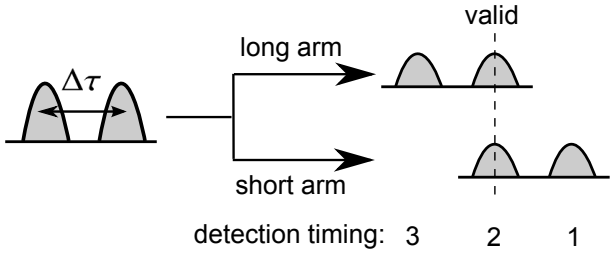

Figure 4.2: Sketch of valid interference at Bob's site. The double pulses are split and the ones going through the longer arm are delayed by $\Delta\tau$ from the others going through the shorter arm. The interference between the first pulse in the longer arm and the second pulse in the shorter arm is regarded as valid, which occurs at Timing 2 (in the figure) with probability 1/2.

for 10 ns switching time [103]). Thus, the problem of half invalid detections is essential in the PE-BB84 protocol, and actually, it is the origin of the advantage of the DQPS protocol over the PE-BB84 protocol, which is considered in Chapter 5.

4.3.2 Decoy-state method

The decoy-state method is a practical countermeasure against PNS attacks, which was proposed and developed by Hwang [36], Lo *et al*. [104] and Wang [37]. They are incorporated to various protocols, such as the BB84 protocol, the six-state protocol [48], the MDI protocols [63, 105, 16], and high-dimensional protocols [106, 107]. In the decoy-state method, Alice chooses the intensity (mean photon number) of each signal from a predetermined set $\{\mu_i\}$ ($0 \leq i \leq i_{\text{decoy}}$, $i = 0$ corresponds to the signal) and monitor the detection rate separately for each intensity. Define Q_i as the observed detection rate for the intensity μ_i. Let $p_i^{(m)}$ be the probability that the source emits m photons under the condition of mean photon number μ_i. With parameters Y_m defined in Sec. 4.2.3, we have the following $i_{\text{decoy}} + 1$ simultaneous equations in the asymptotic limit.

$$\left\{ Q_i = \sum_{m \geq 0} p_i^{(m)} Y_m \right\} \qquad (0 \leq i \leq i_{\text{decoy}}). \tag{4.74}$$

This implies that if we increase the number of decoy intensity i_{decoy}, the better bound of Y_m is obtained. Recalling the fact that the value of Y_m was totally under control of Eve with PNS attacks (see Eq. (4.3) and Eq. (4.4)), we see that threat of PNS attack can be limited by adopting decoy states. In practice, it is shown that the BB84 protocol with two decoy states ($i_{\text{decoy}} = 2$) achieves nonzero key rate over 100 km communication in finite-key regime [15].

Although the decoy-state method seems attractive, there still remain practical problems because additional operations tend to enlarge the gap between physical models of devices and their practical behaviours. Let us show two examples for a light source. Although we use weak coherent pulses in QKD implementations, the distribution of $p^{(m)}$ can deviate from Poissonian and it has to be estimated through the calibration of the light source. Although the security proof with a general light source using decoy states was conducted [39], it assumes the following infinite number of inequalities, which cannot be confirmed through calibration:

$$\frac{p_L^{(1)}}{p_U^{(1)}} \leq \frac{p_L^{(m)}}{p_U^{(m)}} \quad (\text{for } m \geq 2), \tag{4.75}$$

where $p_L^{(m)}$ and $p_U^{(m)}$ represent the lower and the upper bound of $p^{(m)}$, respectively. Another example is that the intensity of a decoy pulse deviates from the predetermined value because the intensity of the decoy pulse is in the middle of the signal's intensity and the vacuum, and hence

it is at the steep slope in the intensity-modulation curve. The deviation over 10% is reported in Ref. [108], for example.

Even if the above problems are solved from either theoretical or experimental side, the decoy-state method holds inevitable complexity and disadvantage associated with it. Since it uses higher-order $p^{(m)}$ to estimate the value of Y_m, more complicated calibration method is required compared to the protocol without decoy states. Since it includes more estimation processes, the larger overhead is sacrificed by the statistical fluctuation in the finite-key analysis. Thus, for short distance communication where PNS attacks are not so threatening, the protocol without decoy states may be preferred from the perspective of simplicity.

4.4 Differential-phase-shift protocol

The differential-phase-shift (DPS) protocol is as simple (or simper) protocol as the PE-BB84 protocol, in which only two phases $\{0, \pi\}$ are used for the relative phase between neighboring pulses. It was proposed by Inoue *et al*. in 2002 [89] as a protocol with robustness against PNS attacks. Although there are several protocols which are expected to be robust against PNS attacks [109, 110, 111], the simplicity of the DPS protocol is outstanding, which enables the demonstration with a high clock rate of 10 GHz [40]. Since the DPS protocol is an origin of the differential-quadrature-phase-shift (DQPS) protocol which is treated in Chapter 5, here we review the DPS protocol and its security. In this section, the protocol description and the security analysis of the DPS protocol are briefly introduced based on Ref.[90]. Afterwards, we discuss the round-robin DPS protocol, which is a variant of the DPS protocol solving the complexity of the security proof for the DPS protocol.

4.4.1 Protocol description

Here, we describe the DPS protocol based on Ref. [90]. The set up for the DPS protocol is identical to that of the PE-BB84 protocol with several exceptions (see Fig. 4.3). In the DPS protocol, sequential pulses are divided by a block of L pulses for the convenience of security proof. The phase-randomizing operation is applied to the whole block. Differently from the PE-BB84 protocol, the relative phase is either 0 or π, hence the phase modulator is not necessary at the receiver's site. The photon-number resolving detectors were assumed as in Ref. [90]. If there is a detection from the superposition of the l-th and $(l-1)$-th original pulses, we call it as valid detection at l-th timing $(1 \leq l \leq L-1)$. The protocol is described as follows.

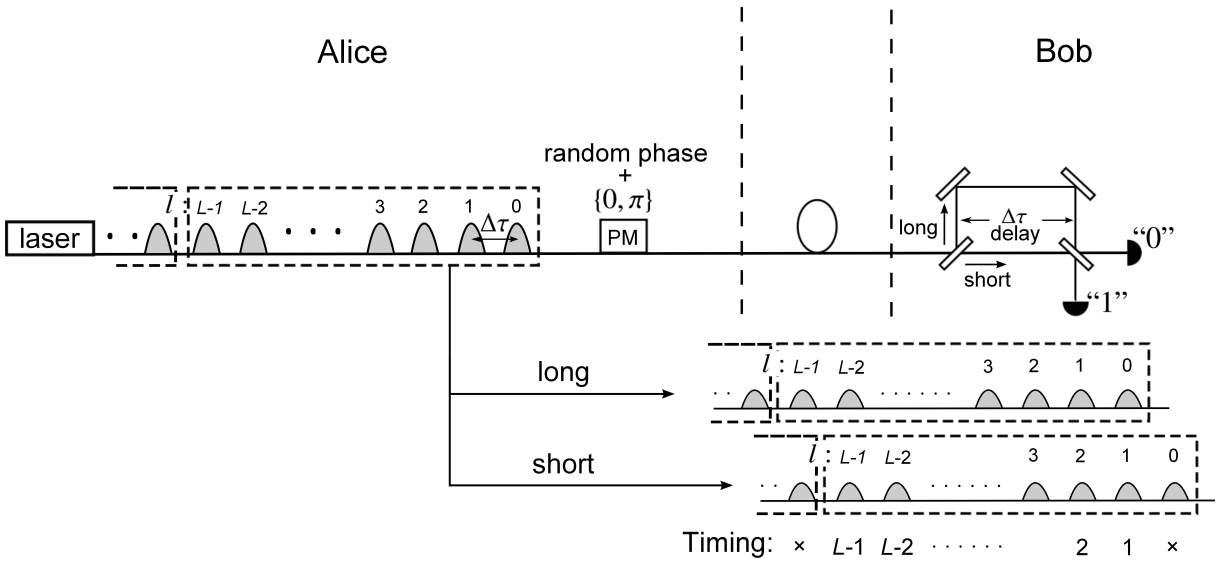

Figure 4.3: Set up of the DPS protocol. At Alice's site, pulse trains are generated by a laser followed by phase randomization as well as phase modulation (PM) with $\{0, \pi\}$ based on her random bits. At Bob's site, each pulse train is fed to a delayed Mach-Zehnder interferometer. The trains leaving the interferometer are measured by two photon detectors corresponding to bit values "0" and "1". Valid timings of detection are labeled by integers $1, 2, .., L-1$, according to the index of the pulse from the short arm of the interferometer. Detection from interference between pulses from different blocks is regarded as invalid and ignored.

1. Alice generates L random bits $a_l \in \{0, 1\}$ $(0, 1, .., L-1)$.
2. Alice prepares L optical pulses (system S) in the state

$$\bigotimes_{l=0}^{L-1} |(-1)^{a_l} \sqrt{\mu}\rangle_{S,l}, \tag{4.76}$$

where $|\sqrt{\mu}\rangle_{S,l}$ represents a coherent state $e^{-\mu/2} \sum_k \frac{\sqrt{\mu}^k}{\sqrt{k!}} |k\rangle_{S,l}$ of the l-th pulse mode. Alice randomizes the overall optical phase of the L-pulse train, and sends it to Bob.

3. If there is no detection of photons in the valid timings, Bob sets $j = 0$. Bob also sets $j = 0$ if he detects two photons or more in the whole $L + 1$ time slots. If detections have only occurred at a single valid timing, the variable j is set to the index of the timing. If $j \neq 0$, Bob determines his raw key bit $b \in \{0, 1\}$ depending on which detector has reported detection at the j-th timing. Bob announces j through the public channel.
4. If $j \neq 0$, Alice determines her raw key bit as $a = a_{j-1} + a_j$.
5. Alice and Bob repeat the above procedures n_{rep} times.

6. Alice and Bob randomly select a small portion of the rounds with $j \neq 0$, and compare the bit values over the public channel. They define sifted keys $\boldsymbol{\kappa}_A$ and $\boldsymbol{\kappa}_B$, respectively, by concatenating the remaining bits with $j \neq 0$.
7. Alice and Bob conduct error correction and privacy amplification by discussing over the public channel and obtain the final key $\boldsymbol{\kappa}_A^{\text{fin}}$ and $\boldsymbol{\kappa}_B^{\text{fin}}$.

The plus sign in Step 4 represents addition modulo 2 and corresponds to reading the relative phase of neighboring pulses.

4.4.2 Security of DPS protocol

Since the DPS protocol does not require multiple bases but uses the set of non-orthogonal states Eq. (4.76), it seems close to the B92 protocol [86] rather than the BB84 protocol. The remarkable property of the DPS protocol is that the optical phase of each pulse is not independent of each other but connected via the relative phases, just as chain. In fact, the robustness of the DPS protocol against PNS attacks can also be explained intuitively with the property of "coherence chain". If Eve splits photons from a multi-photon signal and sends a remaining photon to Bob, the probability that her detection timing j is identical to Bob's one is only $1/(L-1)$. Furthermore, if she attempts to make the photon detected at the same timing as hers, it disturbs the coherence chain and causes a bit error between Alice and Bob. Thus, the DPS protocol is expected to be robust against PNS attacks.

On the other hand, the property of coherence chain introduces difficulty in the security proof for the DPS protocol as well. This is because the coherence chain prohibits us from working on each pulse separately, and we have to deal with a large Hilbert space at once. In spite of the complexity, the security of the DPS protocol was proved in 2012 by Tamaki *et al*. in the asymptotic limit [90]. They focused on the fact that the phase errors in the DPS protocol are related to the photon number contained in pulses, and used the technique to estimate the photon-number information. The proof shows that a key can be generated from two-photon signals, as well as shows that the dependence of key rate on the channel transmittance η is $O(\eta^{3/2})$ in the range of small η, which certifies the expected robustness of the DPS protocol against PNS attacks. On the other hand, the security proof was still complicated and the obtained key rate was low because of the asymmetric property of the DPS protocol. For example, one of Eve's optimal attacks was that she sends Bob a superposition of the states containing photons in l-th timing whose coefficients are not uniform. This is coming from the fact that the detections only with $1 \leq j \leq L-1$ are regarded as valid and the detections at the edge of a block are discarded. The problem due to the asymmetry led to the idea of the round-robin DPS protocol introduced in the

following subsection.

4.4.3 Round-robin DPS protocol

The round-robin DPS (RR-DPS) protocol is regarded as the "symmetrized" DPS protocol, which removes the asymmetry among detection timings by modifying the set up of the protocol [41]. While the DPS protocol uses fixed amount of delay $\Delta\tau$ at the interferometer, the delay is variable in $\{\Delta\tau, 2\Delta\tau, ..., (L-1)\Delta\tau\}$ in the RR-DPS protocol. This additional randomness at Bob's site prevents Eve from fixing two pulses which cause interference at her will, as well as largely simplifies the security proof. The security proof adopts a similar idea to that of the DPS protocol, in which phase errors are related to the photon number contained in the signal pulses. The obtained key rate is expressed as

$$Q\left(1 - h(e_{\rm bit}) - \frac{e_{\rm src}}{Q} - (1 - \frac{e_{\rm src}}{Q})h(\frac{\nu_{\rm th}}{L-1})\right), \tag{4.77}$$

where $e_{\rm bit}$ is the observed error rate, and $e_{\rm src}$ and $\nu_{\rm th}$ are connected through the following inequality in terms of the photon number ν in L pulses:

$$\Pr(\nu > \nu_{\rm th}) \leq e_{\rm src}. \tag{4.78}$$

In Eq. (4.77), the second term represents the cost for error correction, and the third and fourth terms represent the cost for privacy amplification. Eq. (4.77) implies that the amount of privacy amplification is independent of the observed error rate $e_{\rm bit}$ and only depends on the property of a light source and the predetermined block size L. This is totally a new concept in the security of QKD because the security of QKD protocols prior to this protocol was based on the uncertainty principle and the amount of leaked information is estimated by monitoring signal disturbance (bit error). It is not certain what kind of principle in quantum mechanics enables such a property, though the authors implies [41] that it may relate to the information causality [112].

Thanks to the property of $e_{\rm bit}$-independence, it has high tolerance against noisy environment. The numerical simulation in Ref. [41] shows that it still generates a key at the error rate $e_{\rm bit} \geq 11\%$, in which no key can be extracted with the BB84 protocol. On the other hand, the simplicity of the DPS protocol is sacrificed in the RR-DPS protocol. Although several demonstrations have already been conducted, implementations of the variable delay with large L ($L = 5$ [43], $L = 65$ [45], $L = 129$ [44]) are not considered to be simple.

Chapter 5

Security of the DQPS protocol

As introduced in the previous chapter, the DPS protocol is composed of simple devices and is robust against PNS attacks, while the security proof is complicated. In this chapter, we seek after the benefit of the DPS protocol in a different direction, namely, for short-distance communication in which PNS attacks do not impose a severe problem. We provide a security proof of a variant of the DPS protocol called differential quadrature phase shift (DQPS) protocol [46] by applying the simple proof for the BB84 protocol, and establish its definite advantage over the PE-BB84 protocol. The DQPS protocol can be implemented with essentially the same hardware as the PE-BB84 protocol, but our security proof shows that its key generation rate is 8/3 as high as that of the PE-BB84 protocol. The benefit from the simplicity of PE-BB84 protocol is not sacrificed because the requirement for the properties of the light source and the detection apparatus is shown to be kept to minimum as in the PE-BB84 protocol. Although the security proof is limited to the asymptotic regime in this chapter, it is extended to the finite-key case in Chapter 6.

In this chapter, we use several different notations from those in the previous chapters. We call the basis to generate a key "data basis" and call the basis for monitoring signal disturbance "check basis". In the BB84 protocol considered in the previous sections, the data basis and the check basis were called Z basis and X basis, respectively. But here, we do not associate the data and check bases to qubit bases (such as X and Z) in the description of the DQPS protocol in Sec. 5.1. Qubits will be introduced in the security analysis in Sec. 5.2. There, we opt to follow the convention of taking the photon-number states as the standard basis, and hence associate the $\{|0\rangle, |1\rangle\}$ basis of a qubit to the (parity of) photon number. We assume that Alice's state preparation on the data basis is replaced by $\{|+\rangle, |-\rangle\}$-basis measurement, and also assume that the measurement to obtain phase error is made by $\{|-i\rangle, |+i\rangle\}$ basis where $|\pm\rangle := (|0\rangle \pm |1\rangle)/\sqrt{2}$ and $|\pm i\rangle := (|0\rangle \pm i|1\rangle)/\sqrt{2}$. When we represent an outcome of the $\{|+\rangle, |-\rangle\}$ basis measurement by a bit, it should be understood that state $|+\rangle$ corresponds to bit value 0 and state $|-\rangle$ to 1. On the other

hand, for $\{|-i\rangle, |+i\rangle\}$-basis measurement, we adopt an unconventional rule that $|-i\rangle$ corresponds to bit value 0 and $|+i\rangle$ to 1 for the convenience of the proof.

This chapter is organized as follows. In Sec. 2, we describe details of the DQPS protocol and assumptions on the light source and the detection apparatus. Sec. 3 gives the security proof of the protocol, and shows an explicit formula for the key rate. Based on the formula, numerical results for the secure key rate is shown in Sec. 4. Finally, Sec. 5 deals with discussions including an analytical expression for the scaling of the optimal key rate and simple off-line calibration methods for the light source.

5.1 Protocol and assumptions

Here we introduce a DQPS protocol considered in this chapter, which is slightly modified from the one [46] proposed by Inoue and Iwai (See Fig. 5.1). The protocol uses two bases, data basis for generating the final key and check basis for monitoring the leak of information. In the data and check bases, relative phases between adjacent pulses are modulated by $\{0, \pi\}$ and $\{\frac{\pi}{2}, \frac{3\pi}{2}\}$, respectively. The protocol regards a train of L pulses as a block, and the working basis is randomly chosen for each block. The randomization of overall optical phase is also done for each block of L pulses. Bob's receiver is composed of delayed interferometer with its delay being equal to the interval $\Delta\tau$ of adjacent pulses. The longer arm of the interferometer passes through a phase modulator that incurs phase shift $\theta_B = 0$ or $\frac{\pi}{2}$. After the interferometer, the pulses are measured by two photon detectors corresponding to bit values "0" and "1". If there is a detection from the superposition of the l-th and the $(l-1)$-th original pulses, we call it as valid detection at l-th timing $(1 \leq l \leq L-1)$.

The protocol proceeds as follows, which includes predetermined parameters $\tilde{p}_1 > 0$, $\tilde{p}_0 := 1 - \tilde{p}_1$, $\mu > 0$, and $n_{\rm rep}$. In its description, $|\boldsymbol{\kappa}|$ represents the length of a bit sequence $\boldsymbol{\kappa}$.

1. Alice selects a bit $c \in \{0, 1\}$ with probability $\tilde{p}_0$ and $\tilde{p}_1$, which correspond to the choice of data basis and check basis, respectively. Bob also selects $d \in \{0, 1\}$ with probability $\tilde{p}_0$ and $\tilde{p}_1$.

2. Alice generates L random bits $a_l \in \{0, 1\}$ $(0, 1, .., L-1)$, and prepares L optical pulses (system S) in the state

$$\bigotimes_{l=0}^{L-1} |e^{i\theta_l(a_l,c)}\sqrt{\mu}\rangle_{S,l}, \quad \theta_l(a_l, c) := a_l\pi + \frac{\pi}{2}lc, \tag{5.1}$$

where $|\alpha\rangle_{S,l}$ represents coherent state $e^{-|\alpha|^2/2}\sum_k \frac{\alpha^k}{\sqrt{k!}}|k\rangle_{S,l}$ of the l-th pulse mode. Alice randomizes the overall optical phase of the L-pulse train, and sends it to Bob.

3. If $d = 0$, Bob sets $\theta_B = 0$. If $d = 1$, he sets $\theta_B = \frac{\pi}{2}$.

4. If there is no detection of photons in the valid timings, Bob sets $j = 0$. If the detections have

only occurred at a single valid timing, the variable j is set to the index of the timing. If there are detections at multiple timings, the smallest (earliest) index of them is assigned to j. If $j \neq 0$, Bob determines his raw key bit $b \in \{0, 1\}$ depending on which detector has reported detection at the j-th timing. If both detectors have reported at the j-th timing, a random bit is assigned to b. Bob announces j through the public channel.

5. If $j \neq 0$, Alice determines her raw key bit as $a = a_{j-1} + a_j$ where the plus sign represents addition modulo 2.

6. Alice and Bob repeat the above procedures n_{rep} times. They publicly disclose c and d for each of the n_{rep} rounds.

7-1. Alice and Bob define sifted keys $\boldsymbol{\kappa}_{A1}$ and $\boldsymbol{\kappa}_{B1}$, respectively, by concatenating their determined bits with $j \neq 0$ and $c = d = 1$. They publicly disclose $\boldsymbol{\kappa}_{A1}$ and $\boldsymbol{\kappa}_{B1}$.

7-2. Alice defines a sifted key $\boldsymbol{\kappa}_{A0}$ by concatenating her determined bits with $j \neq 0$ and $c = d = 0$.

7-3. Bob defines a sifted key $\boldsymbol{\kappa}_{B0}$ by concatenating his determined bits with $j \neq 0$ and $c = d = 0$.

8. Bob corrects the errors in his sifted key $\boldsymbol{\kappa}_{B0}$ to make it coincide with Alice's key $\boldsymbol{\kappa}_{A0}$ through $|\boldsymbol{\kappa}_{A0}|S_{\text{EC}}$ bits of encrypted public communication from Alice by consuming the same length of pre-obtained secret key. Alice and Bob conduct privacy amplification by shortening their keys by $|\boldsymbol{\kappa}_{A0}|S_{\text{PA}}$ to obtain the final keys.

In this chapter, we only consider the secure key rate in the asymptotic limit of an infinite sifted key length. We consider the limit of $n_{\text{rep}} \to \infty$ while the following observed parameters are fixed:

$$Q := \frac{|\boldsymbol{\kappa}_{A0}|}{n_{\text{rep}}\tilde{p}_0^2}, \quad E_0 := \frac{\text{wt}(\boldsymbol{\kappa}_{B0} - \boldsymbol{\kappa}_{A0})}{n_{\text{rep}}\tilde{p}_0^2}, \quad E_1 := \frac{\text{wt}(\boldsymbol{\kappa}_{B1} - \boldsymbol{\kappa}_{A1})}{n_{\text{rep}}\tilde{p}_1^2}, \tag{5.2}$$

where the minus sign is a bit-by-bit modulo-2 subtraction. In this limit, S_{EC} is given by a function of the bit error rate E_0/Q. In Sec. 5.2, the asymptotic value of S_{PA} is determined as a function of Q and E_1. The asymptotic key rate per pulse R_L is then given by

$$R_L = \frac{\tilde{p}_0^2}{L} Q(1 - S_{\text{PA}}(Q, E_1) - S_{\text{EC}}(E_0/Q)). \tag{5.3}$$

The security of the above protocol is proved in Sec. 5.2 under the following assumptions on the devices used by Alice and Bob. For clarity, up to Sec. 5.3, we assume that Alice's laser source and modulator produces the states in Eq. (1) precisely. The assumption on the laser will then be relaxed in Sec. 5.4. The randomization of the overall phase in Step 2 is assumed to be done by choosing a common optical phase shift ϕ randomly from the continuous range of $[0, 2\pi)$, and applying it to all the L pulses. As is seen in Sec. 4.2.1, this eliminates the coherence among different photon-number states. The state emitted from Alice in Step 2 is thus expressed as

$$\sum_m \hat{N}_m \Big(\bigotimes_{l=0}^{L-1} |e^{i\theta_l(a_l,c)}\sqrt{\mu}\rangle_{S,l} \langle e^{i\theta_l(a_l,c)}\sqrt{\mu}| \Big) \hat{N}_m, \tag{5.4}$$

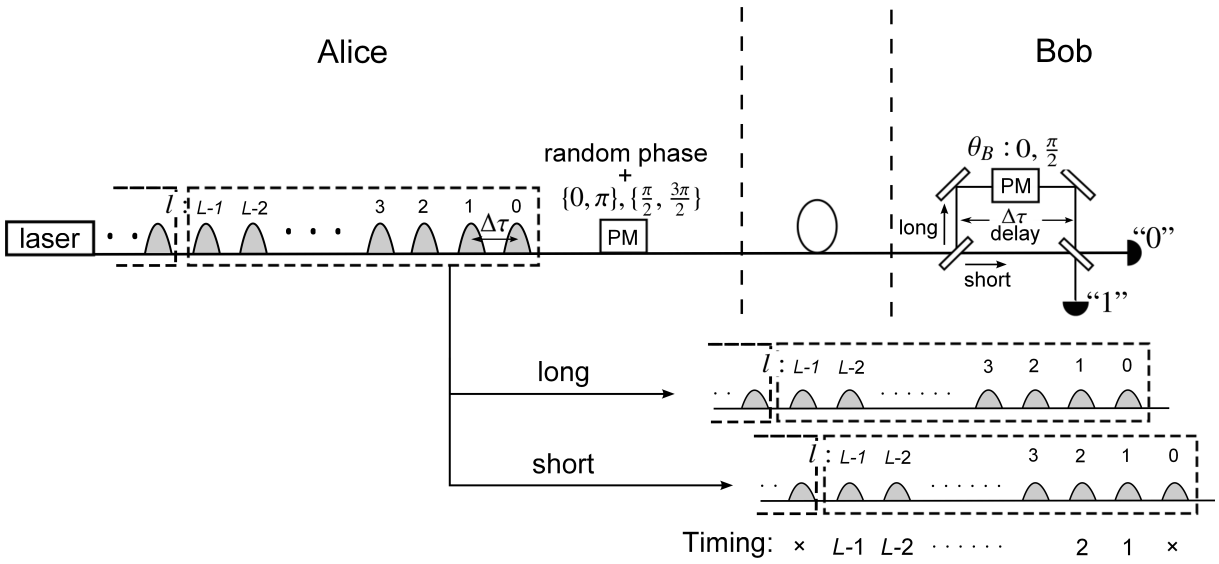

Figure 5.1: Setup for the L-pulse DQPS protocol. At Alice's site, pulse trains are generated by a laser followed by phase randomization as well as phase modulation (PM) with $\{0,\pi\}$ or $\{\frac{\pi}{2},\frac{3\pi}{2}\}$ according to her random bits and basis choice. At Bob's site, each pulse train is fed to a delayed Mach-Zehnder interferometer with phase shift 0 or $\frac{\pi}{2}$ according to his basis choice. The trains leaving the interferometer are measured by two photon detectors corresponding to bit values "0" and "1". Valid timings of detection are labeled by integers $1, 2, .., L-1$, according to the index of the pulse from the short arm of the interferometer. Detection from interference between pulses from different blocks is regarded as invalid and ignored.

where $\hat{N}_m$ represents the projector onto the subspace with m photons in the L pulses.

