The Error Tolerance Bound for Secure Multi-Qubit QKD Against Incoherent Attack

Kyongchun Lim, Heasin Ko, Kiung Kim, Changho Suh, *Member, IEEE*, and June-Koo Kevin Rhee, *Member, IEEE*

***Abstract*—The tolerance bound for quantum symbol error rate in a multi-qubit quantum key distribution system is derived in consideration of an incoherent attack on a single-photon quantum channel, where multi-qubit encoding and measurement can be applied to a single photon in combination of polarization, phase, and frequency modulations. This paper presents a solid theoretical evidence of a multiqubit gain in secrecy performance.**

***Index Terms*—Protocols, public key cryptography, quantum theory, security, wire communications.**

I. Introduction

Unconditional secure communication has been sought for decades and the most critical advancement for a practical application has been achieved for the last several years as the internet transports sensitive information over the public domain. Quantum key distribution (QKD) has been proved to be unconditionally secure in the presence of unauthenticated third parties. Recently, several QKD field tests [1]–[6] have demonstrated meaningful application results that can be immediately extended for commercialization of QKD services in the near future.

A pioneering work on QKD protocols is reported by Bennett and Brassard. In 1984, they developed a QKD protocol widely known as the BB84 protocol [7]. This protocol uses four different quantum states for QKD. The states are represented as $|0\rangle$, $|1\rangle$, $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. The former two and the latter two can be measured as pure states in two different bases, respectively. In the BB84 protocol, Alice transmits a sequence of qubits, each in a single photon, to Bob, where each is encoded with one of the four quantum states. Bob measures the state of each photon with a random choice of one of the two bases. After the transmission of the whole sequence and measurements, they share the basis information selected for generation and measurement of the qubit state of each photon through an authenticated classical channel. Comparing basis information, they perform a process, called sifting, which discards qubits for which Alice and Bob used different bases. Subsequently, they perform error estimation to determine the presence of Eve and abort protocol if the error rate is higher than a threshold value called the *error tolerance bound*. If they get allowable error rate, they perform an additional process, called post-processing, which consists of *error correction* and *privacy amplification* [8]. This final process leads to obtaining the secret key of interest.

An error rate can reflect the presence of eavesdropper especially when the error event is mainly due to Eve's attack on the quantum channel. In this work, we focus on this simple scenario in which the Eve's attack is the major source of the error. For simplicity, we assume that a quantum channel does not contain any error source, e.g., channel impairments occurred in fiber transmission and single photon state measurement. Under the BB84 protocol, the error tolerance bounds were investigated for two models on Eve's attack strategy: (1) intercept-and-resend attack; (2) the optimal incoherent attack aided by an approximate quantum cloning machine [9]. It has been shown that the error tolerance bounds are 25% and 14.9% under the two attack models respectively.

It is known in [10] that employing more quantum states for QKD enables a higher error tolerance bound. The authors in [10] consider a QKD protocol that uses six states with three bases. In this protocol, they observed that more quantum states induce additional uncertainty in Eve's guess on the encoded states, and this contributes to increasing the error tolerance bounds. Specifically, they considered a six-state protocol which uses the two additional quantum states: $\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$, $\frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$, and showed that the protocol can tolerate 1/3 and 1/6 error rate for the above two attack models, respectively. These error tolerance bounds are the fundamental quantities that can provide guidelines as to how to design QKD systems that ensure secure communication.

Recently, an experimental trial of a two-qubit single-photon QKD has been reported yet with no discussion on the improvement of secrecy performance [11]. In this scheme, a single photon is encoded twice with two different coding schemes: polarization and phase coding. So in this protocol, a single photon carries two-qubit information. One can also extend this scheme to N-qubit QKD by incorporating more coding schemes such as frequency and spatial mode encodings. However, the achievable key rate has not been explored in consideration of the security bound. Moreover, the tolerable qubit-error-rate bound has not been characterized. In this paper, we provide the security proof of the N-qubit QKD protocol and derive the error tolerance

Manuscript received August 1, 2014; revised October 22, 2014; accepted October 31, 2014. This work was supported by the ICT R&D program of MSIP/IITP, Republic of Korea [2014-044-014-004. Development of core technology for the quantum cryptography].

K. Lim, H. Ko, K. Kim, and C. Suh are with the Department of Electrical Engineering, Korea Advanced Institute of Science and Technology, Daejeon 305-701, Korea (e-mail: lim.kc@kaist.ac.kr; ko.hs@kaist.ac.kr; kw0729@kaist.ac.kr; chsuh@kaist.ac.kr).

J.-K. K. Rhee is with the Graduate School of Information Security and the Department of Electrical Engineering, Korea Advanced Institute of Science and Technology, Daejeon 305-701, Korea (e-mail: rhee.jk@kaist.ac.kr).

Digital Object Identifier 10.1109/JSTQE.2014.2369498

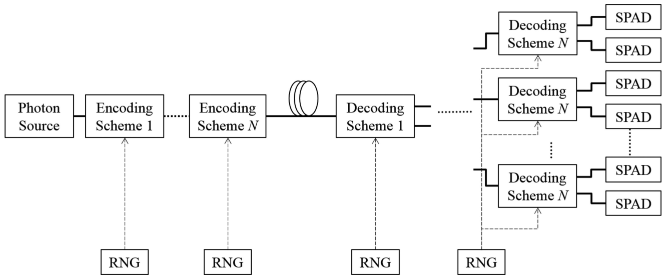

Fig. 1. N-qubit QKD system model.