As for Bob's apparatus, we assume that he uses threshold detectors, and further assume that the inefficiency and dark countings of the detectors are equivalently represented by an absorber and a stray photon source placed in front of Bob's apparatus, and hence they are included in the quantum channel. This allows us to regard each of the detectors in Fig. 5.1 as a perfect threshold detector, which reports detection if and only if it receives one or more photons. To represent a relevant consequence of that assumption in a useful form, we introduce POVM elements for Bob's procedure in Steps 3 and 4. Let $\{\hat{B}_j^{(d)}\}_{j=0,\ldots,L-1}$ be the POVM for Bob's procedure of determining j, when the basis d was selected in Step 1. We further decompose the elements for $j \neq 0$ as $\hat{B}_j^{(d)} = \hat{B}_{j,0}^{(d)} + \hat{B}_{j,1}^{(d)}$, where $\hat{B}_{j,b}^{(d)}$ corresponds to the outcome (j,b). These operators satisfy

$$\hat{B}_0^{(d)} + \sum_{j=1}^{L-1} (\hat{B}_{j,0}^{(d)} + \hat{B}_{j,1}^{(d)}) = \hat{\mathbb{1}}. \tag{5.5}$$

Under the model of detectors mentioned above, whether there is a detection or not at each timing does not depend on the phase shift applied on the long arm. Hence, the procedure to determine j is the same for $d = 0$ and $d = 1$, and we have

$$\hat{B}_j^{(0)} = \hat{B}_j^{(1)} \quad (0 \leq j \leq L-1), \tag{5.6}$$

which will be used in the security proof given in the next section.

5.2 Security proof

Here we prove the security of the protocol introduced in Sec. 5.1 and determine the amount of privacy amplification $S_{\mathrm{PA}}(Q, E_1)$ in the asymptotic limit. Our proof is based on the security analysis with complementarity as well as the tagging technique with a modification. Before introducing the detail of the proof, let us discuss the difference between the original tagging idea and ours. In the security proof of the PE-BB84 protocol, if a pair of pulses emitted from Alice contains more than a single photon, that signal is considered to be tagged and totally insecure. The argument relies on the fact that the state emitted by Alice is expressed as mixture of photon-number states as in Eq. (4.6) with Eq. (4.13). Intuitively, we might want to use the same idea for the security proof of the DQPS protocol because a key bit is generated from a pair of pulses like in the PE-BB84 protocol. However, this turns out to be difficult because in the DQPS protocol, Alice generates a key bit $a = a_{j-1} + a_j$ after Bob's announcement of detection timing j. Obviously, the $(j-1)$-th and j-th pulses were already received by Bob and it is too late for Alice to conduct a direct measurement to determine the total photon number, and hence it is impossible to assume the form of Eq. (4.6), even in principle. In what follows, we will circumvent this issue by introducing a tagging rule defined through measurements on Alice's fictitious auxiliary qubits, which remain at Alice's site during the whole protocol.

5.2.1 Virtual protocol

For the security proof with complementarity, we consider virtual protocol in which Alice's sifted key $\boldsymbol{\kappa}_{A0}$ are obtained from measurements on auxiliary qubits on $\{|+\rangle, |-\rangle\}$ basis, while Bob, instead of aiming to learn $\boldsymbol{\kappa}_{A0}$, tries to guess the value of the complementary observable (the outcome of $\{|-i\rangle, |+i\rangle\}$-basis measurement) for Alice's qubits. The virtual protocol is designed to fulfill the following conditions:

(i) Alice's procedure of releasing optical pulses, making her public announcement $\boldsymbol{\kappa}_{A1}$, and producing the final key is identical to the actual protocol.

(ii) Bob's procedure of receiving L pulses and making his public announcement j (for each round) and $\boldsymbol{\kappa}_{B1}$ in the actual protocol is identical to the corresponding procedure in the virtual protocol.

Apparently, the protocol satisfying the conditions (i) and (ii) also satisfies the condition of the virtual protocol mentioned in Sec. 3.2.3. Hence, Alice's final key in the actual protocol is secure (random and decoupled from Eve's system) if that in the virtual protocol is secure against Eve's general attack.

Now we introduce an virtual entanglement-based protocol satisfying conditions (i) and (ii) by using the replacement of state preparation (see Sec. 3.2.1). In the protocol, Alice correlates an auxiliary qubit to each optical pulse, and prepare a state by making measurement on $\{|+\rangle, |-\rangle\}$ basis. A controlled-NOT (CNOT) gate $\hat{U}^{(j)}_{\mathrm{CNOT}}$ appearing in the protocol below is defined on $\{|0\rangle, |1\rangle\}$ basis by $\hat{U}^{(j)}_{\mathrm{CNOT}} |x\rangle_{A,j} |y\rangle_{A,j-1} = |x\rangle_{A,j} |x + y \bmod 2\rangle_{A,j-1}$ $(x, y \in \{0, 1\})$. The detail of the virtual protocol is described below, where a step including a different procedure from the actual protocol is marked with an asterisk (*).

Virtual protocol.

1. Alice selects a bit $c \in \{0, 1\}$ with probability $\tilde{p}_0$ and $\tilde{p}_1$, which correspond to the choice of data basis and check basis, respectively. Bob also selects $d \in \{0, 1\}$ with probability $\tilde{p}_0$ and $\tilde{p}_1$.

2*. Alice prepares L auxiliary qubits (system A) and L optical pulses (system S) in state

$$|\Psi(c)\rangle_{AS} := \bigotimes_{l=0}^{L-1} |\psi(c)\rangle_{AS,l} \tag{5.7}$$

depending on her basis choice, where

$$|\psi(c)\rangle_{AS,l} := \frac{1}{\sqrt{2}}(|+\rangle_{A,l} |e^{i\frac{\pi}{2}lc} \sqrt{\mu}\rangle_{S,l} + |-\rangle_{A,l} |-e^{i\frac{\pi}{2}lc} \sqrt{\mu}\rangle_{S,l}). \tag{5.8}$$

She measures the total photon number m in the L pulses with the projective measurement $\{\hat{N}_m\}$, and sends the L pulses to Bob.

3*. Bob sets $\theta_B = \frac{\pi}{2}$ regardless of the value of d.

4. If there is no detection of photons in the valid timings, Bob sets $j = 0$. If the detections have only occurred at a single valid timing, the variable j is set to the index of the timing. If there are detections at multiple timings, the smallest (earliest) index of them is assigned to j. If $j \neq 0$, Bob determines his raw key bit $b \in \{0, 1\}$ depending on which detector has reported detection at the j-th timing. If both detectors have reported at the j-th timing, a random bit is assigned to b. Bob announces j through the public channel.

5-1*. If $j = 0$, proceed to Step 6. Otherwise, Alice operates a CNOT gate $\hat{U}^{(j)}_{\mathrm{CNOT}}$ on the $(j-1)$-th

qubit (target) and the j-th qubit (control).
5-2*. Alice measures all the qubits but the j-th one on $\{|0\rangle_{A,l}, |1\rangle_{A,l}\}$ basis to obtain the outcomes z_l ($l \neq j$).
5-3*. Alice measures the j-th qubit on $\{|+\rangle_{A,j}, |-\rangle_{A,j}\}$ basis and determines her raw key bit a accordingly.
6. Alice and Bob repeat the above procedures $n_{\rm rep}$ times. They publicly disclose c and d for each of the $n_{\rm rep}$ rounds.
7-1. Alice and Bob define sifted keys $\boldsymbol{\kappa}_{A1}$ and $\boldsymbol{\kappa}_{B1}$, respectively, by concatenating their determined bits with $j \neq 0$ and $c = d = 1$. They publicly disclose $\boldsymbol{\kappa}_{A1}$ and $\boldsymbol{\kappa}_{B1}$.
7-2. Alice defines a sifted key $\boldsymbol{\kappa}_{A0}$ by concatenating her determined bits with $j \neq 0$ and $c = d = 0$.
7-3*. Bob defines a sifted key $\boldsymbol{\kappa}^*_{B0}$ by concatenating his determined bits with $j \neq 0$ and $c = d = 0$. He publicly discloses $\boldsymbol{\kappa}^*_{B0}$.
8*. Alice conducts privacy amplification by shortening her key by $|\boldsymbol{\kappa}_{A0}| S_{\rm PA}$ to obtain the final key.

The above protocol satisfies the condition (ii) because of the following reasons. Since Step 3* is identical to the actual protocol for $d = 1$, so is Bob's announcement of $\boldsymbol{\kappa}_{B1}$. The change in Step 3* does not affect the announcement of j in each round due to Eq. (5.6). Note that the change in Step 7-3* is an additional announcement which is not disclosed in the actual protocol. In order to see that the condition (i) holds, we will modify the virtual protocol in such a way that Alice's procedure dictated in (i) is unchanged. Since the outcomes $\{z_l\}$ in Step 5-2* are neither announced nor used in determining the final key, we can omit this step. Since a CNOT gate on $\{|0\rangle, |1\rangle\}$ basis is equivalent to a CNOT gate on $\{|+\rangle, |-\rangle\}$ basis with target and control exchanged, Steps 5-1* and 5-3* are equivalently done by measuring all the L qubits on $\{|+\rangle, |-\rangle\}$ basis to obtain L bits $a_0, a_1, .., a_{L-1}$ as the outcome, and then setting $a = a_{j-1} + a_j$. Since the $\{|+\rangle, |-\rangle\}$-basis measurement on all the qubits does not require the knowledge of j, we may assume that it is done in Step 2*. Then, using the relation

$$ {}_{A,l}\langle \pm | \, |\psi(c)\rangle_{AS,l} = \frac{1}{\sqrt{2}} \, |\pm e^{i\frac{\pi}{2}lc} \sqrt{\mu}\rangle \,, \tag{5.9} $$

we see that the L-bit sequence $a_0, a_1, .., a_{L-1}$ is random and conditioned on its value the emitted state is identical to Eq. (5.4). Hence, it is equivalent to Steps 2 and 5 of the actual protocol. Finally, Steps 7-3* and 8* are the same as in the actual protocol as far as Alice is concerned. Therefore, the virtual protocol satisfies the condition (i), as well as (ii), which means that the security of the virtual protocol implies the security of the actual protocol.

5.2.2 Alternative definition of tagging

To prove the security of the virtual protocol, we focus on the tagging technique for the PE-BB84 protocol, in which the incidents with multi-photon emission in double pulses are tagged and considered to be insecure. In a similar vein, we might want to tag the events where the $(j-1)$-th and j-th pulses include multiphotons upon emission. However, the number of emitted photons in the two pulses is not well-defined due to the phase coherence with other pulses. Instead, we define a rule to classify tagged ($t = 1$) and untagged ($t = 0$) incidents in terms of variables well-defined in the virtual protocol:

$$\sum_{l\neq j} z_l = m \;\rightarrow\; t = 0, \qquad \sum_{l\neq j} z_l < m \;\rightarrow\; t = 1. \tag{5.10}$$

Let $\boldsymbol{\kappa}_{A0,\mathrm{unt}}$ be the concatenation of all the untagged bits in $\boldsymbol{\kappa}_{A0}$, and define the ratio of tagged incidents as

$$\Delta := 1 - \frac{|\boldsymbol{\kappa}_{A0,\mathrm{unt}}|}{|\boldsymbol{\kappa}_{A0}|}. \tag{5.11}$$

From Eq. (4.45) and the argument in Sec. 4.2.2, if the phase-error rate for untagged portion is bounded by $\delta(Q, E_1, \Delta)$, $\boldsymbol{\kappa}_{A0}$ can be made to be secure in the asymptotic limit by reducing its length by $|\boldsymbol{\kappa}_{A0}|S_{\mathrm{PA}}$ satisfying

$$S_{\mathrm{PA}}(Q, E_1) \geq \max_{\Delta} \left(\Delta + (1-\Delta)h\left(\delta(Q, E_1, \Delta)\right)\right). \tag{5.12}$$

Let us discuss the implication of the condition Eq. (5.10) for the tagging, and derive important relations that will be used in the subsequent proof of security. According to Eq. (5.8), it is not difficult to see that ${}_{A,l}\langle 0|\,|\psi(c)\rangle_{AS,l}$ includes only even number of photons, and ${}_{A,l}\langle 1|\,|\psi(c)\rangle_{AS,l}$ does odd number of photons. For convenience, let us define projectors related to such a property by

$$\begin{aligned}
\hat{\Upsilon}_{AS} &:= \bigotimes_{l=0}^{L-1} \hat{\Upsilon}^{(l)}, \\
\hat{\Upsilon}^{(l)} &:= \hat{P}(|0\rangle_{A,l}) \left(\sum_{n:\mathrm{even}} \hat{P}(|n\rangle_{S,l}) \right) + \hat{P}(|1\rangle_{A,l}) \left(\sum_{n:\mathrm{odd}} \hat{P}(|n\rangle_{S,l}) \right),
\end{aligned} \tag{5.13}$$

where $\hat{P}(|\cdot\rangle) = |\cdot\rangle\langle\cdot|$. Notice that the initial state in Eq. (5.7) satisfies

$$\hat{\Upsilon}_{AS}\,|\Psi(c)\rangle_{AS} = |\Psi(c)\rangle_{AS}\,. \tag{5.14}$$

Thanks to the correlation specified by $\hat{\Upsilon}_{AS}$, the measured quantities $\{z_l\}$ are related to the parity of the photon numbers in the system S. To see this, let us define the projector corresponding to the state of m_l photons in the l-th pulse by

$$\hat{N}_{\{m_l\}} := \bigotimes_{l=0}^{L-1} \hat{P}(|m_l\rangle_{S,l}). \tag{5.15}$$

Alice's procedure of determining $\{z_l\}$ $(l \neq j)$ at Steps 5-1* and 5-2* will be associated with the projector defined by

$$\begin{aligned}\hat{F}^{(j)}_{\{z_l\}} &:= \hat{U}^{(j)\dagger}_{\rm CNOT}\left(\hat{\mathbb{1}}_{A,j}\otimes\Big(\bigotimes_{l\neq j}\hat{P}(|z_l\rangle_{A,l})\Big)\right)\hat{U}^{(j)}_{\rm CNOT}\\ &= \Big[\hat{P}(|0\rangle_{A,j-1}\,|z_{j-1}\rangle_{A,j}) + \hat{P}(|1\rangle_{A,j-1}\,|1-z_{j-1}\rangle_{A,j})\Big]\bigotimes_{l\neq j-1,j}\hat{P}(|z_l\rangle_{A,l}).\end{aligned} \tag{5.16}$$

Then, it is easy to confirm that

$$\begin{aligned}&(\hat{F}^{(j)}_{\{z_l\}}\otimes\hat{N}_{\{m_l\}})\hat{\Upsilon}_{AS}\neq 0 \ \text{ only if}\\ &z_l = m_l \mod 2\ (l\neq j-1, j)\ \text{ and }\ z_{j-1} = m_{j-1}+m_j \mod 2.\end{aligned} \tag{5.17}$$

Since $\hat{N}_m\hat{N}_{\{m_l\}} = 0$ unless $\sum_l m_l = m$, we have

$$\begin{aligned}&(\hat{F}^{(j)}_{\{z_l\}}\otimes\hat{N}_m\hat{N}_{\{m_l\}})\hat{\Upsilon}_{AS}\neq 0 \ \text{ only if}\\ &z_l\leq m_l\ (l\neq j-1, j),\ \ z_{j-1}\leq m_{j-1}+m_j \ \text{ and }\ \sum_l m_l = m.\end{aligned} \tag{5.18}$$

If we confine ourselves to the case with $\sum_{l\neq j} z_l = m$, the condition in the above equation is satisfied only by $z_l = m_l$ $(l\neq j-1, j)$ and $z_{j-1} = m_{j-1}+m_j$. We thus conclude that

$$(\hat{F}^{(j)}_{\{z_l\}}\otimes\hat{N}_m)\hat{\Upsilon}_{AS} = (\hat{F}^{(j)}_{\{z_l\}}\otimes\hat{\Xi}^{(j)}_{\{z_l\}})\hat{\Upsilon}_{AS}\ \text{ for }\ \sum_{l\neq j} z_l = m, \tag{5.19}$$

where

$$\hat{\Xi}^{(j)}_{\{z_l\}} := \hat{P}(|0\rangle_{S,j-1}\,|0\rangle_{S,j})\bigotimes_{l\neq j-1,j}\hat{P}(|z_l\rangle_{S,l})\ \text{ for }\ z_{j-1}=0 \tag{5.20}$$

$$\hat{\Xi}^{(j)}_{\{z_l\}} := [\hat{P}(|0\rangle_{S,j-1}\,|1\rangle_{S,j}) + \hat{P}(|1\rangle_{S,j-1}\,|0\rangle_{S,j})]\bigotimes_{l\neq j-1,j}\hat{P}(|z_l\rangle_{S,l})\ \text{ for }\ z_{j-1}=1. \tag{5.21}$$

This may lead to an interpretation that, whenever the event is untagged, every pulse should have contained no more than one photon upon emission, and the $(j-1)$-th and the j-th pulse pair contained no more than one photon in total. On the other hand, we should also take notice that Alice's measurement of $\{z_l\}$ $(l\neq j)$ in the virtual protocol can be carried out only after the pulse train was measured by Bob and the value of j was announced. Hence the above interpretation has an ambiguity in the operational sense, which is why we only use strict mathematical statements of Eqs. (5.14) and (5.19) in the subsequent proof and do not rely on the interpretation.

5.2.3 Phase-error rate for untagged portion

Our next goal is to determine the upper bound of the phase-error rate for untagged portion $\delta(Q, E_1, \Delta)$ following the definition in the security proof with complementarity (see Sec. 3.2.2). To represent the phase error explicitly, let us introduce the following procedure instead of the Steps 5-3* and 7-2.

5-3**. If $c = 1$, Alice measures the j-th qubit on $\{|+\rangle_{A,j}, |-\rangle_{A,j}\}$ basis and determines her raw key bit a accordingly. If $c = 0$, Alice measures the j-th qubit on $\{|-i\rangle_{A,j}, |+i\rangle_{A,j}\}$ basis and determines her raw key bit a accordingly.
7-2**. Alice defines a sifted key $\boldsymbol{\kappa}^*_{A0}$ by concatenating her determined bits with $j \neq 0$ and $c = d = 0$.

Let $\boldsymbol{\kappa}^*_{A0,\mathrm{unt}}$ and $\boldsymbol{\kappa}^*_{B0,\mathrm{unt}}$ be the concatenations of all the untagged bits in $\boldsymbol{\kappa}^*_{A0}$ and $\boldsymbol{\kappa}^*_{B0}$, respectively. Phase errors for untagged portion are given as bit errors between $\boldsymbol{\kappa}^*_{A0,\mathrm{unt}}$ and $\boldsymbol{\kappa}^*_{B0,\mathrm{unt}}$ and the number of the phase errors is given by $\mathrm{wt}(\boldsymbol{\kappa}^*_{B0,\mathrm{unt}} - \boldsymbol{\kappa}^*_{A0,\mathrm{unt}})$. Suppose that we have a bound on phase error rate $\delta_{\mathrm{unt}}(Q, E_1, \Delta)$, which asymptotically satisfies

$$\delta_{\mathrm{unt}}(Q, E_1, \Delta) \geq \frac{\mathrm{wt}(\boldsymbol{\kappa}^*_{B0,\mathrm{unt}} - \boldsymbol{\kappa}^*_{A0,\mathrm{unt}})}{|\boldsymbol{\kappa}^*_{A0,\mathrm{unt}}|}. \tag{5.22}$$

Notice that the measurement on Alice's qubits for extracting $\boldsymbol{\kappa}_{A0}$ or $\boldsymbol{\kappa}^*_{A0}$ can be postponed until after Step 7-3*, namely, after she learns the values of Q, E_1, Δ and $\boldsymbol{\kappa}^*_{B0,\mathrm{unt}}$. Then, an extreme case of $\delta_{\mathrm{unt}}(Q, E_1, \Delta) = 0$ will mean that the state of $|\boldsymbol{\kappa}_{A0,\mathrm{unt}}|$ untagged qubits before the measurement is exactly a $\{|-i\rangle, |+i\rangle\}$-basis eigenstate specified by $\boldsymbol{\kappa}^*_{B0,\mathrm{unt}}$, and hence $\boldsymbol{\kappa}_{A0,\mathrm{unt}}$, which is an outcome of $\{|+\rangle, |-\rangle\}$-basis measurement, is secure (random and decoupled from Eve's system).

It can be shown that δ_{unt} is connected to the check-basis error rate E_1 of the actual protocol through a fair sampling. For given values of c and j, Alice's procedure of determining $\{z_l\}$ and a at Steps 5-1*, 5-2* and 5-3** corresponds to the projection onto the state $|\mathcal{A}^{(c,j)}_{a,\{z_l\}}\rangle_A$, which is defined by

$$|\mathcal{A}^{(c,j)}_{a,\{z_l\}}\rangle_A := \frac{1}{\sqrt{2}} \hat{U}^{(j)\dagger}_{\mathrm{CNOT}} \left(\left(|0\rangle_{A,j} - (-1)^a \, i^{\,c+1} |1\rangle_{A,j} \right) \bigotimes_{l \neq j} |z_l\rangle_{A,l} \right). \tag{5.23}$$

Since these states satisfy

$$\hat{F}^{(j)}_{\{z_l\}} |\mathcal{A}^{(c,j)}_{a,\{z_l\}}\rangle_A = |\mathcal{A}^{(c,j)}_{a,\{z_l\}}\rangle_A, \tag{5.24}$$

Eqs. (5.19) and (5.24) lead to

$${}_A\langle \mathcal{A}^{(c,j)}_{a,\{z_l\}}| \hat{N}_m \hat{\Upsilon}_{AS} = {}_A\langle \mathcal{A}^{(c,j)}_{a,\{z_l\}}| \hat{\Xi}^{(j)}_{\{z_l\}} \hat{\Upsilon}_{AS} \quad \text{for} \quad \sum_{l \neq j} z_l = m. \tag{5.25}$$

From Eq. (5.14), we have

$$ {}_A\langle \mathcal{A}^{(c,j)}_{a,\{z_l\}}| \hat{N}_m |\Psi(c)\rangle_{AS} = {}_A\langle \mathcal{A}^{(c,j)}_{a,\{z_l\}}| \hat{\Xi}^{(j)}_{\{z_l\}} |\Psi(c)\rangle_{AS} \quad \text{for} \quad \sum_{l\neq j} z_l = m. \tag{5.26} $$

The basis-choice dependence of states $|\mathcal{A}^{(c,j)}_{a,\{z_l\}}\rangle_A$ and $|\Psi(c)\rangle_{AS}$ can be represented by

$$ |\mathcal{A}^{(c,j)}_{a,\{z_l\}}\rangle_A = \left(\hat{P}(|0\rangle_{A,j}) + i^{\,c}\,\hat{P}(|1\rangle_{A,j})\right)|\mathcal{A}^{(0,j)}_{a,\{z_l\}}\rangle_A \tag{5.27} $$

and

$$ |\Psi(c)\rangle_{AS} = \left(\bigotimes_{l=0}^{L-1} i^{\,l\hat{m}_l c}\right)|\Psi(0)\rangle_{AS}\,, \tag{5.28} $$

where $\hat{m}_l := \sum_m m\hat{P}(|m\rangle_l)$ is the photon number operator for the l-th pulse. Since the range of the projector $\hat{\Xi}^{(j)}_{\{z_l\}}$ includes only zero- or one-photon states for each mode, we have

$$ [(\hat{P}(|0\rangle_{A,j}) + (-i)^c\hat{P}(|1\rangle_{A,j})) \otimes \hat{\Xi}^{(j)}_{\{z_l\}}]\hat{\Upsilon}_{AS} = (-i)^{c\hat{m}_j}\hat{\Xi}^{(j)}_{\{z_l\}}\hat{\Upsilon}_{AS}. \tag{5.29} $$

Combining Eqs. (5.14), (5.27), (5.28) and (5.29), we obtain

$$ {}_A\langle \mathcal{A}^{(c,j)}_{a,\{z_l\}}| \hat{\Xi}^{(j)}_{\{z_l\}} |\Psi(c)\rangle_{AS} = {}_A\langle \mathcal{A}^{(0,j)}_{a,\{z_l\}}| (-i)^{\hat{m}_j c}\left(\bigotimes_{l=0}^{L-1} i^{\,l\hat{m}_l c}\right)\hat{\Xi}^{(j)}_{\{z_l\}} |\Psi(0)\rangle_{AS}\,. \tag{5.30} $$

Using the definition of Eqs. (5.20) and (5.21), it is easy to confirm that

$$ (-i)^{c\hat{m}_j}\left(\bigotimes_{l=0}^{L-1} i^{\,l\hat{m}_l c}\right)\hat{\Xi}^{(j)}_{\{z_l\}} = i^{\,(j-1)z_{j-1}c}\left(\prod_{l\neq j-1,j} i^{\,lz_l c}\right)\hat{\Xi}^{(j)}_{\{z_l\}} \tag{5.31} $$

holds. Therefore, we have

$$ {}_A\langle \mathcal{A}^{(0,j)}_{a,\{z_l\}}| \hat{\Xi}^{(j)}_{\{z_{j-1}\}} |\Psi(0)\rangle_{AS} = (-i)^{u(j)}{}_A\langle \mathcal{A}^{(1,j)}_{a,\{z_l\}}| \hat{\Xi}^{(j)}_{\{z_{j-1}\}} |\Psi(1)\rangle_{AS}\,, \tag{5.32} $$

where $u(j) := \sum_{l\neq j-1,j} lz_l + (j-1)z_{j-1}$ and this leads, with Eq. (5.26), to

$$ {}_A\langle \mathcal{A}^{(0,j)}_{a,\{z_l\}}| \hat{N}_m |\Psi(0)\rangle_{AS} = (-i)^{u(j)}{}_A\langle \mathcal{A}^{(1,j)}_{a,\{z_l\}}| \hat{N}_m |\Psi(1)\rangle_{AS} \quad \text{for} \quad \sum_{l\neq j} z_l = m. \tag{5.33} $$

This relation may suggest that for untagged incidents, the state of pulses transmitted from Alice would be independent of the value of c, and hence the $c = d = 1$ incidents would be regarded as a fair sampling. Again, this interpretation suffers from ambiguity since the protocol assumes that Alice's qubits are measured only after the optical pulses are received by Bob and the value of j is announced. Therefore we need a mathematical proof for the fairness of the sampling, which is given in Appendix B. The proof confirms that

$$ \frac{\mathrm{wt}(\boldsymbol{\kappa}^*_{B0,\mathrm{unt}} - \boldsymbol{\kappa}^*_{A0,\mathrm{unt}})}{\mathrm{wt}(\boldsymbol{\kappa}_{B1,\mathrm{unt}} - \boldsymbol{\kappa}_{A1,\mathrm{unt}})} = \left(\frac{\tilde{p}_0}{\tilde{p}_1}\right)^2 \tag{5.34} $$

holds in the limit of $n_{\rm rep} \to \infty$. Then we have

$$\begin{aligned} \frac{{\rm wt}(\boldsymbol{\kappa}^*_{B0,{\rm unt}} - \boldsymbol{\kappa}^*_{A0,{\rm unt}})}{|\boldsymbol{\kappa}^*_{A0,{\rm unt}}|} &= \left(\frac{\tilde{p}_0}{\tilde{p}_1}\right)^2 \frac{{\rm wt}(\boldsymbol{\kappa}_{B1,{\rm unt}} - \boldsymbol{\kappa}_{A1,{\rm unt}})}{|\boldsymbol{\kappa}^*_{A0,{\rm unt}}|} \\ &\le \left(\frac{\tilde{p}_0}{\tilde{p}_1}\right)^2 \frac{{\rm wt}(\boldsymbol{\kappa}_{B1} - \boldsymbol{\kappa}_{A1})}{|\boldsymbol{\kappa}^*_{A0,{\rm unt}}|} \\ &= \frac{E_1}{Q(1-\Delta)}. \end{aligned} \tag{5.35}$$

Thus, $\delta(Q, E_1, \Delta) = E_1/(Q(1-\Delta))$ is an upper bound on the phase error rate satisfying Eq. (5.22). From Eq. (5.12), we conclude that asymptotically a privacy amplification with a ratio

$$S_{\rm PA}(Q, E_1) \ge \max_{\Delta} (\Delta + (1-\Delta) h\Big(\frac{E_1}{Q(1-\Delta)}\Big)) \tag{5.36}$$

is enough to make the sifted key $\boldsymbol{\kappa}_{A0}$ secure.