TABLE I
STATE REPRESENTATIONS FOR TWO-QUBIT SYSTEM

		Scheme i
Basis Z	state 0	$\lvert q_{z0}\rangle_i = \lvert 0\rangle_z$
	state 1	$\lvert q_{z1}\rangle_i = \lvert 1\rangle_z$
Basis X	state 0	$\lvert q_{x0}\rangle_i = \frac{1}{\sqrt{2}}(\lvert q_{z0}\rangle_i + \lvert q_{z1}\rangle_i)$
	state 1	$\lvert q_{x1}\rangle_i = \frac{1}{\sqrt{2}}(\lvert q_{z0}\rangle_i - \lvert q_{z1}\rangle_i)$

$|q_{bs}\rangle_i$ represents a qubit encoded with scheme i where $b \in \{\mathrm{z}, \mathrm{x}\}$ and $s \in \{0, 1\}$ indicate indices for basis and state, respectively.

bound. As an attack model, we assume the optimal incoherent attack strategy.[1]

Related Work: Two protocols have been investigated for high-dimensional QKD systems in [12]. The first protocol consists of two bases, each having d states. The second protocol consists of non-orthogonal d bases (e.g., superposition transforms of $|0\rangle, |1\rangle$ and $|+\rangle, |-\rangle$ bases), and each basis has two states. It has been demonstrated that the second protocol outperforms the first one in terms of security. On the other hand, the multi-qubit protocol considered in this work uses different numbers of bases and states. Specifically in the protocol, a single photon is encoded with multiple independent coding schemes. So bases are orthogonal among different coding schemes, and the numbers of bases and states simultaneously increase with the number of employed coding schemes. We will also show that the multi-qubit protocol is more beneficial than those in [12] in the aspects of security and key rate.

The remaining parts of this paper are organized as follows. In Section II, we describe a multi-qubit QKD system and the considered attack model. For illustrative purpose, we focus on the two-qubit system and defer the general case to Appendix A. We derive the error tolerance bound and provide the proof in Sections III and IV respectively. The results are discussed in the simple two-qubit case and the general results are given in Appendix A. We conclude the paper in Section V.

II. Multi-Qubit QKD System

A. System Description

In a multi-qubit QKD system, the sender Alice employs multiple N independent coding schemes to encode a single photon such that it delivers multiple qubit information as in linear optical quantum computing [13]. Hence, the single photon can accommodate classical N-bit information. Fig. 1 depicts an N encoding and decoding scheme in Alice's and Bob's sides, respectively. Random choice of a basis and a state for each coding scheme can be performed by random number generators. Throughout the encoding part, Alice can transmit a photon containing N-bit information to Bob via optical fiber. The decoding part consists of decoders and 2^N single-photon avalanche diode (SPAD) detectors to distinguish states in a specific basis. Upon the reception of a photon, Bob measures an N-qubit state with random choices of bases as one of the SPADs detects a photon. Since each coding scheme has two bases and thus the total number of bases is 2^N, the security key rate normalized by the number of bases is $\frac{N}{2^N}$ after sifting as in BB84. The detailed discussion can be found in Section II-B.

One can be intrigued by this multi-qubit QKD system on the security proof: What is the tolerance of quantum errors against the most powerful type of attack by Eve? An incoherent attack can be considered as the most comprehensive attack model in which an approximate quantum cloning machine and quantum memory can be utilized for Eve to measure the mutual information between Alice and Bob during a sifting process. It is known that this attack can alter the quantum states of photons (intended for Bob) with the approximate cloning, thereby causing quantum errors in Bob's measurements. It has been broadly studied in the framework of the BB84 protocol. In a multi-qubit QKD system, this incoherent attack can break the security with different degrees. In this work, we find that an N-qubit QKD security analysis is rather straightforward once we understand an example of a two-qubit QKD model. A detailed analysis of a general N-qubit system is provided in Appendix A.

B. Two-Qubit QKD States

The property of each coding scheme in a multi-qubit QKD system is exactly the same as that of BB84. In the BB84 protocol, Alice encodes a qubit with one state from one of two bases, which are labeled as Z and X bases. Here the Z basis is a projection onto $|0\rangle$ and $|1\rangle$ while the X basis is a projection onto $|+\rangle$ and $|-\rangle$ states. In a two-qubit case, we use two sets of the aforementioned bases for each qubit. For simplicity, we label the two encoding schemes as scheme 1 and scheme 2. Since these schemes are independent, it is possible to acquire two-bit information from a single photon with only one measurement. In this sense, a qubit encoded with two coding schemes can be considered as two qubits. Thus, a single photon quantum state encoded twice with two independent coding schemes is represented as follows:

$$|\mathbf{Q}\rangle = |q_{bs}\rangle_1 \otimes |q_{bs}\rangle_2 . \tag{1}$$

Combining the two qubits with four states each (see Table I), a single photon quantum state can be in one of the following

[1] Since intercept-and-resend attack is known as a less powerful eavesdropping strategy than an optimal incoherent attack, we focus on investigating a more powerful attack that is an optimal incoherent attack. For an understanding of this eavesdropping strategy, a simple security analysis of intercept-and-resend attack is described in Appendix-B.

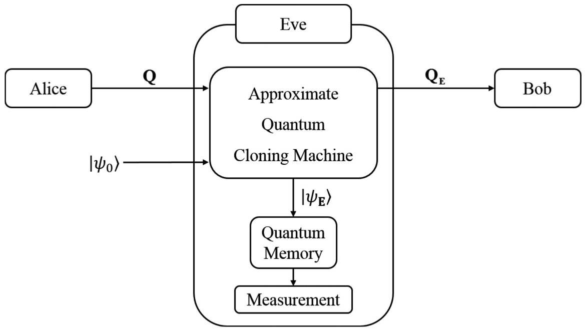

Fig. 2. Eve's system model including approximate quantum cloning machine and quantum memory.

16 states that can be measured in the four different bases in the tensor product space:

$$\begin{aligned}
\text{Basic ZZ}: &\quad |q_{z0}q_{z0}\rangle, |q_{z1}q_{z0}\rangle, |q_{z0}q_{z1}\rangle, |q_{z1}q_{z1}\rangle\\
\text{Basic XZ}: &\quad |q_{x0}q_{z0}\rangle, |q_{x1}q_{z0}\rangle, |q_{x0}q_{z1}\rangle, |q_{x1}q_{z1}\rangle\\
\text{Basic ZX}: &\quad |q_{z0}q_{x0}\rangle, |q_{z1}q_{x0}\rangle, |q_{z0}q_{x1}\rangle, |q_{z1}q_{x1}\rangle\\
\text{Basic XX}: &\quad |q_{x0}q_{x0}\rangle, |q_{x1}q_{x0}\rangle, |q_{x0}q_{x1}\rangle, |q_{x1}q_{x1}\rangle.
\end{aligned}$$

In the two-qubit QKD system , Alice and Bob perform the QKD procedures similar to the BB84 protocol using the above 16 states. First, Alice selects one of the four bases uniformly at random. Second, she chooses one of the four states uniformly at random within the chosen basis and transmits a single photon with the corresponding encoding to Bob via optical quantum channel. When Bob receives the photon from Alice, he selects one of the four bases uniformly at random for measurement. In turn, Alice and Bob perform the sifting process. Then the rest of post-processing is performed to obtain the final secret key.

C. Eve's Attack Model

In an incoherent attack model under the BB84 protocol, Eve performs single qubit attack by interacting each qubit on the way to Bob from Alice with her auxiliary system. Eve's auxiliary system, which is designed to investigate the encoded state of a qubit, consists of an approximate quantum cloning machine and quntum memory [9], [10], [14] as shown in Fig. 2. There are theoretical [15]–[18] and experimental [19]–[21] works on the approximate quantum cloning. Even though Eve uses an optimized auxiliary system, perfect cloning of a quantum state is impossible due to the no-cloning theorem [22]. Therefore, Eve can only guess in a probabilistic manner which state was sent by Alice by investigating resulting states of the cloning machine. Moreover, it may corrupt the original qubit state with some probability which induces some errors on Bob's measurements.

Since the errors are unavoidable when Eve probes the incoming qubit with her system, Eve's most critical issue is not to be revealed directly. Thus, Eve designs her system to evenly distribute the error probability for all bases because the presence of Eve is easily detected by basis check if the error probability is different among bases. In other words, Eve adopts *symmetric* eavesdropping strategy that enables the same error probability for all bases. Note that, since Eve measures her final state after Alice and Bob announce their basis information, she can always select the same basis with coincidental bases between Alice's and Bob's for measuring Alice–Bob mutual information from her quantum memory during sifting process between Alice and Bob.

A generalized two-qubit cloning system of Eve, where the initial state $|\psi_0\rangle$ changes as it interacts with Alice's qubit under an operation, can be represented as follows:

$$|\mathbf{Q}\rangle \otimes |\psi_0\rangle \xrightarrow{U} \sum_{\mathbf{E}\subset\{1,2\}} \sqrt{D_\mathbf{E}}|\mathbf{Q_E}\rangle \otimes |\psi_\mathbf{E}^\mathbf{Q}\rangle \tag{2}$$

where $|\mathbf{Q}\rangle$ represents the incoming qubit from Alice, $|\mathbf{Q_E}\rangle$ is the photon state coming out of Eve's approximate quantum cloning machine, which may have an error (or errors) in a qubit (or qubits) indexed by a set $\mathbf{E}$, and $D_\mathbf{E}$ and $|\psi_\mathbf{E}^\mathbf{Q}\rangle$ are the corresponding probability and quantum memory state of Eve, respectively. Accordingly, $\sum_{\mathbf{E}\subset\{1,2\}} D_\mathbf{E} = 1$.