5.2.4 Upper bound on tagged ratio

Since the argument of the max in Eq. (5.36) is an increasing function of Δ, $S_{\rm PA}$ will be determined through finding an upper bound on Δ. According to the definition of Eq. (5.11), what we need is a lower bound on $|\boldsymbol{\kappa}_{A0,{\rm unt}}|$, which is determined as follows. If we denote by $n(condition)$ the number of rounds satisfying the *condition* in the $n_{\rm rep}$ rounds repeated in the virtual protocol, we have $|\boldsymbol{\kappa}_{A0}| = n(c = d = 0, j \neq 0)$ and $|\boldsymbol{\kappa}_{A0,{\rm unt}}| = n(c = d = 0, j \neq 0, t = 0)$, where $t = 0$ is equivalent to $\sum_{l \neq j} z_l = m$ according to Eq. (5.10). Under a given attack strategy of Eve, the statistics of $n(c = d = 0, j \neq 0)$ and $n(c = d = 0, j \neq 0, t = 0)$ is unchanged if we omit Step 5-3* and stop the protocol at Step 6. We may further equivalently replace Steps 5-1* and 5-2* with a procedure of measuring the L qubits on the $\{|0\rangle_{A,l}, |1\rangle_{A,l}\}$ basis to obtain the outcomes $z'_0, \cdots z'_{L-1}$, followed by substitutions $z_l := z'_l$ $(l \neq j-1, j)$ and $z_{j-1} := z'_{j-1} + z'_j \mod 2$ in case of $j \neq 0$. Let us define a set of values of L nonnegative integers as

$$\Gamma^{(m)} := \left\{ (k_0, \cdots, k_{L-1}) \,\middle|\, k_{l-1} + k_l \le 1 (1 \le l \le L-1), \sum_{l=0}^{L-1} k_l = m \right\}, \tag{5.37}$$

and operators associated with it by

$$\hat{\Pi}^{(m)}_A := \sum_{\{z'_l\} \in \Gamma^{(m)}} \bigotimes_{l=0}^{L-1} \hat{P}(|z'_l\rangle_{A,l}), \quad \hat{\Pi}^{(m)}_S := \sum_{\{m_l\} \in \Gamma^{(m)}} \bigotimes_{l=0}^{L-1} \hat{P}(|m_l\rangle_{S,l}). \tag{5.38}$$

We see that $(z'_0, \cdots z'_{L-1}) \in \Gamma^{(m)}$ implies $\sum_{l\neq j} z_l = m$ regardless of the value of j, as long as $j \neq 0$. Hence we have

$$\begin{aligned} & n(c=d=0, j\neq 0, t=0) \\ \geq\ & n(c=d=0, j\neq 0, (z'_0, \cdots z'_{L-1}) \in \Gamma^{(m)}) \\ =\ & n(c=d=0, j\neq 0) - n(c=d=0, j\neq 0, (z'_0, \cdots z'_{L-1}) \notin \Gamma^{(m)}) \\ \geq\ & n(c=d=0, j\neq 0) - n(c=d=0, (z'_0, \cdots z'_{L-1}) \notin \Gamma^{(m)}). \end{aligned} \tag{5.39}$$

The number $n(c=d=0, (z'_0, \cdots z'_{L-1}) \notin \Gamma^{(m)})$ is independent of Eve's strategy, and it follows the binomial distribution with success probability $\tilde{p}_0^2 r_{\text{tag}}$ with

$$r_{\text{tag}} \coloneqq 1 - \sum_m {}_{AS}\langle \Psi(0)| \hat{\Pi}_A^{(m)} \otimes \hat{N}_m |\Psi(0)\rangle_{AS}\,. \tag{5.40}$$

Since $z'_l = m_l \mod 2$ and $(m_0, \ldots, m_{L-1}) \in \Gamma^{(m)}$ imply $(z'_0, \cdots z'_{L-1}) \in \Gamma^{(m)}$, we have $\hat{\Pi}_S^{(m)}\hat{\Upsilon}_{AS} = (\hat{\Pi}_A^{(m)} \otimes \hat{\Pi}_S^{(m)})\hat{\Upsilon}_{AS}$. On the other hand, $z'_l = m_l \mod 2$ and $\sum_l z'_l = \sum_l m_l$ imply $z'_l = m_l$, which leads to $(\hat{\Pi}_A^{(m)} \otimes \hat{N}_m)\hat{\Upsilon}_{AS} = (\hat{\Pi}_A^{(m)} \otimes \hat{\Pi}_S^{(m)})\hat{\Upsilon}_{AS}$. We thus obtain

$$(\hat{\Pi}_A^{(m)} \otimes \hat{N}_m)\hat{\Upsilon}_{AS} = \hat{\Pi}_S^{(m)}\hat{\Upsilon}_{AS}\,. \tag{5.41}$$

Combined with Eq. (5.14), we obtain

$$r_{\text{tag}} = 1 - \sum_m {}_{AS}\langle \Psi(0)| \hat{\Pi}_S^{(m)} |\Psi(0)\rangle_{AS}\,, \tag{5.42}$$

which gives us a clear interpretation of quantity r_{tag} being the probability that the L-pulse train emitted from Alice contains at least two photons in the same pulse or in neighboring pulses. As a function of μ, it is calculated as

$$r_{\text{tag}} \ =\ 1 - \sum_{m=0}^{\lceil L/2\rceil} e^{-\mu L}\mu^m \frac{(L+1-m)!}{m!(L+1-2m)!}. \tag{5.43}$$

In the asymptotic limit of $n_{\text{rep}} \to \infty$, Eq. (5.39) implies

$$\frac{n(c=d=0, j\neq 0, t=0)}{n_{\text{rep}}} \geq \frac{n(c=d=0, j\neq 0)}{n_{\text{rep}}} - \tilde{p}_0^2 r_{\text{tag}}, \tag{5.44}$$

which means that $|\boldsymbol{\kappa}_{A0,\text{unt}}|/n_{\text{rep}} \geq |\boldsymbol{\kappa}_{A0}|/n_{\text{rep}} - \tilde{p}_0^2 r_{\text{tag}}$. Using Eqs. (5.2) and (5.11), we have

$$\Delta \leq \frac{r_{\text{tag}}}{Q}. \tag{5.45}$$

Hence, choosing

$$S_{\text{PA}}(Q, E_1) = \frac{r_{\text{tag}}}{Q} + \left(1 - \frac{r_{\text{tag}}}{Q}\right) h\left(\frac{E_1}{Q - r_{\text{tag}}}\right) \tag{5.46}$$

makes the virtual protocol, and hence the actual protocol, secure. An achievable asymptotic key rate per pulse is thus given by

$$R_L = \frac{\tilde{p}_0^2}{L}\Big((Q - r_{\rm tag})(1 - h\Big(\frac{E_1}{Q - r_{\rm tag}}\Big)) - QS_{EC}(E_0/Q)\Big) \tag{5.47}$$

whenever the right side is positive.

5.3 Key rates

We show results of numerical calculation of the key rate per pulse R_L given by Eq. (5.47) to compare the conventional passive PE-BB84 protocol (L=2) and the DQPS protocol ($L \geq 3$). In Fig. 5.2, dependence of R_L on overall transmission η (including detector efficiency) is shown for $L = 2, 4, 20$. We adopted $S_{\rm EC}(E_0/Q) = h(E_0/Q)$ and $\tilde{p}_0 = 1$. The solid curves represent the key rate R_L under the assumption that a dark count probability is $p_{\rm dark} = 0.5 \times 10^{-5}$ per pulse per detector. We assume $Q = 1 - e^{-(L-1)\mu\eta} + 2(L-1)p_{\rm dark}$, reflecting the fact that there are $(L-1)$ valid timings per block of pulses. We also assume that the error rate depends on $p_{\rm dark}$ and η in addition to a loss-independent rate 3%, namely, $E_0 = E_1 = 0.03(1 - e^{-(L-1)\mu\eta}) + (L-1)p_{\rm dark}$. The key rate R_L was then optimized over μ for each value of η. We see that except for a very low loss, a larger value of L leads to a higher rate and achieves a longer distance. The dotted curves represent the key rate for $p_{\rm dark} = 0$. From these curves, we see that, R_L for different values of L are all proportional to η^2 in the limit of small η, but its coefficient increases as L gets larger. For example, at 20 dB loss, we found that $R_{20}/R_2 \cong 2.67$, which clearly shows an advantage of the DQPS protocol over the PE-BB84 protocol when we use essentially the same hardware. We also see that even in the limit of no loss ($\eta \to 1$), the DQPS protocol with $L = 4$ is superior to the PE-BB84 protocol.

5.4 Discussion and conclusion

Figure 2 shows that the optimized key rates are proportional to η^2 in the limit of $\eta \to 0$, with its coefficient dependent on the block size L. In the special case where the bit error rate is zero, we can analytically determine the coefficient as a function of L. For $L\mu^2 \ll 1$, the parameter $r_{\rm tag}$ in Eq. (5.43) is approximated as $r_{\rm tag} = \frac{3L-2}{2}\mu^2$. For $L\mu\eta \ll 1$, the parameter Q is approximated as $Q = (L-1)\mu\eta$. Hence, for $L\eta^2 \ll 1$, the key rate $R_L = (Q - r_{\rm tag})/L$ is optimized at $\mu = \mu^{\rm opt} := \frac{L-1}{3L-2}\eta$ to attain the optimal value $R_L^{\rm opt} := \frac{(L-1)^2}{2L(3L-2)}\eta^2$. In the limit of a large block size, we have $R_{L\to\infty}^{\rm opt} = \eta^2/6$ and $R_{L\to\infty}^{\rm opt}/R_2^{\rm opt} = 8/3$. The result seems interesting in the sense that the secure key rate for a large value of L is *more than twice* as large as that of $L = 2$ while the inherent loss in

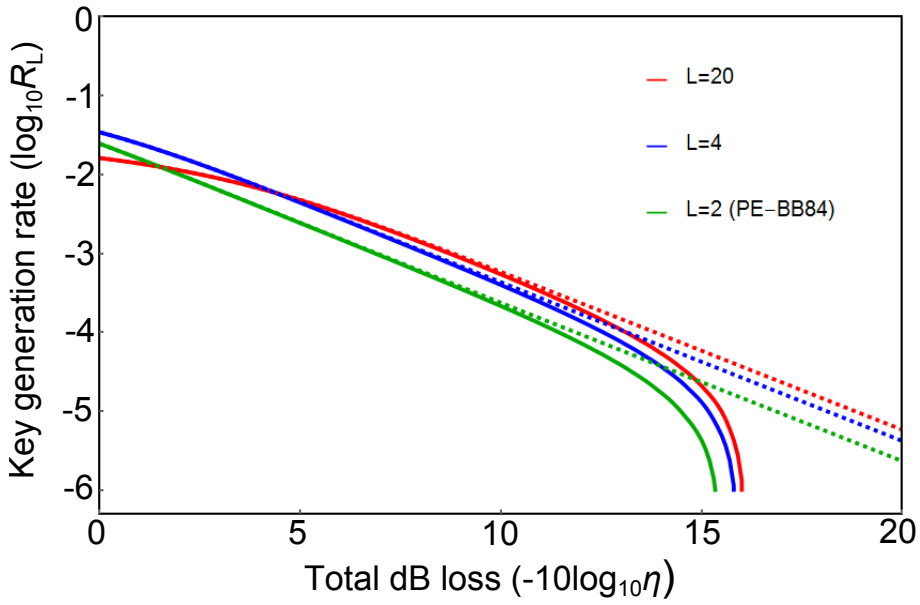

Figure 5.2: Secure key rate per pulse R_L as a function of the overall channel transmission η. The solid curves represent the key rate under the assumption that a dark count probability is $p_{\text{dark}} = 0.5\times10^{-5}$ per pulse per detector, and the dotted curves represent the key rate with $p_{\text{dark}} = 0$. For both solid and dotted curves, the top, the middle and the bottom curve (at a high dB loss) represent the rates for $L = 20$, $L = 4$ and $L = 2$, respectively. The bit error rate of the sifted key depends on p_{dark} and η in addition to a 3% loss-independent error. The block size L is chosen to be 2, 4, and 20, where $L = 2$ corresponds to the PE-BB84 protocol and the other values to the DQPS protocol.

the passive interferometer itself is 1/2 for $L = 2$. On the other hand, it does not mean that the key rate exceeds the case of $L = 2$ without the interferometer loss, namely, implementation with an ideal active optical switch. Since $R_L^{\rm opt} \propto \eta^2$ holds in the limit of small η, the key rate of an ideal active protocol is 4 times the rate of the passive one for $L = 2$. If the loss in the optical switch is taken into account, the passive DQPS protocol is more efficient than the active PE-BB84 protocol when the loss of optical switch is larger than $\sim 20\%$.

While we have assumed so far that the initial pure state represented in Eq. (5.1) is prepared by Alice, the proof can be extended to a general light source, which is shown in Appendix C. The proof there assumes that the phase modulator (PM in Fig. 5.1) works perfectly, and that every L-pulse train from the source is independent and represented by the same density operator $\hat{\sigma}_S$ (not necessarily identical for each pulse). For the general light source described above, the secure key rate is still given by Eq. (5.47) with

$$r_{\rm tag} = 1 - \sum_m {\rm tr}\left(\hat{\Pi}_S^{(m)} \hat{\sigma}_S\right). \tag{5.48}$$

Even when the state $\hat{\sigma}_S$ of the L pulse train is unknown, an upper bound on $r_{\rm tag}$ can be determined from an off-line coincidence measurement on the light source using a few detectors. As shown in Appendix D, the calibration method reveals an upper bound that is close to the true value of $r_{\rm tag}$, as long as the state from the source is close to a coherent state with its mean photon number $\mu \ll L^{-1/2}$.

For long distance communication, the DQPS protocol can be improved by using decoy-state method, in which intensities of L pulses are randomly changed block by block. However, it is less effective as L gets larger. This is because only the statistics of the total number of photons emitted in the L pulses are obtained and no further information on their distribution over the L pulses is available. As a result, the improvement is limited to the events where a single photon has been emitted in the L pulses. Thus, for long distance communication, a secret key is extracted only from such single-photon events. When Alice uses a laser source, the maximum probability that a single photon is contained in L pulses is $1/e$ regardless of L. Bob's detection has a loss of $1/L$ due to detection at invalid timings in Fig. 5.1. Therefore, the efficiency of key generation per pulse is $\propto (L-1)/L^2$, which shows that the key rates of $L > 2$ is smaller than that of $L = 2$ in the limit of long distance.

On the other hand, for short distance communication, the DQPS protocol is expected to compensate for several disadvantages of the decoy-state BB84 protocol mentioned in Sec. 4.3.2. First, the decoy-state BB84 protocol uses the knowledge on the probability of higher photon numbers from the light source, which will require complicated devices for calibration while the DQPS protocol requires as simple devices as the BB84 protocol. Second, the decoy-state BB84 protocol relies on an involved parameter estimation, which leads to a large overhead from the finite-key

size effect. In comparison, the simplicity of the key rate formula (5.47) of the DQPS protocol suggests a small overhead from the finite-key size effect, which is actually confirmed in Chapter 6. From the above insights, the DQPS protocol is expected to be useful for the practical cases where one prefers a simple setup or short time operation for short distance communication.

Another possible improvement of our result may be obtained from the expected robustness of general DPS protocols against PNS attacks. As is seen in Sec. 4.4.2, in the DPS protocols (including the DQPS protocol), Eve's attempts to control the timing of detection j tends to violate the coherence chain and increase the probability of a bit error, which is expected to result in the robustness against PNS attacks. While the robustness can be seen as a $\eta^{\frac{3}{2}}$-dependence of the key rate in a security proof of the DPS protocol [90], our key rate of the DQPS protocol scales as η^2. This is because our proof assumed the pessimistic assumption that Eve is able to control the value of j without causing any bit error. If we analyze the security based on the proof technique for the DPS protocol [90], our protocol may benefit from the robustness against PNS attacks without using decoy states.

As a conclusion, we have proved the security of differential quadrature phase shift (DQPS) quantum key distribution protocol, which can be implemented with almost the same setup as the phase-encoding (PE) BB84 protocol. The proof is based on the a careful adaptation of the tagging idea and the complementarity argument. We found that the key generation rate exceeds that of the PE-BB84 protocol for any channel transmission, and is 8/3 as high as the rate of the PE-BB84 protocol in the limit of small transmission.

Chapter 6

Simple method of finite-key analysis for WCP-QKD

In contrast to the asymptotic analysis conducted in Chapter 5, security analysis of QKD should take into account statistical fluctuations due to the finite size of communication data, which requires so-called "finite-key analysis". Although the secure key generation rate of the DQPS protocol was higher than that of the PE-BB84 protocol in the asymptotic analysis, it is not obvious whether the advantage is still retained in the finite-key regime since the security proof of the DQPS protocol is not as straightforward as that of the BB84 protocol. This motivates us to conduct finite-key analysis for the DQPS protocol. Interestingly, on the way to address this problem, we discovered a new method for finite-key analysis which is suitable not only for the DQPS protocol but also for other QKD protocols using WCP, enabling a smaller number of estimated parameters. The method is based on Bernoulli sampling, which is related to binomial distribution, in contrast to the currently used method based on the simple random sampling, which is associated with hypergeometric distribution. For WCP-BB84 protocol, a higher key generation rate is obtained with the proposed method compared to the conventional method with simple random sampling. Furthermore, the required number of detected signals to generate a secret key reduces drastically from the previous works. By applying the proposed method to the DQPS protocol, we show that the advantage of the DQPS protocol over the PE-BB84 protocol still remains in the finite key regime.

This chapter is organized as follows. In Sec. 6.1, we briefly introduce basic ideas in the sampling problem which are necessary for finite-key analysis, simple random sampling and Bernoulli sampling, and also mention related works. In Sec. 6.2, we propose a method of finite-key analysis based on Bernoulli sampling, and applies it to the ideal BB84 protocol where Alice and Bob can manipulate perfect single-photon states. The proposed method is then applied to the BB84

protocol with WCP as well as the DQPS protocol in Sec. 6.3. Finally, we give discussion and conclusion in Sec. 6.4. The results of this chapter complete the security proof for the BB84 protocol in Sec. 3.3 and Sec. 4.2.2 by explicitly determining the bounds on the numbers of phase errors and untagged rounds.

6.1 Sampling problem in finite-key analysis

The statistical fluctuations in the finite-key analysis appear in the estimation of the number of phase errors and the estimation of the number of untagged incidents, for example. To obtain concise analysis and also to avoid the effect of unnecessary fluctuations, a simple method with a smaller number of estimation processes is preferred. Although several proofs [17, 113, 114] use Azuma's inequality [25] to treat specific protocols, a number of recent finite-key analyses [13, 15, 16, 24, 76] are based on the method with simple random sampling, which is used to model n_1 draws, without replacement, from a finite population of size n_2 that contains k_2 errors. The probability that the number of errors in the sample is k_1 obeys hypergeometric distribution

$$\mathrm{HG}(k_1; n_1, k_2, n_2) := \frac{\binom{k_2}{k_1}\binom{n_2-k_2}{n_1-k_1}}{\binom{n_2}{n_1}}. \tag{6.1}$$

In several finite-key analyses [24, 76] based on simple random sampling, efforts were made to find bounds on hypergeometric distribution which are related to binomial distribution in order to simplify numerical calculation.

In order to mitigate the inefficiency arising from basis mismatch between the sender and the receiver, the BB84 protocol is often implemented with biased basis choice [115], in which the minor basis is used solely for monitoring leaked information in the major basis. The BB84 protocols and the DQPS protocol we have investigated in Chaps. 3-5 include such a bias in the form of the basis choice probabilities $\tilde{p}_Z$ and $\tilde{p}_X$ (or $\tilde{p}_0$ and $\tilde{p}_1$). In such cases, the whole data from the rounds in the monitoring basis is regarded as a sample, with each round selected with a constant probability dictated in the protocol as that of the basis choice. This suggests that the data from the monitoring basis is related to Bernoulli sampling, in which each element of the population of size n_2 is sampled with fixed probability $\tilde{p}_1$. The number of samples n_1 obeys binomial distribution

$$\mathrm{BI}(n_1; n_2, \tilde{p}_1) := \binom{n_2}{n_1} \tilde{p}_1^{n_1} (1-\tilde{p}_1)^{n_2-n_1}. \tag{6.2}$$

If the BB84 protocol with biased basis choice essentially includes the property of the binomial distribution, analysis based on the conventional simple random sampling may introduce unneces-

sary complexity and possibly leads to a lower key rate. This is the intuitive advantage expected in using the Bernoulli sampling for finite-key analysis, which is certified in the following chapters.

6.2 Analysis for the ideal BB84 protocol

Here we consider finite-key analysis for the ideal BB84 protocol. The protocol follows the description in Sec. 2.2.3 and assumptions in Sec. 3.3. For convenience, we define several variables and parameters as

$$n_{\rm tot} := n_Z + n_X, \tag{6.3}$$

and

$$\begin{aligned} p_Z :=& \frac{\tilde{p}_Z^2}{\tilde{p}_Z^2 + \tilde{p}_X^2}, \\ p_X :=& \frac{\tilde{p}_X^2}{\tilde{p}_Z^2 + \tilde{p}_X^2}. \end{aligned} \tag{6.4}$$

6.2.1 Formalism for key length

We show a formalism for key length in terms of phase errors by using the result of 3.3. From Sec. 3.2.2, a phase error is defined as a bit error which occurs when Alice and Bob conduct virtual X-basis measurement on a Z-labeled round after Step (7') in Sec. 3.3.1. An important property which will be used in the next subsection is that the measurement for a phase error on a Z-labeled round and the measurement for a bit error on an X-labeled round are identical, and hence they only differs in the labeling.

Let $k_{\rm ph}$ be a random variable which represents the number of phase errors on n_Z Z-labeled rounds. Once we have a good upper bound on $k_{\rm ph}$, a secure key length can be calculated as follows. Suppose that we have a function $f(k_X, n_X, n_{\rm tot})$ which satisfies

$$\Pr(k_{\rm ph} > f(k_X, n_X, n_{\rm tot})) \leq \epsilon_{\rm PE} \tag{6.5}$$

regardless of Eve's attack strategy. From the theorem in Sec. 3.3.2, by setting

$$\epsilon_{\rm s} = \sqrt{2}\sqrt{\epsilon_{\rm PE} + \epsilon_{\rm PA}}, \tag{6.6}$$

the protocol is $\epsilon_{\rm c}$-correct and $\epsilon_{\rm s}$-secret if the final key length $l_{\rm fin}$ satisfies

$$l_{\rm fin} \leq n_Z(1 - h\left(\frac{f(k_X, n_X, n_{\rm tot})}{n_Z}\right)) - \log_2 \frac{2}{\epsilon_{\rm PA}} - \lambda_{\rm EC}(\epsilon_{\rm c}), \tag{6.7}$$

where $\lambda_{\rm EC}(\epsilon_{\rm c})$ is the cost of error correction to achieve $\epsilon_{\rm c}$-correctness.