In order to understand how Eve's attack can be mathematically modeled, let us consider an example of approximate quantum cloning of both qubits in the Z basis of each. Using Eq. (2), the case of $|\mathbf{Q}\rangle = |q_{z0}q_{z0}\rangle$ can be represented as follows:

$$\begin{aligned}
|q_{z0}q_{z0}\rangle \otimes |\psi_0\rangle \xrightarrow{U}\ & \sqrt{D_\emptyset}|q_{z0}q_{z0}\rangle \otimes |\psi_\emptyset^{q_{z0}q_{z0}}\rangle\\
&+ \sqrt{D_{\{1\}}}|q_{z1}q_{z0}\rangle \otimes |\psi_{\{1\}}^{q_{z0}q_{z0}}\rangle\\
&+ \sqrt{D_{\{2\}}}|q_{z0}q_{z1}\rangle \otimes |\psi_{\{2\}}^{q_{z0}q_{z0}}\rangle\\
&+ \sqrt{D_{\{1,2\}}}|q_{z1}q_{z1}\rangle \otimes |\psi_{\{1,2\}}^{q_{z0}q_{z0}}\rangle.
\end{aligned} \tag{3}$$

Eq. (3) can be obtained by extending the operation of a quantum cloning machine in an one-qubit system, which is used in [10]. Note that $\emptyset$ represents an empty set: $D_\emptyset$ represents the probability that a cloned qubit has no error; and $|\psi_\emptyset^{q_{z0}q_{z0}}\rangle$ denotes Eve's final state when Alice sent $|q_{z0}q_{z0}\rangle$ and the cloned qubits have no errors.

In a similar way as in [10], using the Schmidt decomposition [23] and characteristics of unitary transformation [10], Eve's final state $|\psi_\mathbf{E}^\mathbf{Q}\rangle$ should satisfy the following condition:

$$\langle\psi_{\mathbf{E}_1}^{\mathbf{Q}_1}|\psi_{\mathbf{E}_2}^{\mathbf{Q}_2}\rangle = 0 \text{ for } \mathbf{E}_1 \neq \mathbf{E}_2, \tag{4}$$

where $\mathbf{Q}_1, \mathbf{Q}_2$ are any arbitrary states that Alice can send and $\mathbf{E}_1, \mathbf{E}_2 \subset \{1, 2\}$.

In [10], the authors realized that an analysis with respect to only one basis can represent those for all other bases due to the requirement of symmetric attack by Eve. They parameterize an Eve's system for one-qubit QKD as a four-dimensional Hilbert space due to a consequence of the fact that there exist only four Eve's states after cloning. Likewise, in a two-qubit system, there are 16 Eve's states after cloning per each basis because there are four Eve's states per each state as shown in Eq. (3) and each basis consists of four states. Therefore, we need a 16-dimensional Hilbert space to represent Eve's states which should follow Eq. (4). This analysis concludes that Eve ought to have four qubits to retain required quantum information to attack each photon.

In case of basis ZZ analysis, Eve can measure the state of her system with basis ZZ from the quantum memory. In that case, Eve's final state $|\psi_{\mathbf{E}}^{\mathbf{Q}}\rangle$ can be parameterized without loss of generality using Eq. (4) as follows:

$$|\psi_{\emptyset}^{q_{z0}q_{z0}}\rangle = |0\rangle|0\rangle|0\rangle|0\rangle, \tag{5}$$

$$|\psi_{\{1\}}^{q_{z0}q_{z0}}\rangle = |0\rangle|1\rangle|0\rangle|0\rangle, \tag{6}$$

$$|\psi_{\{2\}}^{q_{z0}q_{z0}}\rangle = |0\rangle|0\rangle|0\rangle|1\rangle, \tag{7}$$

$$|\psi_{\{1,2\}}^{q_{z0}q_{z0}}\rangle = |0\rangle|1\rangle|0\rangle|1\rangle, \tag{8}$$

$$|\psi_{\emptyset}^{q_{z1}q_{z0}}\rangle = |a_1\rangle|0\rangle|0\rangle|0\rangle, \tag{9}$$

$$|\psi_{\{1\}}^{q_{z1}q_{z0}}\rangle = |b_1\rangle|1\rangle|0\rangle|0\rangle, \tag{10}$$

$$|\psi_{\{2\}}^{q_{z1}q_{z0}}\rangle = |a_1\rangle|0\rangle|0\rangle|1\rangle, \tag{11}$$

$$|\psi_{\{1,2\}}^{q_{z1}q_{z0}}\rangle = |b_1\rangle|1\rangle|0\rangle|1\rangle, \tag{12}$$

$$|\psi_{\emptyset}^{q_{z0}q_{z1}}\rangle = |0\rangle|0\rangle|a_2\rangle|0\rangle, \tag{13}$$

$$|\psi_{\{1\}}^{q_{z0}q_{z1}}\rangle = |0\rangle|1\rangle|a_2\rangle|0\rangle, \tag{14}$$

$$|\psi_{\{2\}}^{q_{z0}q_{z1}}\rangle = |0\rangle|0\rangle|b_2\rangle|1\rangle, \tag{15}$$

$$|\psi_{\{1,2\}}^{q_{z0}q_{z1}}\rangle = |0\rangle|1\rangle|b_2\rangle|1\rangle, \tag{16}$$

$$|\psi_{\emptyset}^{q_{z1}q_{z1}}\rangle = |a_1\rangle|0\rangle|a_2\rangle|0\rangle, \tag{17}$$

$$|\psi_{\{1\}}^{q_{z1}q_{z1}}\rangle = |b_1\rangle|1\rangle|a_2\rangle|0\rangle, \tag{18}$$

$$|\psi_{\{2\}}^{q_{z1}q_{z1}}\rangle = |a_1\rangle|0\rangle|b_2\rangle|1\rangle, \tag{19}$$

$$|\psi_{\{1,2\}}^{q_{z1}q_{z1}}\rangle = |b_1\rangle|1\rangle|b_2\rangle|1\rangle, \tag{20}$$