6.2.2 Bounds on phase errors

In this subsection, we discuss the specific methods to obtain $f(k_X, n_X, n_{\rm tot})$ in Eq. (6.5) including a method based on the Bernoulli sampling, and a more conventional method based on the simple random sampling. We also introduce a third, rather convoluted method, which will help to elucidate the difference between the former two methods.

Before discussing each of the methods, we first derive general statistical properties. Since the Z-labeled phase error and the X-labeled bit error are obtained by identical measurements, the procedure to obtain those errors is equivalent to the following steps after Step (5') in Sec. 3.3.1: (a) Alice and Bob further discard each of the remaining rounds with probability $1 - \tilde{p}_Z^2 - \tilde{p}_X^2$. (b) They make X-basis measurements on the remaining $n_{\rm tot}$ rounds and obtain $k_{\rm tot}$ errors. (c) Finally, they label each of the $n_{\rm tot}$ rounds as Z or X with probability p_Z and p_X (see Eq. (6.4)), respectively, and obtain $k_{\rm ph}$ phase errors in Z-labeled rounds and $k_X = k_{\rm tot} - k_{\rm ph}$ bit errors in X-labeled rounds[*1)]. In this procedure, since k_X errors are sampled from $k_{\rm tot}$ errors with a fixed probability p_X, it follows a binomial distribution if $k_{\rm tot}$ and $n_{\rm tot}$ are fixed:

$$\Pr(k_X \mid k_{\rm tot}, n_{\rm tot}) = {\rm BI}(k_X; k_{\rm tot}, p_X). \tag{6.8}$$

On the other hand, the step (c) of the above procedure is equivalently denoted as follows: Alice and Bob draw a number n_X based on the binomial distribution ${\rm BI}(n_X; n_{\rm tot}, p_X)$, and then select n_X random rounds among the $n_{\rm tot}$ rounds to label as X, thereby determining k_X. This implies that the number k_X obeys hypergeometric distribution if n_X, $k_{\rm tot}$ and $n_{\rm tot}$ are fixed:

$$\Pr(k_X \mid n_X, k_{\rm tot}, n_{\rm tot}) = {\rm HG}(k_X; n_X, k_{\rm tot}, n_{\rm tot}). \tag{6.9}$$

In order to use the properties derived above, it is convenient to reformulate Eq. (6.5) as follows. From Eq. (6.5), we have

$$\sum_{k_{\rm tot}, n_{\rm tot}} \Pr(k_{\rm ph} > f(k_X, n_X, n_{\rm tot}) \mid k_{\rm tot}, n_{\rm tot}) \Pr(k_{\rm tot}, n_{\rm tot}) \le \epsilon_{\rm PE}. \tag{6.10}$$

Since $\Pr(k_{\rm tot}, n_{\rm tot})$ can be under control of Eve, we seek for $f(k_X, n_X, n_{\rm tot})$ satisfying

$$\Pr(k_{\rm ph} > f(k_X, n_X, n_{\rm tot}) \mid k_{\rm tot}, n_{\rm tot}) \le \epsilon_{\rm PE} \tag{6.11}$$

for any $k_{\rm tot}$ and $n_{\rm tot}$, which is a sufficient condition for Eq. (6.5). For later convenience, we equivalently describe Eq. (6.11) as

$$\sum_{k_X, n_X; k_X < k_{\rm tot} - f(k_X, n_X, n_{\rm tot})} \Pr(k_X, n_X \mid k_{\rm tot}, n_{\rm tot}) \le \epsilon_{\rm PE}. \tag{6.12}$$

[*1)] If one uses sampled bits on Z-labeled rounds to determine the cost for error correction (see Actual protocol in Sec. 3.3.1), it should be done as a Bernoulli sampling with a probability ξ. Since these sampled bits are discarded, the probabilities p_Z and p_X defined in Eq. (6.4) should be modified as $p_Z = \frac{\tilde{p}_Z^2(1-\xi)}{\tilde{p}_Z^2(1-\xi)+\tilde{p}_X^2}$ and $p_X = \frac{\tilde{p}_X^2}{\tilde{p}_Z^2+\tilde{p}_X^2}$, respectively.

The first method to determine $f(k_X, n_X, n_{\rm tot})$, whose utility we will emphasize throughout this chapter, is based on Bernoulli sampling using the property of binomial distribution Eq. (6.8). This method adopts $f(k_X, n_X, n_{\rm tot}) = f_{\rm BI}(k_X)$ where

$$f_{\rm BI}(k_X) := \min\left\{k_{\rm tot}\middle| C_{\rm BI}(k_X; k_{\rm tot}, p_X) \le \epsilon_{\rm PE}\right\} - k_X - 1 \tag{6.13}$$

$$C_{\rm BI}(k_X; k_{\rm tot}, p_X) := \sum_{k'_X \le k_X} {\rm BI}(k'_X; k_{\rm tot}, p_X). \tag{6.14}$$

The proof that $f_{\rm BI}(k_X)$ satisfies Eq. (6.11) is as follows. Define $\bar{k}_X(k_{\rm tot}) := \max\{k_X \mid k_{\rm tot} > f_{\rm BI}(k_X) + k_X\}$. Then we have

$$\sum_{k_X;\ k_{\rm tot} > f_{\rm BI}(k_X)+k_X} {\rm BI}(k_X; k_{\rm tot}, p_X) \le C_{\rm BI}(\bar{k}_X(k_{\rm tot}); k_{\rm tot}, p_X). \tag{6.15}$$

Since $C_{\rm BI}(k_X; k_{\rm tot}, p_X)$ is a decreasing function of $k_{\rm tot}$, from Eq. (6.13) we have $C_{\rm BI}(k_X; k_{\rm tot}, p_X) \le \epsilon_{\rm PE}$ for any pair $(k_X, k_{\rm tot})$ satisfying $k_{\rm tot} \ge f_{\rm BI}(k_X)+k_X+1$. Since $k_{\rm tot} \ge f_{\rm BI}(\bar{k}_X(k_{\rm tot}))+\bar{k}_X(k_{\rm tot})+1$ holds by definition of $\bar{k}_X(k_{\rm tot})$, we have $C_{\rm BI}(\bar{k}_X(k_{\rm tot}); k_{\rm tot}, p_X) \le \epsilon_{\rm PE}$. By connecting this to Eq. (6.15), we have

$$\sum_{k_X;\ k_X < k_{\rm tot} - f_{\rm BI}(k_X)} {\rm BI}(k_X; k_{\rm tot}, p_X) \le \epsilon_{\rm PE} \tag{6.16}$$

for any $k_{\rm tot}$. From Eqs. (6.8) and (6.16), we have

$$\begin{aligned} &\sum_{k_X, n_X;\ k_X < k_{\rm tot} - f_{\rm BI}(k_X)} \Pr(k_X, n_X \mid k_{\rm tot}, n_{\rm tot}) \\ &= \sum_{k_X;\ k_X < k_{\rm tot} - f_{\rm BI}(k_X)} \Pr(k_X \mid k_{\rm tot}, n_{\rm tot}) \\ &\le \epsilon_{\rm PE}, \end{aligned} \tag{6.17}$$

which is identical to Eq. (6.12) with $f(k_X, n_X, n_{\rm tot}) = f_{\rm BI}(k_X)$. Therefore, we have

$$\Pr(k_{\rm ph} > f_{\rm BI}(k_X) \mid k_{\rm tot}, n_{\rm tot}) \le \epsilon_{\rm PE}. \tag{6.18}$$

As a result of the Bernoulli-sampling method, the protocol is $\epsilon_{\rm c}$-correct and $\epsilon_{\rm s}$-secret if the final key length $l_{\rm fin}$ satisfies

$$l_{\rm fin} \le l^{\rm (BI)} := n_Z\left(1 - h\left(\frac{f_{\rm BI}(k_X)}{n_Z}\right)\right) - \log_2 \frac{2}{\epsilon_{\rm PA}} - \lambda_{\rm EC}(\epsilon_{\rm c}), \tag{6.19}$$

where $\epsilon_{\rm s}$ is given by Eq. (6.6).

The second method is based on simple random sampling, applying the property of the hypergeometric distribution Eq. (6.9), which is already seen in Ref. [13, 15, 16, 24], for example. This method adopts $f(k_X, n_X, n_{\rm tot}) = f_{\rm HG}(k_X, n_X, n_{\rm tot})$ where

$$\begin{aligned} f_{\rm HG}(k_X, n_X, n_{\rm tot}) &:= \min\left\{ k_{\rm tot} \middle| C_{\rm HG}(k_X; n_X, k_{\rm tot}, n_{\rm tot}) \le \epsilon_{\rm PE} \right\} - k_X - 1 \\ C_{\rm HG}(k_X; n_X, k_{\rm tot}, n_{\rm tot}) &:= \sum_{k'_X \le k_X} {\rm HG}(k'_X; n_X, k_{\rm tot}, n_{\rm tot}). \end{aligned} \tag{6.20}$$

The proof that $f_{\rm HG}(k_X, n_X, n_{\rm tot})$ satisfies Eq. (6.11) is similar to the proof for $f_{\rm BI}(k_X)$. Recall that the proof for $f_{\rm BI}(k_X)$ did not use the explicit form of ${\rm BI}(k'_X, k_{\rm tot}, p_X)$ but only used the decreasing property of $C_{\rm BI}(k_X; k_{\rm tot}, p_X)$ as a function of $k_{\rm tot}$. Since $C_{\rm HG}(k_X; n_X, k_{\rm tot}, n_{\rm tot})$ is also a decreasing function of $k_{\rm tot}$, we have

$$\sum_{k_X;\ k_X < k_{\rm tot} - f_{\rm HG}(k_X, n_X, n_{\rm tot})} {\rm HG}(k_X; n_X, k_{\rm tot}, n_{\rm tot}) \le \epsilon_{\rm PE} \tag{6.21}$$

for any n_X, $k_{\rm tot}$ and $n_{\rm tot}$, which is analogous to Eq. (6.16). From Eqs. (6.9) and (6.21), we have

$$\begin{aligned} &\sum_{k_X, n_X;\ k_X < k_{\rm tot} - f_{\rm HG}(k_X, n_X, n_{\rm tot})} \Pr(k_X, n_X \mid k_{\rm tot}, n_{\rm tot}) \\ &= \sum_{k_X, n_X;\ k_X < k_{\rm tot} - f_{\rm HG}(k_X, n_X, n_{\rm tot})} \Pr(k_X \mid n_X, k_{\rm tot}, n_{\rm tot}) \Pr(n_X \mid k_{\rm tot}, n_{\rm tot}) \\ &\le \epsilon_{\rm PE}, \end{aligned} \tag{6.22}$$

which is identical to Eq. (6.12) with $f(k_X, n_X, n_{\rm tot}) = f_{\rm HG}(k_X, n_X, n_{\rm tot})$. Therefore, we have

$$\Pr(k_{\rm ph} > f_{\rm HG}(k_X, n_X, n_{\rm tot}) \mid k_{\rm tot}, n_{\rm tot}) \le \epsilon_{\rm PE}. \tag{6.23}$$

As a result of the method with simple random sampling, the protocol is $\epsilon_{\rm c}$-correct and $\epsilon_{\rm s}$-secret if the secret key length $l_{\rm fin}$ satisfies

$$l_{\rm fin} \le l^{\rm (HG)} := n_Z \left(1 - h\left(\frac{f_{\rm HG}(k_X, n_X, n_{\rm tot})}{n_Z}\right)\right) - \log_2 \frac{2}{\epsilon_{\rm PA}} - \lambda_{\rm EC}(\epsilon_{\rm c}) \tag{6.24}$$

where $\epsilon_{\rm s}$ is given by Eq. (6.6).

To understand the relation between the two methods with Bernoulli sampling and simple random sampling, we introduce another method which uses full knowledge of the distribution $\Pr(k_X, n_X \mid k_{\rm tot}, n_{\rm tot})$ appearing in Eq. (6.12). The argument before Eq. (6.8) also implies that the number $m_X := n_X - k_X$ of X-labeled rounds without bit error obeys binomial distribution ${\rm BI}(m_X; n_{\rm tot} - k_{\rm tot}, p_X)$, and that m_X and k_X are independent conditioned on $k_{\rm tot}$ and $n_{\rm tot}$. We thus obtain

$$\Pr(k_X, n_X \mid k_{\rm tot}, n_{\rm tot}) = {\rm BI}(k_X; k_{\rm tot}, p_X) {\rm BI}(n_X - k_X; n_{\rm tot} - k_{\rm tot}, p_X). \tag{6.25}$$

The argument leading to Eq. (6.9) gives another expression for the distribution as

$$\Pr(k_X, n_X \mid k_{\rm tot}, n_{\rm tot}) = {\rm HG}(k_X; n_X, k_{\rm tot}, n_{\rm tot}){\rm BI}(n_X; n_{\rm tot}, p_X). \tag{6.26}$$

As a result, Eq. (6.12) is expressed in the following two equivalent ways:

$$\sum_{k_X, m_X; k_X < k_{\rm tot} - f(k_X, k_X + m_X, n_{\rm tot})} {\rm BI}(k_X; k_{\rm tot}, p_X){\rm BI}(m_X; n_{\rm tot} - k_{\rm tot}, p_X) \le \epsilon_{\rm PE}. \tag{6.27}$$

or

$$\sum_{k_X, n_X; k_X < k_{\rm tot} - f(k_X, n_X, n_{\rm tot})} {\rm HG}(k_X; n_X, k_{\rm tot}, n_{\rm tot}){\rm BI}(n_X; n_{\rm tot}, p_X) \le \epsilon_{\rm PE}. \tag{6.28}$$

Since $f_{\rm BI}(k_X)$ satisfies Eq. (6.16), Eq. (6.27) holds if $f(k_X, k_X + m_X, n_{\rm tot}) = f_{\rm BI}(k_X)$. Similarly, since $f_{\rm HG}(k_X, n_X, n_{\rm tot})$ satisfies Eq. (6.21), Eq. (6.28) holds if $f(k_X, n_X, n_{\rm tot}) = f_{\rm HG}(k_X, n_X, n_{\rm tot})$. On the other hand, the condition of Eqs. (6.27) and (6.28) do not imply Eq. (6.16) or Eq. (6.21). Therefore, there could be a better bound compared to $f_{\rm BI}(k_X)$ and $f_{\rm HG}(k_X, n_X, n_{\rm tot})$ based on Eq. (6.27) or Eq. (6.28). In general, it is very complicated to determine the optimal function $f(k_X, n_X, n_{\rm tot})$ for the final key length $l_{\rm fin}$, since it will depend on the explicit functional dependence of $l_{\rm fin}$ on $f(k_X, n_X, n_{\rm tot})$.

The difference between the two equivalent conditions Eqs. (6.27) and (6.28) is the choice of two variables from three no-independent random variables k_X, n_X and m_X. When (k_X, n_X) are chosen in Eq. (6.28), the distribution of k_X, ${\rm HG}(k_X; n_X, k_{\rm tot}, n_{\rm tot})$ is dependent on the value of n_X. On the other hand, Eq. (6.27) implies that two variables (k_X, m_X) are independent of each other. This suggests that the underlying statistics in the BB84 protocol with biased basis choice are understood in terms of independent binomial distributions.

Let us mention the difference from the other works [24, 76] which deal with relations between bounds on binomial distribution and ones on hypergeometric distribution since the former are easily treated with existing mathematical packages. Ref. [24] uses the property, which dates back to Hoeffding [116], that expectation of a convex function over hypergeometric distribution is no larger than that over binomial distribution. In [76], Ahrens map [117] was used to show that hypergeometric distribution is bounded by a permutated binomial distribution within a factor of $\sqrt{2}$. In contrast to these works, in our case the probability distribution Eq. (6.8) reflects the binomial distribution inherent in the BB84 protocol with biased basis choice.

6.2.3 Numerical examples

Here we numerically compare the final key lengths derived from the three methods in the last subsection in the simplest cases. We calculate the key lengths for the case where no error is

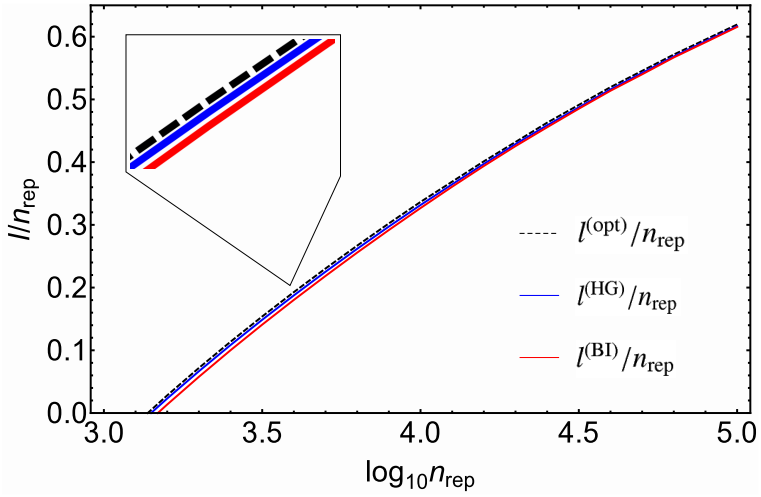

Figure 6.1: Secure key ratio of the qubit-based BB84 protocol to the asymptotic limit as a function of total rounds of the protocol $n_{\rm rep}$. We assume no errors ($k_X = 0$) and no loss ($n_{\rm tot} = n_{\rm rep}$). The security parameters are set to $\epsilon_{\rm c} = 10^{-15}$ and $\epsilon_{\rm s} = 10^{-10}$. The top, middle and bottom curves represent the ratios $l^{(\rm opt)}/n_{\rm rep}$, $l^{(\rm HG)}/n_{\rm rep}$ (method with simple random sampling) and $l^{(\rm BI)}/n_{\rm rep}$ (Bernoulli-sampling method), respectively. In the limit of $n_{\rm rep} \to \infty$, each curve converges to $l/n_{\rm rep} = 1$.

observed ($k_X = 0$) and every signal is detected ($n_{\rm tot} = n_{\rm rep}$). The cost of error correction is set to $\lambda_{\rm EC}(\epsilon_{\rm c}) = \log_2(1/\epsilon_{\rm c})$. We also assume $n_Z = n_{\rm rep}\tilde{p}_Z^2$ and $n_X = n_{\rm rep}\tilde{p}_X^2$.

If we do not care about the key length for $k_X > 0$, the optimal choice of $f(k_X, n_X, n_{\rm tot})$ satisfying Eq. (6.28) (or Eq. (6.27)) is given by $f(k_X, n_X, n_{\rm tot}) = n_{\rm tot} - n_X$ for $k_X \geq 1$ and $f(0, n_X, n_{\rm tot}) = f_{\rm opt}^{(k_X=0)}(n_X, n_{\rm tot})$ with

$$f_{\rm opt}^{(k_X=0)}(n_X, n_{\rm tot}) := \min\left\{k_{\rm tot}\middle| G(n_X; k_{\rm tot}, n_{\rm tot}) \leq \epsilon_{\rm PE}\right\} - 1$$
$$G(n_X; k_{\rm tot}, n_{\rm tot}) := \sum_{n_X \leq n'_X \leq n_{\rm tot} - k_{\rm tot}} {\rm HG}(0; n'_X, k_{\rm tot}, n_{\rm tot}){\rm BI}(n'_X; n_{\rm tot}, p_X). \tag{6.29}$$

The proof is analogous to the one for $f_{\rm BI}(k_X)$ or $f_{\rm HG}(k_X, n_X, n_{\rm tot})$. Since $G(n_X; k_{\rm tot}, n_{\rm tot})$ is a decreasing function of $k_{\rm tot}$, by using an argument similar to the one leading to Eq. (6.16), we have

$$\sum_{n_X;\ k_{\rm tot} > f_{\rm opt}^{(k_X=0)}(n_X, n_{\rm tot})} {\rm HG}(0; n_X, k_{\rm tot}, n_{\rm tot}){\rm BI}(n_X; n_{\rm tot}, p_X) \leq \epsilon_{\rm PE}. \tag{6.30}$$

This is identical to Eq. (6.28) since $k_X < k_{\rm tot} - f(k_X, n_X, n_{\rm tot})$ is never satisfied for $k_X \geq 1$. The key length when $k_X = 0$ was observed is then given by

$$l^{(\rm opt)} := n_Z\left(1 - h\left(\frac{f_{\rm opt}^{(k_X=0)}(n_X, n_{\rm tot})}{n_Z}\right)\right) - \log_2\frac{2}{\epsilon_{\rm PA}} - \lambda_{\rm EC}(\epsilon_{\rm c}). \tag{6.31}$$

In Fig. 6.1, we show the secure key ratios to the asymptotic case $l^{(\mathrm{BI})}/n_{\mathrm{rep}}$, $l^{(\mathrm{HG})}/n_{\mathrm{rep}}$ and $l^{(\mathrm{opt})}/n_{\mathrm{rep}}$ as functions of total rounds of the protocol n_{rep}. For each n_{rep}, the value of $\tilde{p}_X$ was optimized to maximize the key length. In the limit of $n_{\mathrm{rep}} \to \infty$, each curve converges to $l/n_{\mathrm{rep}} = 1$. The security parameters are set to $\epsilon_{\mathrm{c}} = 10^{-15}$ and $\epsilon_{\mathrm{s}} = 10^{-10}$, $\epsilon_{\mathrm{PE}} = 1/4 \times 10^{-20}$ and $\epsilon_{\mathrm{PA}} = 1/4 \times 10^{-20}$. We see that although the key rate $l^{(\mathrm{opt})}$ is the best, the three methods achieve almost the same key length.

6.3 Analysis for WCP-based protocol

Here, we apply the analyses introduced in the previous section to the protocols using WCP. We consider the WCP-based BB84 protocol in the subsections 6.3.1 and 6.3.2, and move to the DQPS protocol in subsection 6.3.3.

6.3.1 The WCP-BB84 protocol

The WCP-BB84 protocol follows the procedures described in Sec. 2.2.3 and assumptions in Sec. 4.2.2. Here, we prove the security of the WCP-BB84 protocol using the theorem in Sec. 4.2.2. From Sec. 3.2.2, a phase error in a Z-labeled round was defined as an error occurring when Alice makes an ideal X-basis measurement on the system A and Bob makes the actual X-basis measurement on the system S (the measurement conducted on X-labeled rounds in the actual protocol). Let $k_{\mathrm{ph,unt}}$ be the total number of phase errors on the untagged Z-labeled rounds. Suppose that an upper bound of $k_{\mathrm{ph,unt}}$ is given as a function of k_X, n_X, n_{tot} and $n_{Z,\mathrm{unt}}$:

$$\Pr(k_{\mathrm{ph,unt}} > f(k_X, n_X, n_{\mathrm{tot}}, n_{Z,\mathrm{unt}})) \leq \epsilon_{\mathrm{PE}}, \tag{6.32}$$

where $n_{Z,\mathrm{unt}}$ is the number of untagged and Z-labeled round defined in Sec. 4.2.2. We also suppose that there is a probabilistic lower bound $\underline{n}_{Z,\mathrm{unt}}$ which satisfies

$$\Pr(n_{Z,\mathrm{unt}} < \underline{n}_{Z,\mathrm{unt}}) \leq \epsilon_{Z,\mathrm{unt}}. \tag{6.33}$$

According to the theorem in Sec. 4.2.2, by setting

$$\epsilon_{\mathrm{s}} = \sqrt{2}\sqrt{\epsilon_{\mathrm{PE}} + \epsilon_{\mathrm{PA}}} + \epsilon_{Z,\mathrm{unt}}, \tag{6.34}$$

the protocol is ϵ_{c}-correct and ϵ_{s}-secret if

$$l_{\mathrm{fin}} \leq \min_{n_{Z,\mathrm{unt}} \geq \underline{n}_{Z,\mathrm{unt}}} \left\{ n_{Z,\mathrm{unt}}\left(1 - h\left(\frac{f(k_X, n_X, n_{\mathrm{tot}}, n_{Z,\mathrm{unt}})}{n_{Z,\mathrm{unt}}}\right)\right) \right\} - \log_2 \frac{2}{\epsilon_{\mathrm{PA}}} - \lambda_{\mathrm{EC}}(\epsilon_{\mathrm{c}}) \tag{6.35}$$

is satisfied.