where, for $i \in \{1, 2\}$, $|a_i\rangle := \cos a_i|0\rangle + \sin a_i|1\rangle$ and $|b_i\rangle := \cos b_i|0\rangle + \sin b_i|1\rangle$. Here, a_1, a_2, b_1, and b_2 are control parameters that characterize Eve's system. These control parameters are utilized to extract the qubit information. Eve can obtain information about qubit encoded with the first coding scheme by adjusting a_1 and b_1. Likewise, the qubit information for the second coding scheme can be obtained by adjusting a_2 and b_2. Since we assume two independent coding schemes are applied on a single photon, eavesdropping strategies controlling a_i and b_i for the i-th qubit are independent from each other. Therefore, we can express all possible Eve's final states by varying the four parameters independently. Throughout Eve's all possible strategies, we find a condition that Eve is able to obtain maximum mutual information between Alice and herself and provide a security proof in Section III. Eve's system is parameterized that the second and fourth qubits are used to extract the error information $\mathbf{E}$, the first and third qubits are used to extract information of a qubit state sent by Alice, which will be specifically introduced in Section II-D.

D. Disturbance Analysis on Eve's Incoherent Attack

For Eve's symmetric attack, she should distribute disturbance evenly among different bases. In order to analyze Eve's incoherent attack, we need to find the disturbance which satisfies the symmetric condition. First, assume Alice sends $|q_{x0}q_{z0}\rangle$ which is one of the four states in basis XZ. Using Eq. (2), the state changes as follows after unitary operation in Eve's system:

$$\begin{aligned}|q_{x0}q_{z0}\rangle \otimes |\psi_0\rangle \xrightarrow{U}\; & \sqrt{D_{\emptyset}}|q_{x0}q_{z0}\rangle \otimes |\psi_{\emptyset}^{q_{x0}q_{z0}}\rangle \\ & + \sqrt{D_{\{1\}}}|q_{x1}q_{z0}\rangle \otimes |\psi_{\{1\}}^{q_{x0}q_{z0}}\rangle \\ & + \sqrt{D_{\{2\}}}|q_{x0}q_{z1}\rangle \otimes |\psi_{\{2\}}^{q_{x0}q_{z0}}\rangle \\ & + \sqrt{D_{\{1,2\}}}|q_{x1}q_{z1}\rangle \otimes |\psi_{\{1,2\}}^{q_{x0}q_{z0}}\rangle. \end{aligned} \tag{21}$$

Since all states in basis XZ can be represented as superposition of states in the basis ZZ by the Table I, state $|q_{x0}q_{z0}\rangle$ can be re-expressed as follows:

$$\begin{aligned}&|q_{x0}q_{z0}\rangle \otimes |\psi_0\rangle \\ &= \frac{1}{\sqrt{2}}(|q_{z0}q_{z0}\rangle + |q_{z1}q_{z0}\rangle) \otimes |\psi_0\rangle \end{aligned} \tag{22}$$

$$\begin{aligned}&\xrightarrow{U} \frac{1}{\sqrt{2}}\Big(\sqrt{D_{\emptyset}}|q_{z0}q_{z0}\rangle \otimes |\psi_{\emptyset}^{q_{z0}q_{z0}}\rangle \\ &\quad + \sqrt{D_{\{1\}}}|q_{z1}q_{z0}\rangle \otimes |\psi_{\{1\}}^{q_{z0}q_{z0}}\rangle \\ &\quad + \sqrt{D_{\{2\}}}|q_{z0}q_{z1}\rangle \otimes |\psi_{\{2\}}^{q_{z0}q_{z0}}\rangle \\ &\quad + \sqrt{D_{\{1,2\}}}|q_{z1}q_{z1}\rangle \otimes |\psi_{\{1,2\}}^{q_{z0}q_{z0}}\rangle\Big) \\ &\quad + \frac{1}{\sqrt{2}}\Big(\sqrt{D_{\emptyset}}|q_{z1}q_{z0}\rangle \otimes |\psi_{\emptyset}^{q_{z1}q_{z0}}\rangle \\ &\quad + \sqrt{D_{\{1\}}}|q_{z0}q_{z0}\rangle \otimes |\psi_{\{1\}}^{q_{z1}q_{z0}}\rangle \\ &\quad + \sqrt{D_{\{2\}}}|q_{z1}q_{z1}\rangle \otimes |\psi_{\{2\}}^{q_{z1}q_{z0}}\rangle \\ &\quad + \sqrt{D_{\{1,2\}}}|q_{z0}q_{z1}\rangle \otimes |\psi_{\{1,2\}}^{q_{z1}q_{z0}}\rangle\Big). \end{aligned}$$

Note that both two-qubit states are represented as those of basis ZZ. When substituting these states with ones in basis XZ and comparing it with Eq. (21), we can get Eve's final state relations between $|\psi_{\mathbf{E}_1}^{q_{x0}q_{z0}}\rangle$ and $|\psi_{\mathbf{E}_2}^{q_{z0}q_{z0}}\rangle$, $|\psi_{\mathbf{E}_2}^{q_{z1}q_{z0}}\rangle$ where $\mathbf{E}_1, \mathbf{E}_2 \subset \{1, 2\}$. Therefore, Eve's final states should obey the relations among them. For example, the case that the cloned qubits have no errors for $|q_{x0}q_{z0}\rangle$ shows the following relation:

$$\begin{aligned}|\psi_{\emptyset}^{q_{x0}q_{z0}}\rangle = \frac{1}{2}\Bigg\{&\Big(|\psi_{\emptyset}^{q_{z0}q_{z0}}\rangle + |\psi_{\emptyset}^{q_{z1}q_{z0}}\rangle\Big) \\ &+ \sqrt{\frac{D_{\{1\}}}{D_{\emptyset}}}\Big(|\psi_{\{1\}}^{q_{z0}q_{z0}}\rangle + |\psi_{\{1\}}^{q_{z1}q_{z0}}\rangle\Big)\Bigg\}. \end{aligned} \tag{23}$$

In the same way, relations similar to Eq. (23) can be obtained for three other error cases.

Using Eqs. (5)–(12) and the condition that $\langle\psi_{\mathbf{E}}^{q_{x0}q_{z0}}|\psi_{\mathbf{E}}^{q_{x0}q_{z0}}\rangle = 1$ for any $\mathbf{E} \subset \{1, 2\}$, we finally get:

$$D_{\emptyset} = f_1 D_{\{1\}}, \quad D_{\{2\}} = f_1 D_{\{1,2\}}, \tag{24}$$

where $f_1 = \frac{1+\cos b_1}{1-\cos a_1}$. Recall that the above case is the one that Alice sends $|q_{x0}q_{z0}\rangle$ which is in basis XZ. By applying exactly the same way for the case where Alice sends a state in the basis

ZX, following relations can be deduced

$$D_{\emptyset} = f_2 D_{\{2\}}, \quad D_{\{1\}} = f_2 D_{\{1,2\}}, \tag{25}$$

where $f_2 = \frac{1+\cos b_2}{1-\cos a_2}$. Since Eve adopts a symmetric eavesdropping strategy, disturbances in Eqs. (24) and (25) should be identical to each other. In addition, from the fact that $\sum_{\mathbf{E}\subset\{1,2\}} D_{\mathbf{E}} = 1$, we can represent the disturbances as follows:

$$\begin{aligned} D_{\emptyset} &= \frac{f_1 f_2}{(1+f_1)(1+f_2)}, \\ D_{\{1\}} &= \frac{f_2}{(1+f_1)(1+f_2)}, \\ D_{\{2\}} &= \frac{f_1}{(1+f_1)(1+f_2)}, \\ D_{\{1,2\}} &= \frac{1}{(1+f_1)(1+f_2)}. \end{aligned} \tag{26}$$

E. Eve's Optimal Incoherent Attack

After Alice's transmission, Eve measures her system by using revealed basis through a public channel. Then, Eve can guess the qubit state sent by Alice from her measured system state, which is possible due to Eq. (2). To guess, Eve performs the following two steps. First, Eve measures the second and fourth qubits in $|\psi^{\mathbf{Q}}_{\mathbf{E}}\rangle$. Since we set the states of the second and fourth qubits in $|\psi^{\mathbf{Q}}_{\mathbf{E}}\rangle$ to satisfy the condition in Eq. (4), Eve has complete error information $\mathbf{E}$ of the qubits received by Bob.

From the first step, we find $\mathbf{E}$, but there are four Eve's system states having the same $\mathbf{E}$. In the next step, by measuring the first and third qubits in $|\psi^{\mathbf{Q}}_{\mathbf{E}}\rangle$, Eve discriminates the four states. However, they are non-orthogonal such as in Eqs. (5), (9), (13), and (17). Therefore, to compute probability of guessing the qubit state sent by Alice, we reorganize $|\psi^{q_{z0}q_{z0}}_{\emptyset}\rangle$, $|\psi^{q_{z1}q_{z0}}_{\emptyset}\rangle$, $|\psi^{q_{z0}q_{z1}}_{\emptyset}\rangle$, and $|\psi^{q_{z1}q_{z1}}_{\emptyset}\rangle$ as a function of the guessing probability

$$\begin{aligned} |\psi'^{q_{z0}q_{z0}}_{\emptyset}\rangle =\ & \beta_{\{1,2\}|\emptyset}|0\rangle|0\rangle|0\rangle|0\rangle + \beta_{\{1\}|\emptyset}|1\rangle|0\rangle|0\rangle|0\rangle \\ & + \beta_{\{2\}|\emptyset}|0\rangle|0\rangle|1\rangle|0\rangle + \beta_{\emptyset|\emptyset}|1\rangle|0\rangle|1\rangle|0\rangle, \end{aligned} \tag{27}$$

$$\begin{aligned} |\psi'^{q_{z1}q_{z0}}_{\emptyset}\rangle =\ & \beta_{\{2\}|\emptyset}|0\rangle|0\rangle|0\rangle|0\rangle + \beta_{\{1,2\}|\emptyset}|1\rangle|0\rangle|0\rangle|0\rangle \\ & + \beta_{\emptyset|\emptyset}|0\rangle|0\rangle|1\rangle|0\rangle + \beta_{\{1\}|\emptyset}|1\rangle|0\rangle|1\rangle|0\rangle, \end{aligned} \tag{28}$$

$$\begin{aligned} |\psi'^{q_{z0}q_{z1}}_{\emptyset}\rangle =\ & \beta_{\{1\}|\emptyset}|0\rangle|0\rangle|0\rangle|0\rangle + \beta_{\emptyset|\emptyset}|1\rangle|0\rangle|0\rangle|0\rangle \\ & + \beta_{\{1,2\}|\emptyset}|0\rangle|0\rangle|1\rangle|0\rangle + \beta_{\{2\}|\emptyset}|1\rangle|0\rangle|1\rangle|0\rangle, \end{aligned} \tag{29}$$