Under the assumptions for the source and measurement apparatus, the basic distributions used in the previous section, Eqs. (6.8) and (6.9), are still valid if we confine ourselves to the untagged rounds. Although the fact may be intuitively obvious for the WCP-BB84 protocol by seeing the equivalent protocol in Sec. 4.2.2, here we give its mathematical justification since it helps when we treat the DQPS protocol in Sec. 6.3.3. We define a set of integers labeling the rounds in the protocol as $\mathcal{N}_{\rm rep} := \{1, 2, ...n_{\rm rep}\}$. As subsets of $\mathcal{N}_{\rm rep}$, let us define the set of the integers labeling the rounds where Alice (Bob) chooses X basis as $\mathcal{X}_A$ ($\mathcal{X}_B$) regardless of detection. Define those labeling the untagged and detected rounds as $\mathcal{N}_{\rm unt}$. Let $\mathcal{K}_{\rm unt}$ be a subset of $\mathcal{N}_{\rm unt}$ labeling the rounds which have errors when Alice and Bob conduct virtual X-basis measurements regardless of their basis choice. For any subset $\mathcal{M}$, let $\overline{\mathcal{M}} := \mathcal{N}_{\rm rep} \setminus \mathcal{M}$. With these notations,

$$\begin{aligned} k_{\rm ph,unt} &= |\overline{\mathcal{X}_A} \cap \overline{\mathcal{X}_B} \cap \mathcal{K}_{\rm unt}|, \\ n_{\rm Z,unt} &= |\overline{\mathcal{X}_A} \cap \overline{\mathcal{X}_B} \cap \mathcal{N}_{\rm unt}|. \end{aligned} \tag{6.36}$$

We define other random variables as follows:

$$\begin{aligned} k_{X,\rm unt} &:= |\mathcal{X}_A \cap \mathcal{X}_B \cap \mathcal{K}_{\rm unt}|, \\ n_{X,\rm unt} &:= |\mathcal{X}_A \cap \mathcal{X}_B \cap \mathcal{N}_{\rm unt}|, \\ k_{\rm tot,unt} &:= k_{X,\rm unt} + k_{\rm ph,unt}, \\ n_{\rm tot,unt} &:= n_{X,\rm unt} + n_{Z,\rm unt}. \end{aligned} \tag{6.37}$$

Since bases are selected at Step (6') in the protocol in Sec. 4.2.2, at which $\mathcal{N}_{\rm unt}$ and $\mathcal{K}_{\rm unt}$ have already been determined, we have

$$\Pr(\mathcal{X}_A \cap \mathcal{N}_{\rm unt} = \mathcal{M}_A, \mathcal{X}_B \cap \mathcal{N}_{\rm unt} = \mathcal{M}_B \mid \mathcal{K}_{\rm unt}, \mathcal{N}_{\rm unt}) = \Theta(\mathcal{M}_A, \mathcal{N}_{\rm unt})\Theta(\mathcal{M}_B, \mathcal{N}_{\rm unt}) \tag{6.38}$$

for all $\mathcal{M}_A \subset \mathcal{N}_{\rm unt}$ and $\mathcal{M}_B \subset \mathcal{N}_{\rm unt}$, where we defined

$$\Theta(\mathcal{M}_1, \mathcal{M}_2) = \tilde{p}_X^{|\mathcal{M}_1|} \tilde{p}_Z^{|\mathcal{M}_2 \setminus \mathcal{M}_1|}. \tag{6.39}$$

By simple calculation of the probability theory, we have

$$\Pr(k_{X,\rm unt} \mid k_{\rm tot,unt}, n_{\rm tot,unt}) = \mathrm{BI}(k_{X,\rm unt}; k_{\rm tot,unt}, p_X) \tag{6.40}$$

and

$$\Pr(k_{X,\rm unt} \mid n_{X,\rm unt}, k_{\rm tot,unt}, n_{\rm tot,unt}) = \mathrm{HG}(k_{X,\rm unt}; n_{X,\rm unt}, k_{\rm tot,unt}, n_{\rm tot,unt}), \tag{6.41}$$

which means that Eqs. (6.8) and (6.9) essentially hold true for the untagged rounds.

Now we derive a key rate formula for the WCP-BB84 protocol based on Eq. (6.40), as was done with the Bernoulli-sampling method for the ideal protocol in Sec. 6.2.2. First, we seek for $f(k_X, n_X, n_{\mathrm{tot}}, n_{Z,\mathrm{unt}})$ which satisfies Eq. (6.32). Analogous to the derivation of Eq. (6.18) from Eq. (6.8), Eq. (6.40) leads to

$$\Pr(k_{\mathrm{ph,unt}} > f_{\mathrm{BI}}(k_{X,\mathrm{unt}}) \mid k_{\mathrm{tot,unt}}, n_{\mathrm{tot,unt}}) \leq \epsilon_{\mathrm{PE}} \tag{6.42}$$

for any $k_{\mathrm{tot,unt}}$ and $n_{\mathrm{tot,unt}}$, and hence we have

$$\Pr(k_{\mathrm{ph,unt}} > f_{\mathrm{BI}}(k_{X,\mathrm{unt}})) \leq \epsilon_{\mathrm{PE}}. \tag{6.43}$$

Since $k_{X,\mathrm{unt}}$ is not an observed value, we use the obvious bound

$$k_{X,\mathrm{unt}} \leq k_X. \tag{6.44}$$

Using the inequality

$$\begin{aligned} & C_{\mathrm{BI}}(k_X + 1; k_{\mathrm{tot}} + 1, p_X) \\ &= C_{\mathrm{BI}}(k_X; k_{\mathrm{tot}}, p_X) + (1 - p_X)\mathrm{BI}(k_X + 1; k_{\mathrm{tot}}, p_X) \\ &\geq C_{\mathrm{BI}}(k_X; k_{\mathrm{tot}}, p_X) \end{aligned} \tag{6.45}$$

in Eq. (6.13), we have $f_{\mathrm{BI}}(k_X) \leq f_{\mathrm{BI}}(k_X + 1)$, implying that $f_{\mathrm{BI}}(k_X)$ is an increasing function. Hence, Eqs. (6.43) and (6.44) lead to

$$\Pr(k_{\mathrm{ph,unt}} > f_{\mathrm{BI}}(k_X)) \leq \epsilon_{\mathrm{PE}}, \tag{6.46}$$

which means that $f_{\mathrm{BI}}(k_X)$ fulfills Eq. (6.32).

Next, we determine $\underline{n}_{Z,\mathrm{unt}}$ which satisfies Eq. (6.33). To determine a lower bound of $n_{Z,\mathrm{unt}}$, we consider an upper bound of $n_{Z,\mathrm{tag}} := n_Z - n_{Z,\mathrm{unt}}$. Let $N_{Z,\mathrm{tag}}$ be the number of rounds where Alice chooses Z basis, Bob chooses Z basis and the light source emits a tagged signal (two photons or more). As those conditions are independent of each other as seen from Eq. (4.6), we have

$$\Pr(N_{Z,\mathrm{tag}}) = \mathrm{BI}(N_{Z,\mathrm{tag}}, n_{\mathrm{rep}}, r_{\mathrm{tag}}\tilde{p}_Z^2). \tag{6.47}$$

Since $n_{Z,\mathrm{tag}}$ is the number of detected rounds among the $N_{Z,\mathrm{tag}}$ rounds,

$$n_{Z,\mathrm{tag}} \leq N_{Z,\mathrm{tag}} \tag{6.48}$$

holds. Eqs. (6.47) and (6.48) lead to

$$\Pr(n_{Z,\mathrm{tag}} > n) \leq 1 - C_{\mathrm{BI}}(n; n_{\mathrm{rep}}, r_{\mathrm{tag}}\tilde{p}_Z^2) \tag{6.49}$$

for any n. Thus, we have

$$\Pr(n_{Z,\mathrm{tag}} > g(r_{\mathrm{tag}}\tilde{p}_Z^2, \epsilon_{Z,\mathrm{unt}})) \leq \epsilon_{Z,\mathrm{unt}}, \tag{6.50}$$

where

$$g(x,y) := \min\left\{n \middle| 1 - C_{\mathrm{BI}}(n; n_{\mathrm{rep}}, x) \leq y\right\}. \tag{6.51}$$

Let $\underline{n}_{Z,\mathrm{unt}}$ be

$$\underline{n}_{Z,\mathrm{unt}} := n_Z - g(r_{\mathrm{tag}}\tilde{p}_Z^2, \epsilon_{Z,\mathrm{unt}}). \tag{6.52}$$

By using $n_{Z,\mathrm{tag}} = n_Z - n_{Z,\mathrm{unt}}$, Eq. (6.50) leads to

$$\Pr(n_{Z,\mathrm{unt}} < \underline{n}_{Z,\mathrm{unt}}) \leq \epsilon_{Z,\mathrm{unt}}. \tag{6.53}$$

Combined with Eqs. (6.35), (6.46) and (6.53), the protocol is ϵ_{c}-correct and ϵ_{s}-secret if

$$l_{\mathrm{fin}} \leq l_{\mathrm{WCP}}^{(\mathrm{BI})} := \underline{n}_{Z,\mathrm{unt}}(1 - h\left(\frac{f_{\mathrm{BI}}(k_X)}{\underline{n}_{Z,\mathrm{unt}}}\right)) - \log_2\frac{2}{\epsilon_{\mathrm{PA}}} - \lambda_{\mathrm{EC}}(\epsilon_{\mathrm{c}}), \tag{6.54}$$

where ϵ_{s} is given by Eq. (6.34). Together with Eqs. (6.13), (6.14), (6.51) and (6.52), Eq. (6.54) constitutes the main result of Sec. 6.3.1.

For the purpose of comparison, here we also discuss what the key rate formula looks like if we start from Eq. (6.41), based on simple random sampling. As we have derived Eq. (6.23) from Eq. (6.9), Eq. (6.41) leads to

$$\Pr(k_{\mathrm{ph,unt}} > f_{\mathrm{HG}}(k_{X,\mathrm{unt}}, n_{X,\mathrm{unt}}, n_{\mathrm{tot,unt}}) \mid k_{\mathrm{tot,unt}}, n_{\mathrm{tot,unt}}) \leq \epsilon_{\mathrm{PE}}, \tag{6.55}$$

which, in turn, leads to

$$\Pr(k_{\mathrm{ph,unt}} > f_{\mathrm{HG}}(k_{X,\mathrm{unt}}, n_{X,\mathrm{unt}}, n_{\mathrm{tot,unt}})) \leq \epsilon_{\mathrm{PE}}. \tag{6.56}$$

Similarly to $f_{\mathrm{BI}}(k_X)$, we can prove that $f_{\mathrm{HG}}(k_X, n_X, n_{\mathrm{tot}})$ is an increasing function of k_X. Since $k_{X,\mathrm{unt}}$ is upper-bounded by Eq. (6.44), Eq. (6.56) leads to

$$\Pr(k_{\mathrm{ph,unt}} > f_{\mathrm{HG}}(k_X, n_{X,\mathrm{unt}}, n_{\mathrm{tot,unt}})) \leq \epsilon_{\mathrm{PE}}. \tag{6.57}$$

In contrast to Eq. (6.46), it requires an additional estimation process for $n_{X,\mathrm{unt}}$ to obtain $f_{\mathrm{HG}}(k_X, n_{X,\mathrm{unt}}, n_{\mathrm{tot,unt}})$. A lower bound defined by $\underline{n}_{X,\mathrm{unt}} := n_X - g(r_{\mathrm{tag}}\tilde{p}_X^2, \epsilon_{X,\mathrm{unt}})$ satisfies

$$\Pr(n_{X,\mathrm{unt}} < \underline{n}_{X,\mathrm{unt}}) \leq \epsilon_{X,\mathrm{unt}}. \tag{6.58}$$

Since $n_{X,\mathrm{unt}}$ is known in principle in the actual protocol (Step (6') in Sec. 4.2.2), the trace distance between the final state and the ideal state is written as a sum of the part for $n_{X,\mathrm{unt}} < \underline{n}_{X,\mathrm{unt}}$ and

the one for $n_{X,\mathrm{unt}} \geq \underline{n}_{X,\mathrm{unt}}$ as in Eq. (4.33). Hence, combined with Eqs. (6.35), (6.53), (6.57) and (6.58), by setting

$$\epsilon_{\mathrm{s}} = \sqrt{2}\sqrt{\epsilon_{\mathrm{PE}} + \epsilon_{\mathrm{PA}}} + \epsilon_{Z,\mathrm{unt}} + \epsilon_{X,\mathrm{unt}}, \tag{6.59}$$

the protocol is ϵ_{c}-correct and ϵ_{s}-secret if

$$\begin{aligned} l_{\mathrm{fin}} \leq\ & l_{\mathrm{WCP}}^{(\mathrm{HG})} := \min_{n_{Z,\mathrm{unt}} \geq \underline{n}_{Z,\mathrm{unt}}} \xi(k_X, \underline{n}_{X,\mathrm{unt}}, n_{Z,\mathrm{unt}}) \\ \xi(k_X, \underline{n}_{X,\mathrm{unt}}, n_{Z,\mathrm{unt}}) :=\ & \tilde{\xi}(k_X, \underline{n}_{X,\mathrm{unt}}, n_{Z,\mathrm{unt}}) - \log_2 \frac{2}{\epsilon_{\mathrm{PA}}} - \lambda_{\mathrm{EC}}(\epsilon_{\mathrm{c}}) \\ \tilde{\xi}(k_X, \underline{n}_{X,\mathrm{unt}}, n_{Z,\mathrm{unt}}) :=\ & n_{Z,\mathrm{unt}}\left(1 - h\left(\frac{f_{\mathrm{HG}}(k_X, \underline{n}_{X,\mathrm{unt}}, \underline{n}_{X,\mathrm{unt}} + n_{Z,\mathrm{unt}})}{n_{Z,\mathrm{unt}}}\right)\right). \end{aligned} \tag{6.60}$$

The reason that the minimization of $n_{Z,\mathrm{unt}}$ appears is because $\tilde{\xi}(k_X, \underline{n}_{X,\mathrm{unt}}, n_{Z,\mathrm{unt}})$ is not monotone-increasing function of $n_{Z,\mathrm{unt}}$. For example, with $\epsilon_{\mathrm{PE}} = 1/16 \times 10^{-20}$, we numerically confirmed that $\tilde{\xi}(0, 25000, 25318) \sim 24631$ and $\tilde{\xi}(0, 25000, 25319) \sim 24623$. This means that the protocol with final key length $l = \xi(k_X, \underline{n}_{X,\mathrm{unt}}, \underline{n}_{Z,\mathrm{unt}})$ is not necessarily secure.

As can be seen from the comparison between Eqs. (6.54) and (6.60), the method with simple random sampling is much more complicated than the Bernoulli-sampling method, involving an additional estimated parameter and a minimization. Moreover, as shown in Sec. 6.3.2, it tends to give a key rate lower than the Bernoulli-sampling method, probably because of the use of pessimistic bound on $n_{X,\mathrm{unt}}$.

6.3.2 Numerical examples

Here, we show two examples of numerical calculation for the WCP-BB84 protocol. We assume that the light source emits a pulse whose photon-number distribution is Poissonian with mean μ, namely, r_{tag} is given by Eq. (4.19). Like Fig. 6.1 for the ideal protocol, we first calculated the simplest case where no error is observed ($k_X = 0$) and no loss occurs ($n_{\mathrm{tot}} = n_{\mathrm{rep}}(1 - e^{-\mu})$), which is shown in Fig. 6.2. The cost of error correction was set to $\lambda_{\mathrm{EC}}(\epsilon_{\mathrm{c}}) = \log_2(1/\epsilon_{\mathrm{c}})$. We assumed $n_Z = n_{\mathrm{tot}}\tilde{p}_Z^2$ and $n_X = n_{\mathrm{tot}}\tilde{p}_X^2$. The values of $\tilde{p}_X$ and μ were optimized for each value of n_{rep}. For calculation of $l_{\mathrm{WCP}}^{(\mathrm{BI})}$, the security parameters were set to $\epsilon_{\mathrm{c}} = 10^{-15}$, $\epsilon_{\mathrm{s}} = 10^{-10}$, $\epsilon_{\mathrm{PE}} = 1/16 \times 10^{-20}$, $\epsilon_{\mathrm{PA}} = 1/16 \times 10^{-20}$ and $\epsilon_{Z,\mathrm{unt}} = 1/2 \times 10^{-10}$. The result is shown as the red curve in Fig. 6.2, where the key length Eq. (6.54) is normalized by the optimized asymptotic key rate of $1/e$ per signal at $\mu = 1$ and $\tilde{p}_X \to 0$. We see that a final key can be extracted when the total rounds n_{rep} is more than $\sim 10^{3.7}$ while the threshold is $n_{\mathrm{rep}} \sim 10^{3.2}$ for the ideal protocol using the same parameters (see also Fig. 6.1). For comparison, we also calculated the value of $\xi(k_X, \underline{n}_{X,\mathrm{unt}}, \underline{n}_{Z,\mathrm{unt}})/(n_{\mathrm{rep}}/e)$ under the same condition, which is shown as the blue curve in Fig. 6.2. The security parameters were the same as the red curve, except for $\epsilon_{Z,\mathrm{unt}} = \epsilon_{X,\mathrm{unt}} = 1/4 \times 10^{-10}$. The quantity $\xi(k_X, \underline{n}_{X,\mathrm{unt}}, \underline{n}_{Z,\mathrm{unt}})$

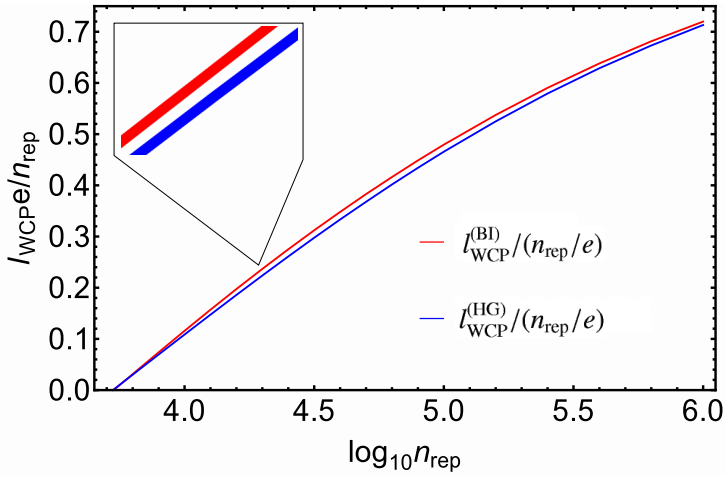

Figure 6.2: Comparison of estimation methods for the WCP-BB84 protocol. Upper curve (Bernoulli-sampling method): Secure key ratio to the asymptotic limit $l^{\rm (BI)}_{\rm WCP}/(n_{\rm rep}/e)$ as a function of total rounds of the protocol $n_{\rm rep}$. Lower curve (method with simple random sampling): An upper bound on the derived secure key ratio $l^{\rm (HG)}_{\rm WCP}/(n_{\rm rep}/e)$. We assume no error ($k_X = 0$) and no loss ($n_{\rm tot} = n_{\rm rep}(1-e^{-\mu})$). The security parameters are set to $\epsilon_{\rm c} = 10^{-15}$ and $\epsilon_{\rm s} = 10^{-10}$. In the limit of $n_{\rm rep} \to \infty$, each curve converges to $l_{\rm WCP}/(n_{\rm rep}/e) = 1$.

is an upper bound of $l^{\rm (HG)}_{\rm WCP}$ derived in Eq. (6.60). The figure shows that the key length $l^{\rm (BI)}_{\rm WCP}$ from Bernoulli sampling is higher than $l^{\rm (HG)}_{\rm WCP}$ from simple random sampling. A possible reason is that the estimation of $\underline{n}_{X,\rm unt}$, which is a pessimistic bound of $n_{X,\rm unt}$, is not required in determining $f_{\rm BI}(k_X)$.

In Fig. 6.3, we show a result in more practical situations based on Eq. (6.54) to make comparison to the previous finite-key analysis for the WCP-BB84 protocol [23]. The figure shows the dependence of secure key rate $l^{\rm (BI)}_{\rm WCP}/n_{\rm rep}$ on the channel transmission η_c. In each curve, the number of Bob's detected signals $n_{\rm det}$ is fixed as $n_{\rm det} = 10^4, 10^5, 10^6$ and 10^7. The parameters were chosen to be the same as [23]: Quantum efficiency of both detectors is $\eta_d = 0.1$ and a dark count probability per pulse is $p_{\rm dark} = 10^{-5}$ per detector. In addition to errors from dark counts, there is a 0.5% loss-independent bit error. The security parameters were set to $\epsilon_{\rm c} = 10^{-10}$, $\epsilon_{\rm s} = 10^{-5}$, $\epsilon_{\rm PE} = 1/16\times10^{-10}$, $\epsilon_{\rm PA} = 1/16\times10^{-10}$, and $\epsilon_{\rm Z,unt} = 1/2\times10^{-5}$. Total transmission rate is $Q = 1-(1-2p_{\rm dark})e^{-\mu\eta_c\eta_d}$, and error rate is given by E/Q where $E = 0.005(1-e^{-\mu\eta_c\eta_d})+p_{\rm dark}e^{-\mu\eta_c\eta_d}$. Based on the parameters above, we assume $\lambda_{\rm EC}(\epsilon_{\rm c}) = 1.05h(E/Q) + \log_2(1/\epsilon_{\rm c})$, $n_{\rm rep} = n_{\rm det}/Q$, $n_Z = n_{\rm det}\tilde{p}_Z^2$, $n_X = n_{\rm det}\tilde{p}_X^2$ and $k_X = n_X E/Q$. To save the computation time, we used Chernoff

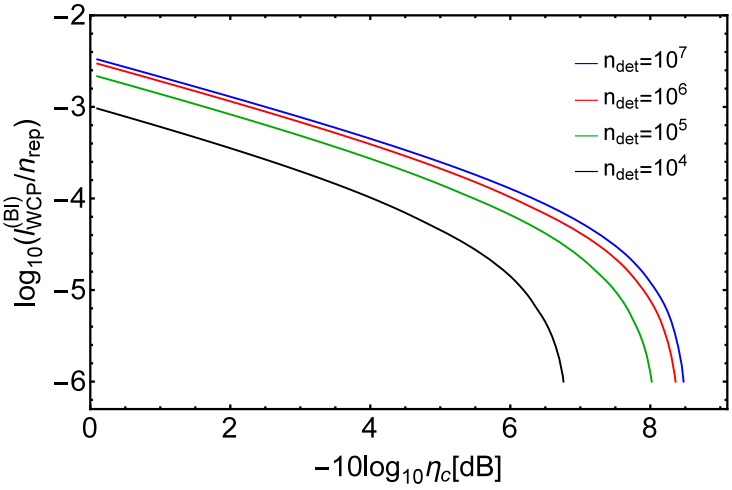

Figure 6.3: Secure key rate per signal of the WCP-BB84 protocol $l^{(\mathrm{BI})}_{\mathrm{WCP}}/n_{\mathrm{rep}}$ as a function of channel transmission η_c. The parameters are set to be the same as Ref. [23]. Quantum efficiency of detectors: $\eta_d = 0.1$. Dark count probability per pulse per detector: $p_{\mathrm{dark}} = 10^{-5}$. Loss-independent bit error: 0.5%. Error correction cost: $\lambda_{\mathrm{EC}}(\epsilon_{\mathrm{c}}) = 1.05h(E/Q) + \log_2(1/\epsilon_{\mathrm{c}})$. The security parameters: $\epsilon_{\mathrm{c}} = 10^{-10}$ and $\epsilon_{\mathrm{s}} = 10^{-5}$. From the top to the bottom curve, the number of detected signals are $n_{\mathrm{det}} = 10^7, 10^6, 10^5$ and 10^4, respectively. The required number of detected signals to generate a final key is less than 10^4, while it was $\sim 10^7$ in the previous result [23].

bound [118]

$$C_{\mathrm{BI}}(k_X; k_{\mathrm{tot}}, p_X) \leq D\left(\frac{k_X}{k_{\mathrm{tot}}}, k_{\mathrm{tot}}, p_X\right) \tag{6.61}$$

for $(k_X, k_{\mathrm{tot}}, p_X)$ satisfying $k_X \leq k_{\mathrm{tot}} p_X$, where

$$D(x, y, z) := \left(\left(\frac{z}{x}\right)^x \left(\frac{1-z}{1-x}\right)^{1-x}\right)^y. \tag{6.62}$$

In Fig. 6.3, we see that a key can be extracted even when $n_{\mathrm{det}} = 10^4$. This is a significant improvement from the result of [23], in which the required number of detected signals to generate a final key is $n_{\mathrm{det}} \sim 10^7$.

6.3.3 The DQPS protocol

In this section, we conduct finite-key analysis of the DQPS protocol based on the property of binomial distribution Eq. (6.40). The precise description of the protocol and physical assumptions for the security proof follow those in Chapter 5 except several notations. In order to establish

the analogy to the WCP-BB84 protocol analyzed in the previous section, we identify Alice's $\{|+\rangle, |-\rangle\}$ measurement with Z-basis measurement, and $\{|-i\rangle, |+i\rangle\}$ measurement with X-basis measurement. Accordingly, we replace the notations as follows:

$$\tilde{p}_0 \to \tilde{p}_Z \tag{6.63}$$

$$\tilde{p}_1 \to \tilde{p}_X \tag{6.64}$$

$$\boldsymbol{\kappa}_{A0},\ \boldsymbol{\kappa}_{B0} \to \boldsymbol{\kappa}_{A,Z},\ \boldsymbol{\kappa}_{B,Z} \tag{6.65}$$

$$\boldsymbol{\kappa}_{A1},\ \boldsymbol{\kappa}_{B1} \to \boldsymbol{\kappa}_{A,X},\ \boldsymbol{\kappa}_{B,X}. \tag{6.66}$$

The alternative tagging rule proposed in Chapter 5 allows the variables $k_{\mathrm{ph,unt}}$ and $n_{Z,\mathrm{unt}}$ to be defined in the same way as in the WCP-BB84 protocol, and the argument up to Eq. (6.35) holds for the DQPS protocol as well. The remaining tasks are to find a function f satisfying Eq. (6.32) and to find a bound $\underline{n}_{Z,\mathrm{unt}}$ satisfying Eq. (6.33), both of which require slightly different approaches from the WCP-BB84 protocol.

Since our tagging definition for the DQPS protocol involves Bob's detection timing j, we cannot decompose the emitted states as in Eq. (4.6). As a result, we cannot rewrite the protocol to postpone the basis selection as in the one shown in Sec. 4.2.2. Hence we need to justify Eq. (6.38) on a different ground. This was essentially done in Chapter 5 along with appendix B, namely, in Eq. (B.4), which reads

$$\Pr(\boldsymbol{c}, \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{j}, \boldsymbol{t}) = \Pr(\boldsymbol{c})\beta(g_{\boldsymbol{t},\boldsymbol{j}}(\boldsymbol{c}), \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{j}, \boldsymbol{t}). \tag{6.67}$$

The random variables $\boldsymbol{c}$, $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{j}$ and $\boldsymbol{t}$ are bit strings of length n_{rep}. Let us rewrite them by various sets introduced in Sec. 6.3.1. Since there is a one-to-one correspondence between $\mathcal{X}_A$ and $\boldsymbol{c}$, and $g_{\boldsymbol{t},\boldsymbol{j}}(\boldsymbol{c})$ is a function of $\{\mathcal{X}_A \cap \overline{\mathcal{N}_{\mathrm{unt}}}, \mathcal{N}_{\mathrm{unt}}\}$, we have

$$\Pr(\mathcal{X}_A, \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{j}, \boldsymbol{t}) = \Pr(\mathcal{X}_A)\tilde{\beta}(\mathcal{X}_A \cap \overline{\mathcal{N}_{\mathrm{unt}}}, \mathcal{N}_{\mathrm{unt}}, \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{j}, \boldsymbol{t}). \tag{6.68}$$

By using the fact that $\mathcal{K}_{\mathrm{unt}}$ and $\mathcal{N}_{\mathrm{unt}}$ are functions of $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{j}$ and $\boldsymbol{t}$, namely, they are written as $\mathcal{K}_{\mathrm{unt}} = F_{\mathcal{K}_{\mathrm{unt}}}(\boldsymbol{j}, \boldsymbol{t})$ and $\mathcal{N}_{\mathrm{unt}} = F_{\mathcal{N}_{\mathrm{unt}}}(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{j}, \boldsymbol{t})$, define

$$\beta'(\mathcal{X}_A \cap \overline{\mathcal{N}_{\mathrm{unt}}}, \mathcal{K}_{\mathrm{unt}}, \mathcal{N}_{\mathrm{unt}}) := \sum_{\boldsymbol{a},\boldsymbol{b},\boldsymbol{j},\boldsymbol{t}} \tilde{\beta}(\mathcal{X}_A \cap \overline{\mathcal{N}_{\mathrm{unt}}}, \mathcal{N}_{\mathrm{unt}}, \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{j}, \boldsymbol{t}), \tag{6.69}$$

where the summation is over $\{\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{j}, \boldsymbol{t}\}$ satisfying $F_{\mathcal{K}_{\mathrm{unt}}}(\boldsymbol{j}, \boldsymbol{t}) = \mathcal{K}_{\mathrm{unt}}$ and $F_{\mathcal{N}_{\mathrm{unt}}}(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{j}, \boldsymbol{t}) = \mathcal{N}_{\mathrm{unt}}$. From Eq. (6.68), we have

$$\Pr(\mathcal{X}_A, \mathcal{K}_{\mathrm{unt}}, \mathcal{N}_{\mathrm{unt}}) = \Pr(\mathcal{X}_A)\beta'(\mathcal{X}_A \cap \overline{\mathcal{N}_{\mathrm{unt}}}, \mathcal{K}_{\mathrm{unt}}, \mathcal{N}_{\mathrm{unt}}), \tag{6.70}$$

which leads to

$$\Pr(\mathcal{X}_A, \mathcal{K}_{\mathrm{unt}}, \mathcal{N}_{\mathrm{unt}}) = \Theta(\mathcal{X}_A, \mathcal{N}_{\mathrm{rep}})\beta'(\mathcal{X}_A \cap \overline{\mathcal{N}_{\mathrm{unt}}}, \mathcal{K}_{\mathrm{unt}}, \mathcal{N}_{\mathrm{unt}}). \tag{6.71}$$

Since $\Theta(\mathcal{M}, \mathcal{N}_{\rm rep})$ defined in Eq. (6.39) satisfies

$$\Theta(\mathcal{M}, \mathcal{N}_{\rm rep}) = \Theta(\mathcal{M} \cap \mathcal{N}_{\rm unt}, \mathcal{N}_{\rm unt})\Theta(\mathcal{M} \cap \overline{\mathcal{N}_{\rm unt}}, \overline{\mathcal{N}_{\rm unt}}) \tag{6.72}$$

for any $\mathcal{M} \subset \mathcal{N}_{\rm rep}$, from Eq. (6.71) we have

$$\begin{aligned} &\Pr(\mathcal{X}_A \cap \mathcal{N}_{\rm unt} = \mathcal{M}_A \mid \mathcal{K}_{\rm unt}, \mathcal{N}_{\rm unt}) \\ &= \Theta(\mathcal{M}_A, \mathcal{N}_{\rm unt})\gamma(\mathcal{K}_{\rm unt}, \mathcal{N}_{\rm unt}) \end{aligned} \tag{6.73}$$

for any $\mathcal{M}_A \subset \mathcal{N}_{\rm unt}$, where

$$\begin{aligned} &\gamma(\mathcal{K}_{\rm unt}, \mathcal{N}_{\rm unt}) \\ &:= \frac{\sum_{\mathcal{M}'_A \subset \overline{\mathcal{N}_{\rm unt}}} \Theta(\mathcal{M}'_A, \overline{\mathcal{N}_{\rm unt}})\beta'(\mathcal{M}'_A, \mathcal{K}_{\rm unt}, \mathcal{N}_{\rm unt})}{\Pr(\mathcal{K}_{\rm unt}, \mathcal{N}_{\rm unt})}. \end{aligned} \tag{6.74}$$

Since the sum of $\Theta(\mathcal{M}_A, \mathcal{N}_{\rm unt})$ over $\mathcal{M}_A$ is unity, Eq. (6.73) leads to $\gamma(\mathcal{K}_{\rm unt}, \mathcal{N}_{\rm unt}) = 1$. Thus, we have

$$\begin{aligned} &\Pr(\mathcal{X}_A \cap \mathcal{N}_{\rm unt} = \mathcal{M}_A \mid \mathcal{K}_{\rm unt}, \mathcal{N}_{\rm unt}) \\ &= \Theta(\mathcal{M}_A, \mathcal{N}_{\rm unt}). \end{aligned} \tag{6.75}$$

In the DQPS protocol, the assumption on Bob's apparatus Eq. (5.6) allows his basis choice to be postponed after he confirms photon detection, which means that the choice of $\mathcal{X}_B$ can be conducted after $\mathcal{K}_{\rm unt}$ and $\mathcal{N}_{\rm unt}$ are determined. Hence, we have

$$\begin{aligned} &\Pr(\mathcal{X}_A \cap \mathcal{N}_{\rm unt} = \mathcal{M}_A, \mathcal{X}_B \cap \mathcal{N}_{\rm unt} = \mathcal{M}_B \mid \mathcal{K}_{\rm unt}, \mathcal{N}_{\rm unt}) \\ &= \Theta(\mathcal{M}_A, \mathcal{N}_{\rm unt})\Theta(\mathcal{M}_B, \mathcal{N}_{\rm unt}), \end{aligned} \tag{6.76}$$

which is identical to Eq. (6.38). Similarly to the WCP-BB84 protocol, Eq. (6.40) holds, which leads to Eq. (6.43):

$$\Pr(k_{\rm ph,unt} > f_{\rm BI}(k_X)) \leq \epsilon_{\rm PE}. \tag{6.77}$$

The task of finding a bound $\underline{n}_{Z,\rm unt}$ satisfying Eq. (6.33) is done as follows. In Chapter 5, a modified protocol having exactly the same $\Pr(n_{Z,\rm tag})$ as the original protocol was introduced, in which a random variable N (denoted as $n(c = d = 0, (z'_0 \ldots z'_{L-1}) \notin \Gamma^{(m)})$ in Eq. (5.39) of Chapter 5) satisfying $N \geq n_{Z,\rm tag}$ is defined. The variable obeys binomial distribution $\mathrm{BI}(N, n_{\rm rep}, r_{\rm tag}\tilde{p}_Z^2)$, where $r_{\rm tag}$ is a property of the light source defined as Eq. (5.43) (or Eq. (5.48) for general light sources). This implies that $\Pr(n_{Z,\rm tag})$ in the original protocol has the following property: There exists a

function $P(n_{Z,\mathrm{tag}}, N)$ satisfying

$$\begin{aligned}
&\Pr(n_{Z,\mathrm{tag}}) = \sum_N P(n_{Z,\mathrm{tag}}, N) \\
&P(n_{Z,\mathrm{tag}}, N) = 0 \ \text{ for } \ n_{Z,\mathrm{tag}} > N \\
&\sum_{n_{Z,\mathrm{tag}}} P(n_{Z,\mathrm{tag}}, N) = \mathrm{BI}(N, n_{\mathrm{rep}}, r_{\mathrm{tag}}\tilde{p}_Z^2).
\end{aligned} \tag{6.78}$$

This leads to

$$\Pr(n_{Z,\mathrm{tag}} > n) \le 1 - C_{\mathrm{BI}}(n; n_{\mathrm{rep}}, r_{\mathrm{tag}}\tilde{p}_Z^2) \tag{6.79}$$

for any n, which is identical to Eq. (6.49). Then, following the same argument as the WCP-BB84 protocol, we see that

$$\Pr(n_{Z,\mathrm{unt}} < \underline{n}_{Z,\mathrm{unt}}) \le \epsilon_{Z,\mathrm{unt}} \tag{6.80}$$

holds with

$$\underline{n}_{Z,\mathrm{unt}} := n_Z - g(r_{\mathrm{tag}}\tilde{p}_Z^2, \epsilon_{Z,\mathrm{unt}}). \tag{6.81}$$

From Eqs. (6.35), (6.77) and (6.80), we arrive at a key rate formula which is identical to Eq. (6.54): The L-pulse DQPS protocol is ϵ_{c}-correct and ϵ_{s}-secret if the final key length l_{fin} satisfies

$$l_{\mathrm{fin}} \le l_{\mathrm{DQPS}} := \underline{n}_{Z,\mathrm{unt}}\left(1 - h\left(\frac{f_{\mathrm{BI}}(k_X)}{\underline{n}_{Z,\mathrm{unt}}}\right)\right) - \log_2\frac{2}{\epsilon_{\mathrm{PA}}} - \lambda_{\mathrm{EC}}(\epsilon_{\mathrm{c}}), \tag{6.82}$$

where ϵ_{s} is given in Eq. (6.34). Together with Eqs. (5.43), (6.13), (6.14), (6.51) and (6.81), Eq. (6.82) constitutes the main result of Sec. 6.3.3.

In Fig. 6.4, we show numerical results of secure key rate per pulse $l_{\mathrm{DQPS}}/(n_{\mathrm{rep}}L)$ as a function of overall transmittance $\eta := \eta_c\eta_d$ to compare the DQPS protocol ($L > 2$) and the PE-BB84 protocol ($L = 2$). The solid curves represent the key rate with fixed pulse number $n_{\mathrm{rep}}L = 10^7$, and the dashed curves represent the one for the asymptotic case, which is obtained in Chapter 5. We assumed that Alice generates a weak coherent pulse of mean photon number μ, namely, r_{tag} is given by Eq. (5.43). We assume dark count rate per pulse per detector $p_{\mathrm{dark}} = 0.5 \times 10^{-5}$ and a loss-independent bit error rate 3%. We also assumed that $Q = 1 - (1 - 2(L-1)p_{\mathrm{dark}})e^{-(L-1)\mu\eta}$, reflecting the fact that there are $L - 1$ valid timings in a block. Error rate is given by E/Q where $E = 0.03(1 - e^{-(L-1)\mu\eta}) + p_{\mathrm{dark}}e^{-(L-1)\mu\eta}(L-1)$. Based on these parameters, we assume $\lambda_{\mathrm{EC}}(\epsilon_{\mathrm{c}}) = 1.1h(E/Q) + \log_2(1/\epsilon_{\mathrm{c}})$, $n_Z = n_{\mathrm{rep}}Q\tilde{p}_Z^2$, $n_X = n_{\mathrm{rep}}Q\tilde{p}_X^2$ and $k_X = n_X E/Q$. The values of $\tilde{p}_X$ and μ are optimized to maximize the key length. In the asymptotic limit, the parameter optimization leads to $\tilde{p}_X \to 0$, $\underline{n}_{Z,\mathrm{unt}} \to n_{\mathrm{rep}}(Q - r_{\mathrm{tag}})$ and $f_{\mathrm{BI}}(k_X)/\underline{n}_{Z,\mathrm{unt}} \to E/(Q - r_{\mathrm{tag}})$ while Q and E are fixed. In finite-key cases, the Chernoff bound is used to calculate the key rate. The

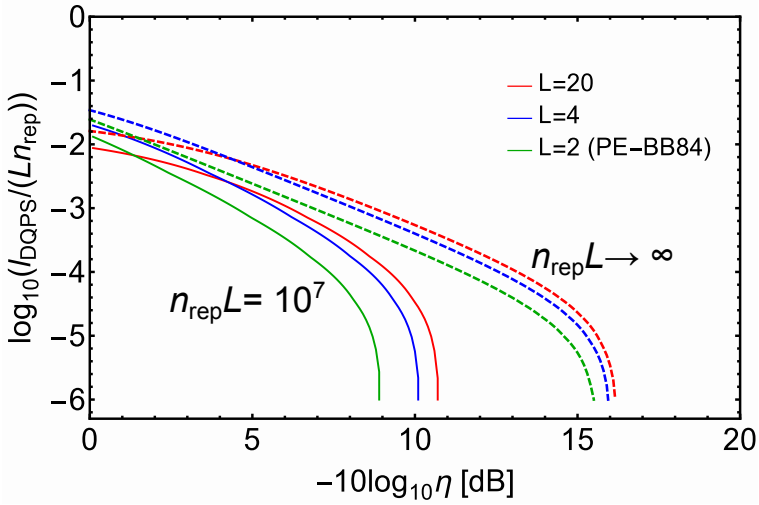

Figure 6.4: Secure key rate per pulse of the DQPS protocol $l_{\mathrm{DQPS}}/(n_{\mathrm{rep}}L)$ as a function of overall transmission η. Solid curves are the results of the finite key analysis with total pulse number $n_{\mathrm{rep}}L = 10^7$ and dashed curves are the results of the asymptotic case ($n_{\mathrm{rep}}L \to \infty$), which are obtained in Chapter 5. For both solid and dotted curves, the top, middle and bottom curves represent the key rate for $L = 20$, $L = 4$ and $L = 2$, respectively. The parameters are set as follows. Dark count rate per pulse per detector: $p_{\mathrm{dark}} = 0.5 \times 10^{-5}$. Loss-independent bit error: 3%. Cost for error correction: $\lambda_{\mathrm{EC}}(\epsilon_{\mathrm{c}}) = 1.1h(E) + \log_2(1/\epsilon_{\mathrm{c}})$. The security parameter: $\epsilon_{\mathrm{c}} = 10^{-15}$ and $\epsilon_{\mathrm{s}} = 10^{-10}$. We see that the key rate of the DQPS protocol ($L > 2$) is higher than that of the PE-BB84 protocol ($L = 2$) for both the asymptotic and finite-key cases.

security parameters are set to be the same as those in Fig. 6.2. We see that the advantage of the DQPS protocol over the PE-BB84 protocol is maintained even if we include the effect of the finiteness of the key.

6.4 Concluding remarks

6.4.1 Summary of results

In this chapter, we proposed a method of finite-key analysis based on Bernoulli sampling instead of simple random sampling. For the BB84 protocol using biased basis choice, the data gathered on one of the basis is solely used for estimation of the disturbance in the other basis, which enables us to regard the former as a sample drawn from the population via Bernoulli sampling. As a result, we obtained finite-sized key-length formulas based on the binomial distribution parametrized by

the probability of the basis choice in the protocol. The appearance of the binomial distribution in our case is a direct consequence of the inherent statistics of the protocol, and it should be differentiated from the previous works which uses a binomial distribution to derive an upper bound on the hypergeometric distribution arising from simple random sampling.

The new method is particularly suited for the BB84 protocol with WCP. It enables simpler analysis compared to the method with simple random sampling since only the latter requires the estimation of the sample size ($n_{X,\mathrm{unt}}$). We may expect that this additional pessimistic bound makes the conventional method less efficient, which is corroborated by a numerical example showing that the key rate for the WCP-BB84 protocol obtained with our method is higher than that with simple random sampling. To make comparison with the previous finite-key analysis for the WCP-BB84 protocol [23], we calculated the key rate as a function of channel transmission and the number of detected signals, in the same practical parameter settings. The result shows that, while $n_{\mathrm{det}} \sim 10^7$ signals are necessary for producing a key in Ref. [23], our method only needs $n_{\mathrm{det}} \sim 10^4$ with the same parameters. In addition, the improved number 10^4 clarifies that the use of WCP instead of an ideal single photon causes only a small change in the finite-size effect. This was also confirmed in the numerical simulation assuming the perfect channel, in which the required number of rounds to generate a key is $n_{\mathrm{rep}} \sim 10^{3.7}$ for the WCP-BB84 protocol and is $n_{\mathrm{rep}} \sim 10^{3.2}$ for the single-photon BB84 protocol.

Finally, we applied the Bernoulli-sampling method to the DQPS protocol, which was recently proved to be secure in the asymptotic regime. Although the asymptotic proof is based on the tagging of the insecure rounds as in the WCP-BB84 protocol, the definition of the tagged round is much more convoluted and makes sense only after the signal was detected by Bob. Nonetheless, our finite-key analysis has led to a key rate formula closely analogous to the one for the WCP-BB84 protocol. Numerical calculation shows that the DQPS protocol retains higher key rates than the PE-BB84 even in the finite-key regime of $n_{\mathrm{rep}} = 10^7$.

6.4.2 Discussion

It is expected that our method can also be applied to protocols with decoy states [36, 37, 38]. Since the existing analyses [15, 16, 24, 76] with decoy states involve the estimation of the sample size $n_{X,\mathrm{unt}}$, the present method may provide a simpler analysis compared to the conventional methods with simple random sampling. It should be mentioned that some of the finite key analyses [15, 16] assumed the announcement of basis choice after each round to make the sample size fixed, which were later pointed out [66] to open a security hole against a sifting attack. This illustrates an importance of simpler and more straightforward methods, and we believe that the method proposed here will contribute in this regard.

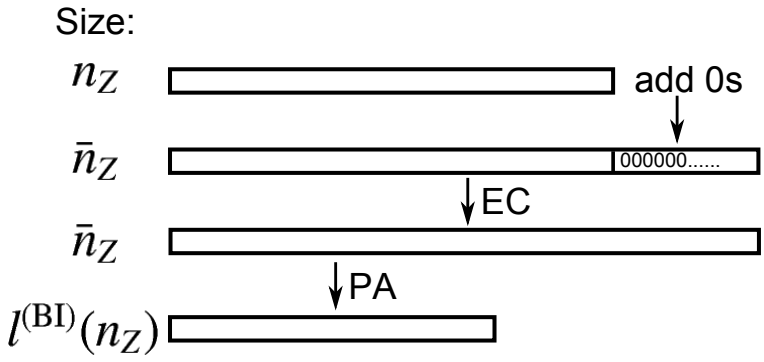

Figure 6.5: Procedures of "0-filling" idea for error correction of fixed data size $\bar{n}_Z$. If the sifted key size n_Z is larger than $\bar{n}_Z$, the protocol aborts. If $n_Z \leq \bar{n}_Z$ is confirmed, $\bar{n}_Z - n_Z$ 0s are added to the sifted key in trivial positions (e.g. the edge of the key). After error correction, privacy amplification is conducted to shorten the key to the size $l^{(\mathrm{BI})}(n_Z)$, which is obtained in the security proof and independent of $\bar{n}_Z$.

Another interest is practical use of our method. In practice, the length of sifted key is desired to be predetermined for the sake of fast error correction, using LDPC code, for example. On the other hand, our method is valid for the protocol where the number of round is fixed and the length of sifted key varies (obeying binomial distribution). Although this may seem to weaken the utility of our method, here we propose a possible idea to amend it (see Fig. 6.5). Suppose that the input-data size for error correction is fixed to $\bar{n}_Z$. In the proposed idea, we determine the number of total rounds n_{rep} so that the length of obtained sifted key n_Z is *smaller* than $\bar{n}_Z$ with high probability, and we add the $\bar{n}_Z - n_Z$ 0s to the sifted key in order to obtain the bit strings of size $\bar{n}_Z$. After the error-correcting process is finished, we shorten the bit strings in privacy-amplification process by the length of $\bar{n}_Z - n_Z$ in addition to non-trivial amount estimated with security analysis. This method is possible without using any secret keys or random numbers, which is in contrast to the recently-proposed method [66] where n_{rep} is determined so that n_Z is *larger* than $\bar{n}_Z$ with high probability followed by discarding $n_Z - \bar{n}_Z$ bits at random. The security of our method is intuitively explained by the tagging idea. That is, if the insecure (tagged) rounds are in principle identified, the size of secret key is determined by the security of the other (untagged) rounds. Obviously, the position of insecure rounds (0s) in the bit strings of size $\bar{n}_Z$ are identified in our idea. Although more rigorous argument is expected in the future, we believe that the utility of the Bernoulli-sampling method is ensured by the proposed idea.

Chapter 7

Conclusion and outlook

7.1 Conclusion

In this thesis, the security of QKD protocols using weak coherent pulses (WCP) was studied. We focused on the DQPS protocol, which is a variant of the DPS protocol and is also regarded as a variant of the PE-BB84 protocol. Although the conventional tagging technique used for the BB84 protocol cannot be applied to the DQPS protocol because of its property of coherence chain, the alternative rule of tagging was constructed through the outcomes of Alice's virtual measurement on ancillary qubits. By using this technique and the security proof of the BB84 protocol with complementarity, the security of the DQPS protocol was proved, and its key generation rate was shown to be 8/3 times as high as that of the PE-BB84 protocol in the asymptotic limit. We also showed that the set up for calibration of light source, which tends to be complicated in the decoy-state method, is kept to be minimum in the DQPS protocol as in the BB84 protocol.

In order to consolidate the advantage of the DQPS protocol over the PE-BB84 protocol, we worked on the finite-key analysis for the WCP-QKD protocols. A new method of the finite-key analysis was proposed based on the Bernoulli sampling related to binomial distribution, which is in contrast to the currently used method based on simple random sampling associated with hypergeometric distribution. Not only the expected advantage of the DQPS protocol was confirmed even in the finite-key regime with the proposed method, the method was shown to be suitable for the WCP-BB84 protocol. For the WCP-BB84 protocol, security analysis with estimation of a smaller number of parameters is possible by using the Bernoulli-sampling method, which leads to a higher key rate compared to the method with simple random sampling. Furthermore, the required number of detected signals reduces to 10^4, which is drastic improvement from the number 10^7 required in the previous work for the WCP-BB84 protocol.

For further development of QKD systems, the simplicity is crucial from both practical and

theoretical aspects. The complicated devices lead to higher cost for their installation, and also enlarge the gap between the physical models assumed in the security proof and their actual behaviors. The DQPS protocol is beneficial in this sense, for it has essentially the same set up as the PE-BB84 protocol including calibration of light source, which only requires a typical laser, phase modulators, a passive interferometer and detectors. For the theoretical aspect, the security analyses of the QKD protocols should be simple and clear since its correctness can not be directly certified by experiment (unlike conventional physics theory), and users of QKD are supposed to rely on the security proofs. In the proposed method based on Bernoulli sampling, binomial distribution parametrized by the probability of basis choice is used instead of hypergeometric distribution, which enables simpler analysis with smaller number of estimations. This method is expected to be applied to the decoy-state method, which has more complicated analysis with larger number of estimating parameters than the WCP-BB84 protocol and the DQPS protocol.

7.2 Related works and future outlook

One of the motivations that I focused on the DQPS protocols was to seek for a more efficient protocol than the BB84 protocol. Although the advantage of the DQPS protocol over the PE-BB84 protocol was shown, further improvement for the security analysis is expected to show its robustness against PNS attacks which was certified in the DPS protocol. Another protocol I worked on was high-dimensional (HD) protocol (qudit-based protocol) although the details were not mentioned in this thesis. HD protocols enable energy-efficient communication, and they are expected to have high-error tolerance [49, 50]. Recently, the entanglement-based HD protocol, which uses time (photon position) and frequency as two bases, were proved to be secure [106, 107] based on the security analysis for continuous variable QKD as well as were demonstrated with high key generation rate [119]. I analyzed the security of a prepare-and-measure-type HD protocol, which uses information of discrete time and frequency, based on the security proof with complementarity to evaluate its tolerance to practical errors. The result was not positive at least in my case, that is, no higher-error tolerance was confirmed compared to the two-dimension protocol (BB84 protocol) if we assume practical errors, mainly because the use of a larger number of temporal modes results in more errors caused by dark counts of detectors. On the other hand, some of my collaborators recently showed that the round-robin DPS (RR-DPS) protocol, which uses many temporal modes with symmetrization, has robustness against PNS attacks as well as high error tolerance that a secret key can be generated even with 50 % errors in principle.

Although the RR-DPS protocol has such an unusual property, it is not fully understood what kind of principle of quantum physics contributes to it. The high error tolerance is not confirmed in the DPS protocol with current complicated security proof resulting in low key generation rate,

while it has a room for improvement. A similar situation applies to another protocol using the property of coherence chain, the coherent-one-way (COW) protocol [111], in which the robustness against PNS attacks is not confirmed against standard predictions but possible improvements of hardware and proof are suggested [98]. The security analysis of the DQPS protocol can be an important step to address the above involved problems. For example, our result implies that if one wants to confirm the robustness against PNS attacks in the non-symmetrized protocol such as the DPS protocol and the DQPS protocol, it is essential to use bit errors reflecting disturbance of coherence chain in the security proof (as is done in the security proof for the DPS protocol). Several theoretical interests still remain:

· Is the symmetrization of the temporal mode necessary to confirm the high error tolerance?

· Although the protocols with coherence chain (DPS, DQPS, RR-DPS, COW) assume that sequential pulses are separated by blocks, is it essentially possible to remove the assumption? If it is true, are some interesting properties (PNS robustness, high error tolerance or others) confirmed as a result of security proof?

Tackling those problems may not only lead to improvements of those protocols in terms of key generation efficiency, but also clarify the mechanism of how quantum properties contribute to the essential bound on leaked information, which can help us to understand the relation between quantum physics and information theory more deeply.