$$\begin{aligned} |\psi'^{q_{z1}q_{z1}}_{\emptyset}\rangle =\ & \beta_{\emptyset|\emptyset}|0\rangle|0\rangle|0\rangle|0\rangle + \beta_{\{1\}|\emptyset}|1\rangle|0\rangle|0\rangle|0\rangle \\ & + \beta_{\{2\}|\emptyset}|0\rangle|0\rangle|1\rangle|0\rangle + \beta_{\{1,2\}|\emptyset}|1\rangle|0\rangle|1\rangle|0\rangle, \end{aligned} \tag{30}$$

where $\beta_{\mathbf{C}|\mathbf{E}}$ is the probability amplitude of $Pr(\mathbf{C}|\mathbf{E})$ which represents, when error information $\mathbf{E}$ is given, the probability that correctly guesses i-th qubit sent by Alice for $i \in \mathbf{C} \subset \{1,2\}$. That is, $\left|\beta_{\mathbf{C}|\mathbf{E}}\right|^2 = Pr(\mathbf{C}|\mathbf{E})$.

Although we arbitrary reorganize Eve's system states as in Eqs. (27)–(30), the states should still follow the inner product relations from Eqs. (5), (9), (13), and (17). For example, $\langle\psi^{q_{z0}q_{z0}}_{\emptyset}|\psi^{q_{z1}q_{z0}}_{\emptyset}\rangle = \langle\psi'^{q_{z0}q_{z0}}_{\emptyset}|\psi'^{q_{z1}q_{z0}}_{\emptyset}\rangle$. Then,

$$\begin{aligned} \cos a_1 =\ & \beta_{\{1,2\}|\emptyset}\beta_{\{2\}|\emptyset} + \beta_{\{1\}|\emptyset}\beta_{\{1,2\}|\emptyset} \\ & + \beta_{\{2\}|\emptyset}\beta_{\emptyset|\emptyset} + \beta_{\emptyset|\emptyset}\beta_{\{1\}|\emptyset}. \end{aligned} \tag{31}$$

In a similar way, we can get two more equations in terms of $\beta_{\mathbf{C}|\emptyset}$. In addition to the relations, since $\sum_{\mathbf{C}} |\beta_{\mathbf{C}|\emptyset}|^2 = 1$ when there are no errors, we can compute $\beta_{\mathbf{C}|\emptyset}$. In a similar way, we can compute $\beta_{\mathbf{C}|\mathbf{E}}$ for the other error cases. Then,

$$\begin{aligned} Pr(\mathbf{C}|\mathbf{E}) = \ & \frac{1}{2^2} \prod_{i\in\mathbf{C}, i\notin\mathbf{E}} (1+\sin a_i) \prod_{i\in\mathbf{C}, i\in\mathbf{E}} (1+\sin b_i) \\ & \prod_{i\notin\mathbf{C}, i\notin\mathbf{E}} (1-\sin a_i) \prod_{i\notin\mathbf{C}, i\in\mathbf{E}} (1-\sin b_i). \end{aligned} \tag{32}$$

The probability that correctly guesses an i-th qubit sent by Alice for $i \in \mathbf{C} \subset \{1,2\}$ is calculated as follows

$$Pr(\mathbf{C}) = \sum_{\mathbf{E}\subset\{1,2\}} D_{\mathbf{E}} Pr(\mathbf{C}|\mathbf{E}). \tag{33}$$

By the definition of mutual information [24], we can compute mutual information between Alice and Eve, I_{AE}

$$\begin{aligned} I_{AE} &= 1 + \sum_{\mathbf{C}} Pr(\mathbf{C}) \log_{2^2} Pr(\mathbf{C}), \\ &= 1 + \sum_{\mathbf{C}} \left(\sum_{\mathbf{E}} D_{\mathbf{E}} Pr(\mathbf{C}|\mathbf{E})\right) \log_{2^2} \left(\sum_{\mathbf{E}} D_{\mathbf{E}} Pr(\mathbf{C}|\mathbf{E})\right), \\ &\le 1 + \sum_{\mathbf{C}} \sum_{\mathbf{E}} D_{\mathbf{E}} Pr(\mathbf{C}|\mathbf{E}) \log_{2^2} Pr(\mathbf{C}|\mathbf{E}). \end{aligned} \tag{34}$$

In Eq. (34), the inequality can be obtained by using Jensen's inequality and convexity of $f(x) = x \log_{2^2} x$. The equality of last inequality holds if the following condition is satisfied

$$Pr(\mathbf{C}|\emptyset) = Pr(\mathbf{C}|\{1\}) = Pr(\mathbf{C}|\{2\}) = Pr(\mathbf{C}|\{1,2\}). \tag{35}$$

This implies that all system parameters are equal for the Eve's optimal incoherent attack. That is, $a_1 = a_2 = b_1 = b_2 = c$, where c is constant. Applying this condition on Eq. (34),

$$I_{AE} \le 1 + \sum_{i=0}^{2} \binom{2}{i} f\left(\frac{1}{2^2}(1+\sin c)^{2-i}(1-\sin c)^i\right), \tag{36}$$

where $f(x) = x \log_{2^2} x$.