Appendix A

Proof of lemma 1

With ancillary system Q and R, let us introduce $|\Psi\rangle_{AEQR}$ and $|\Phi\rangle_{AEQR}$ as purified state of $\hat{\tau}_{AE}$ and $|\tilde{0}\rangle\langle\tilde{0}|_A \otimes \hat{\tau}_E$, respectively, which are written as

$$|\Psi\rangle_{AEQR} := \sum_{i\geq 0} |\tilde{i}\rangle_A |\psi_i\rangle_{EQ} |0\rangle_R \tag{A.1}$$

$$|\Phi\rangle_{AEQR} := |\tilde{0}\rangle_A |\phi\rangle_{EQR}\,, \tag{A.2}$$

where $\{|\tilde{i}\rangle_A\}_{i\geq 0}$ is an orthogonal set. By using Uhlmann's theorem Eq. (2.7),

$$\begin{aligned} &F(\hat{\tau}_{AE},\ |\tilde{0}\rangle\langle\tilde{0}|_A \otimes \hat{\tau}_E) \\ &= \max_{|\Phi\rangle:\ \mathrm{Tr}_{QR}|\Phi\rangle\langle\Phi|=|\tilde{0}\rangle\langle\tilde{0}|_A\otimes\hat{\tau}_E} \left|{}_{AEQR}\langle\Psi|\Phi\rangle_{AEQR}\right|^2 &\text{(A.3)}\\ &= \max_{|\phi\rangle:\ \mathrm{Tr}_{QR}|\phi\rangle\langle\phi|=\hat{\tau}_E} \left|{}_{EQ}\langle\psi_0|_R\langle 0|\phi\rangle_{EQR}\right|^2. &\text{(A.4)} \end{aligned}$$

If we set $|\phi\rangle_{EQR} = \sum_{i\geq 0} |\psi_i\rangle_{EQ}|i\rangle_R$ with an orthogonal set $\{|i\rangle_R\}_{i\geq 0}$, we have

$$\begin{aligned} &\mathrm{Tr}_{QR}(|\phi\rangle\langle\phi|_{EQR}) \\ &= \sum_{i,j} \mathrm{Tr}_{QR}\left(|\psi_i\rangle\langle\psi_j|_{EQ}|i\rangle\langle j|_R\right) &\text{(A.5)}\\ &= \sum_i \mathrm{Tr}_Q\left(|\psi_i\rangle\langle\psi_i|_{EQ}\right) &\text{(A.6)}\\ &= \hat{\tau}_E. &\text{(A.7)} \end{aligned}$$

Then from (A.4),

$$\begin{aligned} &F(\hat{\tau}_{AE},\ |\tilde{0}\rangle\langle\tilde{0}|_A \otimes \hat{\tau}_E) \\ &\geq \left|\sum_i {}_{EQ}\langle\psi_0|_R\langle 0|\psi_i\rangle_{EQ}|i\rangle_R\right|^2 &\text{(A.8)}\\ &= \left|{}_{EQ}\langle\psi_0|\psi_0\rangle_{EQ}\right|^2 &\text{(A.9)} \end{aligned}$$

holds. On the other hand, we have

$$
\begin{aligned}
& F(\hat{\tau}_A,\ |\tilde{0}\rangle\langle\tilde{0}|_A) \\
&= {}_A\langle\tilde{0}|\,\mathrm{Tr}_{EQR}\left(|\Psi\rangle\langle\Psi|_{AEQR}\right)|\tilde{0}\rangle_A && \text{(A.10)} \\
&= \sum_{i,j} {}_A\langle\tilde{0}|\,\mathrm{Tr}_{EQR}\left(|\tilde{i}\rangle\langle\tilde{j}|_A\,|\psi_i\rangle\langle\psi_j|_{EQ}\,|0\rangle\langle 0|_R\right)|\tilde{0}\rangle_A && \text{(A.11)} \\
&= \mathrm{Tr}_{EQ}(|\psi_0\rangle\langle\psi_0|_{EQ}) && \text{(A.12)} \\
&= {}_{EQ}\langle\psi_0|\psi_0\rangle_{EQ}\,. && \text{(A.13)}
\end{aligned}
$$

Eq. (A.9) and Eq. (A.13) lead to

$$
F(\hat{\tau}_{AE},\ |\tilde{0}\rangle\langle\tilde{0}|_A \otimes \hat{\tau}_E) \geq \left(F(\hat{\tau}_A,\ |\tilde{0}\rangle\langle\tilde{0}|_A)\right)^2. \qquad \text{(A.14)}
$$

Appendix B

Untagged check-basis outcomes as an unbiased sample

Here, we prove Eq. (5.34) in the main text by showing that the untagged rounds with $c = 1$ is uniformly extracted from the whole untagged events. For fixed c, j ($\neq 0$) and m, define a projector $\hat{T}^{(c,j,m)}_{a,t} := \sum_{\{z_l\}} |\mathcal{A}^{(c,j)}_{a,\{z_l\}}\rangle_A \langle \mathcal{A}^{(c,j)}_{a,\{z_l\}}|$ where the summation is over $\{z_l\}$ satisfying $\sum_{l\neq j} z_l = m$ for $t = 0$ and $\sum_{l\neq j} z_l < m$ for $t = 1$. The projector $\hat{T}^{(c,j,m)}_{a,t}$ can be regarded as the POVM element for the measurement on system A to determine a and t through Steps 5-1*, 5-2*, and 5-3** with the rule of Eq. (5.10). Although the protocol does not define the values of a, b, and t in case of $j = 0$, it simplifies the notations if we also define those values to be $a = b = t = 0$ for $j = 0$, and define $\hat{T}^{(c,0,m)}_{a,t}$ accordingly. We label each of the $n_{\rm rep}$ rounds by $r = 1, 2, \ldots, n_{\rm rep}$, and use $c_r, a_r, b_r, j_r, m_r, t_r$ to denote the values of c, a, b, j, m, t in the r-th round. Let $\boldsymbol{c}, \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{j}, \boldsymbol{m}, \boldsymbol{t}$ be vectors with $n_{\rm rep}$ elements corresponding to $r = 1, 2, \ldots, n_{\rm rep}$. With these notations, the procedure of determining these vectors in the virtual protocol (with replacement 5-3**) is summarized as follows.

i) Alice selects $\boldsymbol{c}$ randomly, prepares $\hat{\rho}_{AS}(\boldsymbol{c}) := \bigotimes_{r=1}^{n_{\rm rep}} \hat{\sigma}_{AS}(c_r)$ with $\hat{\sigma}_{AS}(c_r) := |\Psi(c_r)\rangle_{AS} \langle \Psi(c_r)|$, and measures $\boldsymbol{m}$ by a projection measurement.

ii) Eve's attack on $n_{\rm rep}$ copies of system S followed by Bob's measurement determines $\boldsymbol{j}$ and $\boldsymbol{b}$. For a given attack strategy by Eve, this whole procedure on $n_{\rm rep}$ systems should be represented by POVM with elements $\{\hat{D}_{\boldsymbol{j},\boldsymbol{b}}\}$.

iii) Given $\boldsymbol{c}$, $\boldsymbol{j}$, and $\boldsymbol{m}$, Alice measures $n_{\rm rep}$ copies of system A to obtain $\boldsymbol{a}$ and $\boldsymbol{t}$, which is represented by the POVM elements $\{\hat{T}^{(\boldsymbol{c},\boldsymbol{j},\boldsymbol{m})}_{\boldsymbol{a},\boldsymbol{t}} := \bigotimes_{r=1}^{n_{\rm rep}} \hat{T}^{(c_r,j_r,m_r)}_{a_r,t_r}\}$.

The joint probability that $\boldsymbol{c}, \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{j}, \boldsymbol{t}$ are obtained is written as

$$\Pr(\boldsymbol{c}, \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{j}, \boldsymbol{t}) = \sum_{\boldsymbol{m}} \Pr(\boldsymbol{c}) \operatorname{tr}\left((\hat{T}^{(\boldsymbol{c},\boldsymbol{j},\boldsymbol{m})}_{\boldsymbol{a},\boldsymbol{t}} \otimes \hat{D}_{\boldsymbol{j},\boldsymbol{b}})(\hat{N}_{\boldsymbol{m}} \hat{\rho}_{AS}(\boldsymbol{c}) \hat{N}_{\boldsymbol{m}})\right). \tag{B.1}$$

Let $g_{\boldsymbol{t},\boldsymbol{j}}(\boldsymbol{c})$ be a function for fixed $\boldsymbol{t}$ and $\boldsymbol{j}$ defined as $g_{\boldsymbol{t},\boldsymbol{j}}(\boldsymbol{c}) = (\bar{c}_1, \bar{c}_2, ..\bar{c}_{n_{\rm rep}})$ where $\bar{c}_r = c_r$ (t_r=1 or $j_r = 0$) and $\bar{c}_r = 0$ (t_r=0 and $j_r \neq 0$). From Eq. (5.33), for $t_r = 0$ and $j_r \neq 0$ we have

$$\mathrm{tr}_A\left((\hat{T}^{(0,j_r,m_r)}_{a_r,0} \otimes \hat{\mathbb{1}}_S)(\hat{N}_{m_r}\hat{\sigma}_{AS}(0)\hat{N}_{m_r})\right) = \mathrm{tr}_A\left((\hat{T}^{(1,j_r,m_r)}_{a_r,0} \otimes \hat{\mathbb{1}}_S)(\hat{N}_{m_r}\hat{\sigma}_{AS}(1)\hat{N}_{m_r})\right), \tag{B.2}$$

since $\hat{\sigma}_{AS}(c_r) = |\Psi(c_r)\rangle_{AS}\,\langle\Psi(c_r)|$. Thus, for $\boldsymbol{c}, \boldsymbol{c}'$ satisfying $g_{\boldsymbol{t},\boldsymbol{j}}(\boldsymbol{c}) = g_{\boldsymbol{t},\boldsymbol{j}}(\boldsymbol{c}') = \boldsymbol{c}_{\rm const}$, we have

$$\mathrm{tr}_A\left((\hat{T}^{(\boldsymbol{c},\boldsymbol{j},\boldsymbol{m})}_{\boldsymbol{a},\boldsymbol{t}} \otimes \hat{\mathbb{1}}_S)(\hat{N}_{\boldsymbol{m}}\hat{\rho}_{AS}(\boldsymbol{c})\hat{N}_{\boldsymbol{m}})\right) = \mathrm{tr}_A\left((\hat{T}^{(\boldsymbol{c}',\boldsymbol{j},\boldsymbol{m})}_{\boldsymbol{a},\boldsymbol{t}} \otimes \hat{\mathbb{1}}_S)(\hat{N}_{\boldsymbol{m}}\hat{\rho}_{AS}(\boldsymbol{c}')\hat{N}_{\boldsymbol{m}})\right). \tag{B.3}$$

Therefore, Eq. (B.1) is written in the form

$$\Pr(\boldsymbol{c}, \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{j}, \boldsymbol{t}) = \Pr(\boldsymbol{c})\beta(g_{\boldsymbol{t},\boldsymbol{j}}(\boldsymbol{c}), \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{j}, \boldsymbol{t}), \tag{B.4}$$

which leads to, for a given value of $\boldsymbol{c}_{\rm const}$, we obtain

$$\begin{aligned} & \frac{\Pr(\boldsymbol{c}, \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{j}, \boldsymbol{t})}{\sum_{\boldsymbol{c}':g_{\boldsymbol{t},\boldsymbol{j}}(\boldsymbol{c}')=\boldsymbol{c}_{\rm const}} \Pr(\boldsymbol{c}', \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{j}, \boldsymbol{t})} \\ = & \frac{\Pr(\boldsymbol{c})\beta(\boldsymbol{c}_{\rm const}, \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{j}, \boldsymbol{t})}{\sum_{\boldsymbol{c}':g_{\boldsymbol{t},\boldsymbol{j}}(\boldsymbol{c}')=\boldsymbol{c}_{\rm const}} \Pr(\boldsymbol{c}')\beta(\boldsymbol{c}_{\rm const}, \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{j}, \boldsymbol{t})} \\ = & \frac{\Pr(\boldsymbol{c})}{\sum_{\boldsymbol{c}':g_{\boldsymbol{t},\boldsymbol{j}}(\boldsymbol{c}')=\boldsymbol{c}_{\rm const}} \Pr(\boldsymbol{c}')} \end{aligned} \tag{B.5}$$

for $\boldsymbol{c}$ satisfying $g_{\boldsymbol{t},\boldsymbol{j}}(\boldsymbol{c}) = \boldsymbol{c}_{\rm const}$. Eq. (B.5) shows that for the rounds with $t = 0$ and $j \neq 0$, the probability of obtaining $c = 0, 1$ is $\tilde{p}_0$, $\tilde{p}_1$ and is independent of the value of a, b, j. Therefore, in the limit of $n_{\rm rep} \to \infty$,

$$\frac{n(c = 0, t = 0, a \neq b, j \neq 0)}{n(c = 1, t = 0, a \neq b, j \neq 0)} = \frac{\tilde{p}_0}{\tilde{p}_1} \tag{B.6}$$

holds, where n(*condition*) denotes the number of rounds satisfying the *condition* in the $n_{\rm rep}$ rounds. Finally, notice that Bob conducts check-basis measurement regardless of the value of d in the virtual protocol, and hence d is independent of the other variables. Therefore, we have

$$\frac{n(c = d = 0, t = 0, a \neq b, j \neq 0)}{n(c = d = 1, t = 0, a \neq b, j \neq 0)} = \left(\frac{\tilde{p}_0}{\tilde{p}_1}\right)^2, \tag{B.7}$$

which corresponds to Eq. (5.34).

Appendix C

Security proof for DQPS with a general light source

Here we show that the security proof in Sec. 5.2 can be extended to the use of a general light source. Suppose that the laser in Fig. 5.1 emits a train of L pulses in a general mixed state $\hat{\sigma}_S$. We assume that every train from the laser is independent and has the same state $\hat{\sigma}_S$. We also assume that the subsequent phase modulation is ideal. The state after the phase modulation, which was given in Eq. (5.1) in the description of the actual protocol, is now given by

$$\left(\bigotimes_{l=0}^{L-1} \exp(i\theta_l(a_l,c)\hat{m}_l)\right) \hat{\sigma}_S \left(\bigotimes_{l'=0}^{L-1} \exp(-i\theta_{l'}(a_{l'},c)\hat{m}_{l'})\right), \tag{C.1}$$

and the one after the randomization of the overall optical phase is (see Sec. 4.2.1)

$$\sum_m \hat{N}_m \left(\bigotimes_{l=0}^{L-1} \exp(i\theta_l(a_l,c)\hat{m}_l)\right) \hat{\sigma}_S \left(\bigotimes_{l'=0}^{L-1} \exp(-i\theta_{l'}(a_{l'},c)\hat{m}_{l'})\right) \hat{N}_m \tag{C.2}$$

instead of Eq. (5.4).

The security proof in Sec. 5.2 used the assumption of pure coherent states Eq. (5.1) in several occasions, which are listed as follows:

i) The state preparation in the virtual protocol [Eq. (5.7)], and its relation [Eq. (5.9)] to the actual protocol.

ii) The parity correlation [Eq. (5.14)] between the auxiliary qubits and the photon numbers in pulses.

iii) The derived properties [Eqs. (5.26), (5.28), (5.30), (5.32), (5.33) and (B.2)] for proving that the sampling is unbiased as in Eq. (5.34).

iv) The expressions [Eqs. (5.40) and (5.48)] for the parameter r_{tag}.

In what follows, we describe how each of the above arguments are rephrased in terms of the general state $\hat{\sigma}_S$.

i) In the virtual protocol, we assume that Alice prepares the following state on system AS,

$$\hat{\sigma}_{AS}(c) \coloneqq \hat{R}(c)\hat{\sigma}_S\hat{R}(c)^\dagger, \tag{C.3}$$

instead of Eq. (5.7). Here $\hat{R}(c)$ is defined by

$$\hat{R}(c) \coloneqq \bigotimes_{l=0}^{L-1}\Big[\frac{1}{\sqrt{2}}\Big(|+\rangle_{A,l}\exp(i\frac{\pi}{2}lc\hat{m}_l) + |-\rangle_{A,l}\exp(i(\pi+\frac{\pi}{2}lc)\hat{m}_l)\Big)\Big]. \tag{C.4}$$

Then it is straightforward to confirm that

$$\begin{aligned}&\Big(\bigotimes_{l=0}^{L-1}{}_{A,l}\langle\pm|\Big)\hat{\sigma}_{AS}(c)\Big(\bigotimes_{l'=0}^{L-1}|\pm\rangle_{A,l'}\Big)\\ =\ &\frac{1}{2^L}\Big(\bigotimes_{l=0}^{L-1}\exp(i\theta_l(a_l,c)\hat{m}_l)\Big)\ \hat{\sigma}_S\ \Big(\bigotimes_{l'=0}^{L-1}\exp(-i\theta_{l'}(a_{l'},c)\hat{m}_{l'})\Big),\end{aligned} \tag{C.5}$$

where $\pm$ of the l-th qubit should be chosen according to the bit a_l. This is the general-state expression for Eq. (5.9), which leads to the equivalence of state preparation between the actual and the virtual protocol.

ii) As $\hat{R}(c)$ is written in Z basis as

$$\begin{aligned}\hat{R}(c) &= \bigotimes_{l=0}^{L-1}\Big[\frac{1}{2}i^{\,lc\hat{m}_l}\Big(|0\rangle_{A,l}(\hat{\mathbb{1}}_{S,l}+(-1)^{\hat{m}_l}) + |1\rangle_{A,l}(\hat{\mathbb{1}}_{S,l}-(-1)^{\hat{m}_l})\Big)\Big]\\ &= \bigotimes_{l=0}^{L-1}\Big[i^{\,lc\hat{m}_l}\Big(|0\rangle_{A,l}\sum_{m_l:\text{even}}\hat{P}(|m_l\rangle_{S,l}) + |1\rangle_{A,l}\sum_{m_l:\text{odd}}\hat{P}(|m_l\rangle_{S,l})\Big)\Big],\end{aligned} \tag{C.6}$$

we have

$$\hat{\Upsilon}_{AS}\hat{R}(c) = \hat{R}(c), \tag{C.7}$$

which is a generalization of Eq. (5.14). It immediately implies that $\hat{\Upsilon}_{AS}\hat{\sigma}_{AS}(c)\hat{\Upsilon}_{AS} = \hat{\sigma}_{AS}(c)$, which indicates a property of state $\hat{\sigma}_{AS}$ that the measurement outcome on Z basis $\{|0\rangle_{A,l}, |1\rangle_{A,l}\}$ always coincides with the parity of photon number in the l-th pulse.

iii) From Eq. (C.6), we have

$$\hat{R}(c) = \Big(\bigotimes_{l=0}^{L-1} i^{\,lc\hat{m}_l}\Big)\hat{R}(0). \tag{C.8}$$

Comparing Eqs. (5.14) and (5.28) to Eqs. (C.7) and (C.8), we see that the derived properties of Eqs. (5.26), (5.30), and (5.32) for $|\Psi(c)\rangle_{AS}$ should also hold for $\hat{R}(c)$. As a result, we obtain

$$ {}_A\langle \mathcal{A}^{(0,j)}_{a,\{z_l\}}|\, \hat{N}_m \hat{R}(0) = (-i)^{u(j)}\, {}_A\langle \mathcal{A}^{(1,j)}_{a,\{z_l\}}|\, \hat{N}_m \hat{R}(1) \quad \text{for} \quad \sum_{l\neq j} z_l = m \tag{C.9} $$

as a generalization of Eq. (5.33). From Eq. (C.9), we have

$$ {}_A\langle \mathcal{A}^{(0,j)}_{a,\{z_l\}}|\, \hat{N}_m \hat{\sigma}_{AS}(0) \hat{N}_m\, |\mathcal{A}^{(0,j)}_{a,\{z_l\}}\rangle_A = {}_A\langle \mathcal{A}^{(1,j)}_{a,\{z_l\}}|\, \hat{N}_m \hat{\sigma}_{AS}(1) \hat{N}_m\, |\mathcal{A}^{(1,j)}_{a,\{z_l\}}\rangle_A \quad \text{for} \quad \sum_{l\neq j} z_l = m, \tag{C.10} $$

which assures that Eq. (B.2) is also true when $\hat{\sigma}_{AS}(c)$ is given by Eq. (C.3). Hence, Eq. (5.34) holds.

iv) For the initial state given by Eq. (C.3), the definition of the parameter r_{tag} of Eq. (5.40) is replaced by

$$ r_{\text{tag}} = 1 - \sum_m \text{tr}\left((\hat{\Pi}^{(m)}_A \otimes \hat{N}_m) \hat{\sigma}_{AS}(0) \right). \tag{C.11} $$

Together with Eqs. (5.41) and (C.7), we have

$$ r_{\text{tag}} = 1 - \sum_m \text{tr}\left((\hat{\mathbb{1}}_A \otimes \hat{\Pi}^{(m)}_S) \hat{\sigma}_{AS}(0) \right) = 1 - \sum_m \text{tr}\left(\hat{\Pi}^{(m)}_S \hat{\sigma}_S \right). \tag{C.12} $$

Appendix D

Calibration of light sources

Here we discuss how we may determine an upper bound on the parameter r_{tag}, which is given by Eq. (C.12), from an off-line experiment on the light source. We use a beam splitter characterized by transmittance T and reflectance R and two threshold detectors with quantum efficiencies $\eta_{\text{det}}^{(1)}$ and $\eta_{\text{det}}^{(2)}$, as in Fig. 3. No precise values of these parameters are needed, and we assume that there are known lower bounds $\eta_1 \leq T\eta_{\text{det}}^{(1)}$ and $\eta_2 \leq R\eta_{\text{det}}^{(2)}$. For simplicity, we neglect the effect of dark countings of the detectors. We assume that the dead time of the detectors are shorter than the pulse interval such that they are ready for every incident pulse. For an L pulse train emitted from the source, we record the timings of detection at the two detectors, and define a double coincidence event to be the case when both detectors have reported detections within a pair of neighboring pulses.

Since a state in the range of $\hat{\mathbb{1}} - \sum_m \hat{\Pi}_S^{(m)}$ contains at least two photons in a pair of neighboring pulses, such a state has a probability of resulting in a double coincidence event no smaller than $2\eta_1\eta_2$. Thus, if we repeat the measurement n_{test} times and find that double coincidence events have occurred n_{double} times, an upper bound on r_{tag} is given by

$$\bar{r}_{\text{tag}} := \frac{n_{\text{double}}}{n_{\text{test}}} \frac{1}{2\eta_1\eta_2} \geq r_{\text{tag}}, \tag{D.1}$$

in the asymptotic limit of large n_{test}. Although the tightness of the upper bound $\bar{r}_{\text{tag}}$ varies depending on the state $\hat{\sigma}_S$ in general, we may show that it can be quite tight when the state is close to an ideal coherent state. Suppose that η_1 and η_2 are equal to the actual efficiencies, and each pulse is exactly in the coherent state with amplitude μ. For every pulse, detector 1 and 2 independently report detection with probability $p_k^{(\text{click})} = 1 - e^{-\eta_k\mu} \leq \eta_k\mu$ $(k = 1, 2)$. Since there are $L + 2(L-1)$ different combinations of timings leading to double coincidence, we have

$$\frac{n_{\text{double}}}{n_{\text{test}}} \leq (3L-2)p_1^{(\text{click})}p_2^{(\text{click})} \leq \eta_1\eta_2\mu^2(3L-2), \tag{D.2}$$

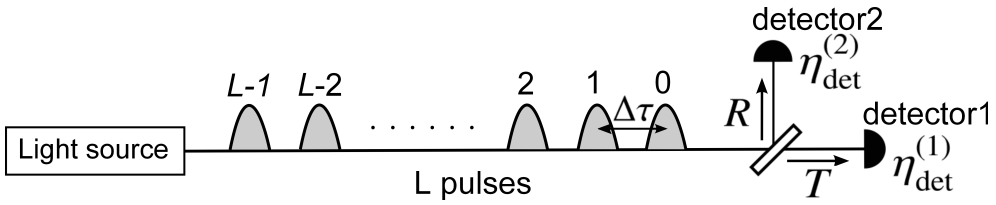

Figure D.1: Off-line calibration setup to determine an upper bound on $r_{\rm tag}$ for a general light source, when the dead time of detectors is shorter than pulse interval $\Delta\tau$. R and T represent reflectance and transmittance of the beam splitter, respectively. $\eta_{\rm det}^{(1)}$ and $\eta_{\rm det}^{(2)}$ represent detection efficiencies of detector 1 and 2, respectively.

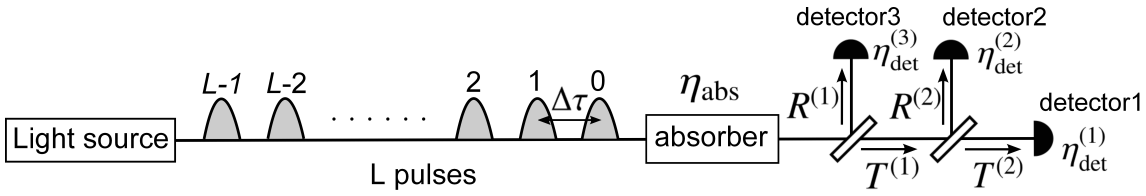

Figure D.2: Off-line calibration setup to determine an upper bound on $r_{\rm tag}$ for a general light source, when the dead time of detectors is longer than pulse interval $\Delta\tau$. An optical linear absorber with transmittance $\eta_{\rm abs}$ is set in front of beam splitters. $R^{(1)}$, $R^{(2)}$, $T^{(1)}$ and $T^{(2)}$ represent reflectance and transmittance of the two beam splitters. $\eta_{\rm det}^{(1)}$, $\eta_{\rm det}^{(2)}$ and $\eta_{\rm det}^{(3)}$ represent detection efficiencies of threshold detector 1, 2 and 3, respectively.

which leads to

$$\bar{r}_{\rm tag} \le \frac{\mu^2(3L-2)}{2}. \tag{D.3}$$

On the other hand, direct calculation shows that, in the limit of $L\mu^2 \to 0$,

$$\begin{aligned} r_{\rm tag} &= \mu^2\frac{3L-2}{2} + \mu^3\Big(\frac{-10L+12}{3}\Big) + \mu^4\Big(\frac{-9L^2+82L-120}{8}\Big) + O(L^2\mu^5 + L^3\mu^6) \\ &= \mu^2\frac{3L-2}{2} - \mu^3 L\Big(\frac{9}{8}\mu L + \frac{10}{3}\Big) + O(L^2\mu^5 + L^3\mu^6), \end{aligned} \tag{D.4}$$

which leads to

$$\frac{\bar{r}_{\rm tag} - r_{\rm tag}}{r_{\rm tag}} \le \mu\Big(\frac{3}{4}\mu L + \frac{20}{9}\Big) + O(L\mu^3 + L^2\mu^4). \tag{D.5}$$

Hence, the bound $\bar{r}_{\rm tag}$ is a good approximation of $r_{\rm tag}$ for $\mu \ll L^{-1/2}$.

In a more practical case where the dead time ($\tau_{\rm dead}$) of the detectors is longer than the pulse interval ($\tau_{\rm dead} > \Delta\tau$), there is a possibility that the presence of two photons is masked by an earlier detection of a third photon. In such a case, we may use a setup in Fig. 4 with three detectors and a linear absorber with transmittance $\eta_{\rm abs}$. Assume that we know lower bounds, $\tilde{\eta}_{\rm abs} \le \eta_{\rm abs}$, $\tilde{\eta}_1 \le T^{(1)}T^{(2)}\eta_{\rm det}^{(1)}$, $\tilde{\eta}_2 \le T^{(1)}R^{(2)}\eta_{\rm det}^{(2)}$ and $\tilde{\eta}_3 \le R^{(1)}\eta_{\rm det}^{(3)}$. Define a triple coincidence event to be the case when all three detectors has reported detections within the whole train of L pulses. Let q_3 be the probability that the L pulse train leaving the linear absorber contains three or more photons. If we repeat the measurement $n_{\rm test}$ times and triple coincidence events have occurred $n_{\rm triple}$ times, we have

$$q_3 \le \frac{n_{\rm triple}}{n_{\rm test}}\frac{1}{6\tilde{\eta}_1\tilde{\eta}_2\tilde{\eta}_3} \tag{D.6}$$

in the limit of large $n_{\rm test}$. Suppose that one records the number $n_{\rm double}^{\rm (obs)}$ of double coincidence events in the same $n_{\rm test}$ runs, which is defined as the case when detectors 1 and 2 have reported detections within a pair of neighboring pulses. Since the effect of the dead time can be simulated with a fictitious detector with no dead time by ignoring detection events that occurred when the real detector would have been dead, we may consider the number $n_{\rm double}^{\rm (true)}$ of double coincidence events defined from these fictitious detectors. Since the two definitions of a double coincidence event differs only when three or more photons are incident on the two detectors, we have

$$\frac{n_{\rm double}^{\rm (true)}}{n_{\rm test}} \le \frac{n_{\rm double}^{\rm (obs)}}{n_{\rm test}} + q_3 \tag{D.7}$$

in the limit of large $n_{\rm test}$. On the other hand, as in Eq. (D.1), $n_{\rm double}^{\rm (true)}$ satisfies

$$r_{\rm tag} \le \bar{r}_{\rm tag} = \frac{n_{\rm double}^{\rm (true)}}{n_{\rm test}}\frac{1}{2\eta_1\eta_2} \tag{D.8}$$

by taking $\eta_1 = \tilde{\eta}_{\rm abs}\tilde{\eta}_1$ and $\eta_2 = \tilde{\eta}_{\rm abs}\tilde{\eta}_2$. We thus obtain an upper bound from Eqs. (D.6)-(D.8) as

$$r_{\rm tag} \leq \bar{r}^{*}_{\rm tag} := \Big(\frac{n^{\rm (obs)}_{\rm double}}{n_{\rm test}} + \frac{n_{\rm triple}}{n_{\rm test}}\frac{1}{6\tilde{\eta}_1\tilde{\eta}_2\tilde{\eta}_3}\Big)\frac{1}{2\tilde{\eta}_1\tilde{\eta}_2\tilde{\eta}^2_{\rm abs}}. \tag{D.9}$$

We show that $\bar{r}^{*}_{\rm tag}$ also approximates $r_{\rm tag}$ well when the light source emits coherent pulses. Suppose that $\tilde{\eta}_1$, $\tilde{\eta}_2$, $\tilde{\eta}_3$ and $\tilde{\eta}_{\rm abs}$ are equal to the actual efficiencies. Since $n^{\rm (obs)}_{\rm double} \leq n^{\rm (true)}_{\rm double}$ holds, we have

$$\bar{r}^{*}_{\rm tag} \leq \bar{r}_{\rm tag} + \frac{n_{\rm triple}}{n_{\rm test}}\frac{1}{6\tilde{\eta}_1\tilde{\eta}_2\tilde{\eta}_3}\frac{1}{2\tilde{\eta}_1\tilde{\eta}_2\tilde{\eta}^2_{\rm abs}}. \tag{D.10}$$

From Eq. (D.5), we have

$$\frac{\bar{r}^{*}_{\rm tag} - r_{\rm tag}}{r_{\rm tag}} \leq \mu\Big(\frac{3}{4}\mu L + \frac{20}{9}\Big) + \frac{n_{\rm triple}}{n_{\rm test}}\frac{1}{6\tilde{\eta}_1\tilde{\eta}_2\tilde{\eta}_3}\frac{1}{2\tilde{\eta}_1\tilde{\eta}_2\tilde{\eta}^2_{\rm abs}}\frac{1}{r_{\rm tag}} + O(L\mu^3 + L^2\mu^4) \tag{D.11}$$

for $L\mu^2 \to 0$. Since L pulses incident on detector k lead to one or more detections at probability $p^{\rm (click)}_k = 1 - e^{-\tilde{\eta}_k\tilde{\eta}_{\rm abs}L\mu} \leq \tilde{\eta}_k\tilde{\eta}_{\rm abs}L\mu$, we have

$$\frac{n_{\rm triple}}{n_{\rm test}} \leq \tilde{\eta}_1\tilde{\eta}_2\tilde{\eta}_3(\tilde{\eta}_{\rm abs}L\mu)^3. \tag{D.12}$$

Thus, we obtain

$$\begin{aligned}\frac{\bar{r}^{*}_{\rm tag} - r_{\rm tag}}{r_{\rm tag}} &\leq \mu\Big(\frac{3}{4}\mu L + \frac{20}{9}\Big) + \frac{(\tilde{\eta}_{\rm abs}L\mu)^3}{12\tilde{\eta}_1\tilde{\eta}_2\tilde{\eta}^2_{\rm abs}}\frac{1}{r_{\rm tag}} + O(L\mu^3 + L^2\mu^4) \\ &= \mu\Big(\frac{3}{4}\mu L + \frac{20}{9}\Big) + \mu\frac{\tilde{\eta}_{\rm abs}L^2}{18\tilde{\eta}_1\tilde{\eta}_2} + O(L\mu^3 + L^2\mu^4).\end{aligned} \tag{D.13}$$

Therefore, $\bar{r}^{*}_{\rm tag}$ becomes a good approximation of $r_{\rm tag}$ when $\mu \ll L^{-1/2}$ and the absorber is chosen to satisfy $\tilde{\eta}_{\rm abs}\mu \ll L^{-2}$.

Bibliography

[1] P. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM J. Cmput.* **26**, 1484 (1997).

[2] C. E. Shannon, "Communication theory of secrecy systems," *Bell system technical journal* **28**, 656 (1949).

[3] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India (IEEE Press, New York, 1984), Vol. 175.

[4] C. H. Bennett, G. Brassard, and J.-M. Robert, "Privacy Amplification by Public Discussion," *SIAM J. Comput.* **17**, 210 (1988).

[5] D. Mayers, "Quantum key distribution and string obvious transfer in noisy channels," *Lect. Notes Comput. Sci.* **1109**, 343 (1996).

[6] P. W. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Phys. Rev. Lett.* **85**, 441 (2000).

[7] H.-K. Lo and H. F. Chau, "Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances," *Science* **283**, 2050 (1999).

[8] G. Brassard, N. Lütkenhaus, T. Mor, and B. Sanders, "Limitations on Practical Quantum Cryptography," *Phy. Rev. Lett.* **85**, 1330 (2000).

[9] H. Inamori, N. Lütkenhaus, and D. Mayers, "Unconditional Security of Practical Quantum Key Distribution," arXiv:quant-ph/0107017 (2001).

[10] D. Gottesman, H.-K. Lo, J. Preskill, and N. Lütkenhaus, "Security of quantum key distribution with imperfect devices," *Quant. Info. Compu.* **5**, 325 (2004).

[11] M. Koashi, "Simple security proof of quantum key distribution via uncertainty principle," arXiv:quant-ph/0505108 (2005).

[12] M. Koashi, "Simple security proof of quantum key distribution based on complementarity," *New J. Phy.* **11**, 045018 (2009).

[13] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography," *Nature Communications* **3**, 634 (2012).

[14] M. Koashi, "Efficient quantum key distribution with practical sources and detectors," arXiv:quant-ph/0609180 (2006).

[15] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, "Concise security bounds for practical decoy-state quantum key distribution," *Phys. Rev. A* **89**, 022307 (2014).

[16] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, "Finite-key analysis for measurement-device-independent quantum key distribution," *Nature Commun ications* **5**, 3732 (2014).

[17] A. Mizutani, M. Curty, C. C. W. Lim, N. Imoto, and K. Tamaki, "Finite-key security analysis of quantum key distribution with imperfect light sources," *New Journal of Physics* **17**, 093011 (2015).

[18] M. Hayashi, "Practical evaluation of security for quantum key distribution," *Phys. Rev. A* **74**, 022307 (2006).

[19] M. Hayashi, "Upper bounds of eavesdropper's performances in finite-length code with the decoy method," *Phys. Rev. A* **76**, 012329 (2007).

[20] R. Renner and R. Konig, in *Theory of Cryptography, Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12, 2005, Proceedings*, Vol. 3378 of *Lecture Notes in Computer Science* (Springer, ADDRESS, 2005), pp. 407–425.

[21] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, in *Theory of Cryptography, Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12, 2005, Proceedings*, Vol. 3378 of *Lecture Notes in Computer Science* (Springer, ADDRESS, 2005), pp. 386–406.

[22] V. Scarani and R. Renner, "Quantum Cryptography with Finite Resources: Unconditional Security Bound for Discrete-Variable Protocols with One-Way Postprocessing," *Phys. Rev. Lett.* **100**, 200501 (2008).

[23] R. Y. Q. Cai and V. Scarani, "Finite-key analysis for practical implementations of quantum key distribution," *New Journal of Physics* **11**, 045024 (2009).

[24] M. Hayashi and R. Nakayama, "Security analysis of the decoy method with the Bennett-Brassard 1984 protocol for finite key lengths," *New Journal of Physics* **16**, 063009 (2014).

[25] K. Azuma, "Weighted sums of certain dependent random variables," *Tohoku Math. J.* **19**, 357 (1967).

[26] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, "The SECOQC quantum key distribution network in Vienna," *New Journal of Physics* **11**, 075001 (2009).

[27] F. Xu, W. Chen, S. Wang, Z. Yin, Y. Zhang, Y. Liu, Z. Zhou, Y. Zhao, H. Li, D. Liu, Z. Han, and G. Guo, "Field Experiment on a Robust Hierarchical Metropolitan Quantum Cryptography Network," arXiv:quant-ph/0906.3576 (2009).

[28] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, "Field test of quantum key distribution in the Tokyo QKD Network," *Opt. Express* **19**, 10387 (2011).

[29] S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter, "Experimental Satellite Quantum Communications," *Nature Photonics* **7**, 382 (2013).

[30] J.-Y. Wang, B. Yang, S.-K. Liao, L. Zhang, Q. Shen, X.-F. Hu, J.-C. Wu, S.-J. Yang, H. Jiang, Y.-L. Tang, B. Zhong, H. Liang, W.-Y. Liu, Y.-H. Hu, Y.-M. Huang, B. Qi, J.-G. Ren, G.-S. Pan, J. Yin, J.-J. Jia, Y.-A. Chen, K. Chen, C.-Z. Peng, and J.-W. Pan, "Direct and full-scale experimental verifications towards ground-satellite quantum key distribution," *Nature Photonics* **7**, 387 (2013).

[31] G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, "Experimental Satellite Quantum Communications," *Phys. Rev. Lett.* **115**, 040502 (2015).

[32] C. Marand and P. D. Townsend, "Quantum key distribution over distances as long as 30 km," *Opt. Lett.* **20**, 1695 (1995).

[33] C. Gobby, Z. L. Yuan, and A. J. Shields, "Quantum key distribution over 122 km of standard telecom fiber," *Applied Physics Letters* **84**, (2004).

[34] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, "Long-Distance Decoy-State Quantum Key Distribution in Optical Fiber," *Phys. Rev. Lett.* **98**, 010503 (2007).

[35] M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Efficient decoy-state quantum key distribution with quantified security," *Opt. Express* **21**, 24550 (2013).

[36] W.-Y. Hwang, "Quantum Key Distribution with High Loss: Toward Global Secure Communication," *Phys. Rev. Lett.* **91**, 057901 (2003).

[37] X.-B. Wang, "Decoy-state protocol for quantum cryptography with four different intensities of coherent light," *Phys. Rev. A* **72**, 012322 (2005).

[38] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.* **94**, 230504 (2005).

[39] X.-B. Wang, L. Yang, C.-Z. Peng, and J.-W. Pan, "Decoy-state quantum key distribution with both source errors and statistical fluctuations," *New Journal of Physics* **11**, 075006 (2009).

[40] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, "Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors," *Nature Photonics* **1**, 343 (2007).

[41] T. Sasaki, Y. Yamamoto, and M. Koashi, "Practical quantum key distribution protocol without monitoring signal disturbance," *Nature* **509**, 475 (2014).

[42] J.-Y. Guan, Z. Cao, Y. Liu, G.-L. Shen-Tu, J. S. Pelc, M. M. Fejer, C.-Z. Peng, X. Ma, Q. Zhang, and J.-W. Pan, "Experimental Passive Round-Robin Differential Phase-Shift Quantum Key Distribution," *Phys. Rev. Lett.* **114**, 180502 (2015).

[43] H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi, "Experimental quantum key distribution without monitoring signal disturbance," *Nature Photonics* **9**, 827 (2015).

[44] Y.-H. Li, Y. Cao, H. Dai, J. Lin, Z. Zhang, W. Chen, Y. Xu, J.-Y. Guan, S.-K. Liao, J. Yin, Q. Zhang, X. Ma, C.-Z. Peng, and J.-W. Pan, "Experimental round-robin differential phase-shift quantum key distribution," *Phys. Rev. A* **93**, 030302 (2016).

[45] S. Wang, Z.-Q. Yin, W. Chen, D.-Y. He, X.-T. Song, H.-W. Li, L.-J. Zhang, Z. Zhou, G.-C. Guo, and Z.-F. Han, "Experimental demonstration of a quantum key distribution without signal disturbance monitoring," *Nature Photonics* **9**, 832 (2015).

[46] K. Inoue and Y. Iwai, "Differential-quadrature-phase-shift quantum key distribution," *Phys. Rev. A* **79**, 022319 (2009).

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

[48] D. Bruß, "Optimal Eavesdropping in Quantum Cryptography with Six States," *Phys. Rev. Lett.* **81**, 3018 (1998).

[49] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, "Quantum Cryptography Using Entangled Photons in Energy-Time Bell States," *Phys. Rev. Lett.* **84**, 4737 (2000).

[50] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, "Security of Quantum Key Distribution Using *d*-Level Systems," *Phys. Rev. Lett.* **88**, 127902 (2002).

[51] F. Grosshans and P. Grangier, "Continuous Variable Quantum Cryptography Using Coherent States," *Phys. Rev. Lett.* **88**, 057902 (2002).

[52] A. Uhlmann, "The " transition probability " in the state space of a $*$-algebra," *Reports on Mathematical Physics* **9**, 273 (1976).

[53] K. Takemoto, Y. Nambu, T. Miyazawa, Y. Sakuma, T. Yamamoto, S. Yorozu, and Y. Arakawa, "Quantum key distribution over 120km using ultrahigh purity single-photon source and superconducting single-photon detectors," *Scientific Reports* **5**, 14383 (2015).

[54] Y. Adachi, T. Yamamoto, M. Koashi, and N. Imoto, "Simple and Efficient Quantum Key Distribution with Parametric Down-Conversion," *Phys. Rev. Lett.* **99**, 180503 (2007).

[55] X. Ma and H.-K. Lo, "Quantum key distribution with triggering parametric down-conversion sources," *New Journal of Physics* **10**, 073018 (2008).

[56] IDQuantique: http://www.idquantique.com/ .

[57] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, "Ultrafast quantum random number generation based on quantum phase fluctuations," *Opt. Express* **20**, 12366 (2012).

[58] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam, "Detecting single infrared photons with 93% system efficiency," *Nature Photonics* **7**, 210 (2013).

[59] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, "Time-shift attack in practical quantum cryptosystems," arXiv:quant-ph/0512080 (2005).

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

[61] 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* **12**, 113026 (2010).

[62] S. Sajeed, P. Chaiwongkhot, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, "Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch," *Phys. Rev. A* **91**, 062301 (2015).

[63] H.-K. Lo, M. Curty, and B. Qi, "Measurement-Device-Independent Quantum Key Distribution," *Phys. Rev. Lett.* **108**, 130503 (2012).

[64] J.-P. Bourgoin, E. Meyer-Scott, B. L. Higgins, B. Helou, C. Erven, H. Hübel, B. Kumar, D. Hudson, , I. D'Souza, R. Girard, R. Laflamme, and T. Jennewein, "A comprehensive design and performance analysis of low Earth orbit satellite quantum communication," *New J. Phys.* **15**, 023006 (2013).

[65] M. Wegman and L. Carter, "New Hash Functions and Their Use in Authentication and Set Equality," *J. Comp. Sys. Sci.* **22**, 265 (1981).

[66] C. Pfister, N. Lutkenhaus, S. Wehner, and P. J. Coles, "Sifting attacks in finite-size quantum key distribution," *New Journal of Physics* **18**, 053001 (2016).

[67] R. G. Gallager, "Low Density Parity Check Codes," *Ph.D Thesis* (1963).

[68] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized Privacy Amplification," *IEEE Trans. Inf. Theory* **41**, 1915 (1995).

[69] J. Carter and M. N. Wegman, "Universal classes of hash functions," *Journal of Computer and System Sciences* **18**, 143 (1979).

[70] M. Hayashi and T. Tsurumaru, "More Efficient Privacy Amplification With Less Random Seeds via Dual Universal Hash Function," *IEEE Transactions on Information Theory* **62**, 2213 (2016).

[71] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, "Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction," *Phys. Rev. A* **87**, 062327 (2013).

[72] R. Canetti, in *Proceedings of the 42nd IEEE Symposium on Foundations of Computer Science, FOCS '01* (IEEE Computer Society, Washington, DC, USA, 2001), pp. 136–145.

[73] M. Ben-Or and D. Mayers, "General Security Definition and Composability for Quantum Classical Protocols," arXiv:quant-ph/0409062 (2004).

[74] D. Unruh, "Simulatable security for quantum protocols," arXiv:quant-ph/0409125 (2004).

[75] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, "Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security against Coherent Attacks," *Phys. Rev. Lett.* **109**, 100502 (2012).

[76] M. Lucamarini, J. F. Dynes, B. Fröhlich, Z. Yuan, and A. J. Shields, "Security Bounds for Efficient Decoy-State Quantum Key Distribution," *IEEE Journal of Selected Topics in Quantum Electronics* **21**, 197 (2015).

[77] J. Müller-Quade and R. Renner, "Composability in quantum cryptography," *New Journal of Physics* **11**, 085006 (2009).

[78] T. Cover and J. Thomas, "Elements of Information Theory," *Wiley Series in Telecommunications* (Wiley, New York, 1991) .

[79] R. König, R. Renner, A. Bariska, and U. Maurer, "Small Accessible Quantum Information Does Not Imply Security," *Phys. Rev. Lett.* **98**, 140502 (2007).

[80] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Phys. Rev. Lett.* **68**, 557 (1992).

[81] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, "Concentrating partial entanglement by local operations," *Phys. Rev. A* **53**, 2046 (1996).

[82] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, "Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels," *Phys. Rev. Lett.* **76**, 722 (1996).

[83] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction," *Phys. Rev. A* **54**, 3824 (1996).

[84] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A* **54**, 1098 (1996).

[85] A. Steane, "Multiple-Particle Interference and Quantum Error Correction," *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences* **452**, 2551 (1996).

[86] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.* **68**, 3121 (1992).

[87] K. Tamaki, M. Koashi, and N. Imoto, "Security of the Bennett 1992 quantum-key distribution protocol against individual attack over a realistic channel," *Phys. Rev. A* **67**, 032310 (2003).

[88] H.-K. Lo, "Proof of unconditional security of six-state quantum key distribution scheme," *Quant. Inform. Comput.* **1**, 81 (2001).

[89] K. Inoue, E. Waks, and Y. Yamamoto, "Differential Phase Shift Quantum Key Distribution," *Phys. Rev. Lett.* **89**, 037902 (2002).

[90] K. Tamaki, M. Koashi, and G. Kato, "Unconditional security of coherent-state-based differential phase shift quantum key distribution protocol with block-wise phase randomization," arXiv:quant-ph/1208.1995 (2012).

[91] M. Tomamichel and R. Renner, "Uncertainty Relation for Smooth Entropies," *Phys. Rev. Lett.* **106**, 110506 (2011).

[92] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, "Leftover Hashing Against Quantum Side Information," *IEEE Transactions on Information Theory* **57**, 5524 (2011).

[93] T. Tsurumaru and K. Tamaki, "Security proof for quantum-key-distribution systems with threshold detectors," *Phys. Rev. A* **78**, 032302 (2008).

[94] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, "Squashing Models for Optical Measurements in Quantum Communication," *Phys. Rev. Lett.* **101**, 093601 (2008).

[95] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, "Loss-tolerant quantum cryptography with imperfect sources," *Phys. Rev. A* **90**, 052314 (2014).

[96] F. Xu, K. Wei, S. Sajeed, S. Kaiser, S. Sun, Z. Tang, L. Qian, V. Makarov, and H.-K. Lo, "Experimental quantum key distribution with source flaws," *Phys. Rev. A* **92**, 032305 (2015).

[97] A. Mizutani, N. Imoto, and K. Tamaki, "Robustness of the round-robin differential-phase-shift quantum-key-distribution protocol against source flaws," *Phys. Rev. A* **92**, 060303 (2015).

[98] T. Moroder, M. Curty, C. C. W. Lim, L. P. Thinh, H. Zbinden, and N. Gisin, "Security of Distributed-Phase-Reference Quantum Key Distribution," *Phys. Rev. Lett.* **109**, 260501 (2012).

[99] H.-K. Lo and J. Preskill, "Security of Quantum Key Distribution Using Weak Coherent States with Nonrandom Phases," *Quantum Info. Comput.* **7**, 431 (2007).

[100] Z. Cao, Z. Zhang, H.-K. Lo, and X. Ma, "Discrete-phase-randomized coherent state source and its application in quantum key distribution," *New Journal of Physics* **17**, 053014 (2015).

[101] T. Kobayashi, A. Tomita, and A. Okamoto, "Evaluation of the phase randomness of a light source in quantum-key-distribution systems with an attenuated laser," *Phys. Rev. A* **90**, 032320 (2014).

[102] 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 multiwavelength sources," *Phys. Rev. A* **84**, 062308 (2011).

[103] EpiPhotonics: http://epiphotonics.com/index.html .

[104] H.-K. Lo, X. Ma, and K. Chen, "Decoy State Quantum Key Distribution," *Phys. Rev. Lett.* **94**, 230504 (2005).

[105] K. Tamaki, H.-K. Lo, C.-H. F. Fung, and B. Qi, "Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw," *Phys. Rev. A* **85**, 042307 (2012).

[106] J. Mower, Z. Zhang, P. Desjardins, C. Lee, J. H. Shapiro, and D. Englund, "High-dimensional quantum key distribution using dispersive optics," *Phys. Rev. A* **87**, 062322 (2013).

[107] Z. Zhang, J. Mower, D. Englund, F. N. C. Wong, and J. H. Shapiro, "Unconditional Security of Time-Energy Entanglement Quantum Key Distribution Using Dual-Basis Interferometry," *Phys. Rev. Lett.* **112**, 120506 (2014).

[108] K.-I. Yoshino, M. Fujiwara, K. Nakata, A. Tomita, and A. Tajima, "Secure Quantum Key Distribution Against Pattern Effects of Optical Pulse Intensities," Poster presentation at QCrypt 2016 .

[109] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations," *Phys. Rev. Lett.* **92**, 057901 (2004).

[110] M. Koashi, "Unconditional Security of Coherent-State Quantum Key Distribution with a Strong Phase-Reference Pulse," *Phys. Rev. Lett.* **93**, 120501 (2004).

[111] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," *Applied Physics Letters* **87**, 194108 (2005).

[112] M. Pawlowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Zukowski, "Information causality as a physical principle," *Nature* **461**, 1101 (2009).

[113] Y. Wang, W.-S. Bao, C. Zhou, M.-S. Jiang, and H.-W. Li, "Tight finite-key analysis of a practical decoy-state quantum key distribution with unstable sources," *Phys. Rev. A* **94**, 032335 (2016).

[114] K. Tamaki, H.-K. Lo, A. Mizutani, G. Kato, C. C. W. Lim, K. Azuma, and M. Curty, "Security of quantum key distribution with iterative sifting," arXiv:1610.06499 (2016).

[115] H.-K. Lo, H. Chau, and M. Ardehali, "Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security," *Journal of Cryptology* **18**, 133 (2004).

[116] W. Hoeffding, "Probability Inequalities for Sums of Bounded Random Variables," *Journal of the American Statistical Association* **58**, 13 (1963).

[117] J. H. Ahrens, in *Ökonomie und Mathematik: Rudolf Henn zum 65. Geburtstag*, edited by O. Opitz and B. Rauhut (Springer Berlin Heidelberg, Berlin, Heidelberg, 1987), pp. 253–265.

[118] H. Chernoff, "A Measure of Asymptotic Efficiency for Tests of a Hypothesis Based on the sum of Observations," *Ann. Math. Stat.* **23**, 493 (1952).

[119] T. Zhong, H. Zhou, R. D. Horansky, C. Lee, V. B. Verma, A. E. Lita, A. Restelli, J. C. Bienfang, R. P. Mirin, T. Gerrits, S. W. Nam, F. Marsili, M. D. Shaw, Z. Zhang, L. Wang, D. Englund, G. W. Wornell, J. H. Shapiro, and F. N. C. Wong, "Photon-efficient quantum key distribution using time-energy entanglement with high-dimensional encoding," *New Journal of Physics* **17**, 022002 (2015).