III. Error Tolerance Bound for Secure Communication

Based on the computed mutual information between Alice and Eve, we can find allowable error bound for secure communication. As discussed in [24], Alice and Bob can perform secure communication iff $I_{AB} \ge I_{AE}$ or $I_{AB} \ge I_{BE}$, where I_{AB} and I_{BE} represent the mutual information between Alice and Bob and between Bob and Eve, respectively. Therefore, computing I_{AB} and comparing it with I_{AE} determines the error bound for the secure communication. Assuming there is no errors caused by device imperfection or environmental issues including noise and loss, I_{AB} can be only affected by the errors caused by Eve's

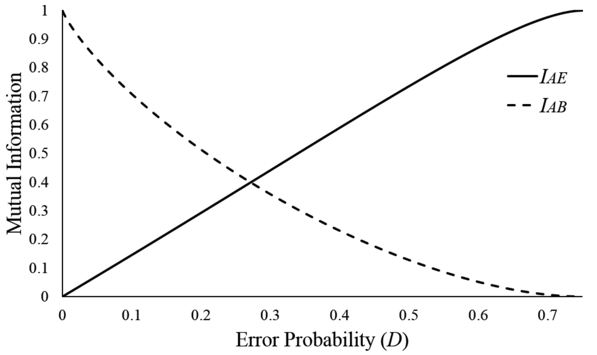

Fig. 3. The mutual information between Alice and Bob, I_{AB}, and between Alice and Eve, I_{AE}, in terms of error probability, D.

system. Using disturbances analyzed in the Section II, I_{AB} can be represented as follows:

$$I_{AB} = 1 + \sum_{\mathbf{E}} D_{\mathbf{E}} \log_{2^2} D_{\mathbf{E}}. \tag{37}$$

With I_{AE} in Eq. (34) and I_{AB} in Eq. (37), we can compute threshold error probability, which satisfies $I_{AB} = I_{AE}$, for the secure communication. To begin with, we define error probability as quantum symbol error probability where a quantum symbol represents a single photon encoded two coding schemes, which is represented as follows:

$$D = \sum_{\mathbf{E}} D_{\mathbf{E}} - D_{\emptyset} = 1 - D_{\emptyset}. \tag{38}$$

Even if we use the symbol error probability, QBER still equals to one-qubit QKD system. To let quantum symbol error rate equal to QBER, we suggest a different way of error estimation compared to that of conventional BB84. In the error estimation after sifting, Alice and Bob consider one symbol error as two-bit error if a symbol has at least one error. Since one-bit and two-bit errors in a symbol imply Eve's presence, the aforementioned way is reasonable.

By using Eqs. (26) and (38), I_{AE} and I_{AB} can be expressed as a function of D. The mutual information in terms of D is plotted in Fig. 3. From the Eqs. (36) and (37) as well as Fig. 3, we can find the threshold value of D is about 27.2%. It means that if the result of error estimation is lower than 27.2%, we can guarantee secure communication. Furthermore, since the probability that Alice and Bob correctly select bases is 1/4 and one symbol has two-bit information, the ratio between sifted key rate and raw key rate is the same as a one-qubit QKD system. Therefore, two-qubit system provides almost doubled error bound for the secure communication compared with the one-qubit system without loss of the ratio between raw key rate and sifted key rate.

From Fig. 3, we can also see that the multi-qubit QKD protocol considered in our work is better than those in [12] in terms of security as well as key rate. Specifically, consider the second protocol in [12] and assume that the number of bases is 4. While our multi-qubit protocol offers the security bound of 27.2% of qubit symbol error rate, the protocol in [12] provides 26.66%. Furthermore, our protocol can achieve the doubled key rate compared to that of [12]. Notice that each basis in [12] has only two states, while the basis in our protocol has four states.

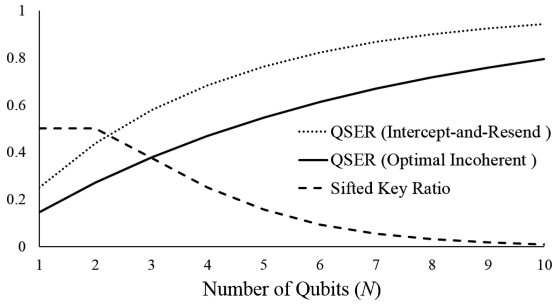

Fig. 4. The threshold of error probability for secure communication and the sifted key ratio in terms of the number of qubits N.

The security bound for intercept-and-resend attack is also plotted in Fig. 4.[2] One can readily see that intercept-and-resend attack introduces more errors in order for Eve to obtain more information than Bob, which means that it is less powerful than the optimal incoherent attack.

Extending the analysis of the two-qubit system, we analyze the security of an N-qubit system in a similar way. As a result, we get the following theorem.

Theorem 1: Consider an N-qubit QKD system where each qubit has two bases, each consisting of two orthonormal states. Suppose that we measure the symbol error D. Then Alice and Bob can generate the secret key if and only if

$$D \le 1 - \left(\frac{\sqrt{2} + 2}{4} \right)^{N}. \tag{39}$$

Proof: Refer to the Appendix. ■

Theorem 1 implies that the error tolerance bound for secure communication increases with the number N of qubits. See Fig. 4. In the figure, we also plot the ratio between the raw key rate and sifted key rate, which is referred as the sifted key ratio. Since there are 2^N bases can be chosen by Bob and a single photon has N-bit information, the ratio between raw key and sifted key rate becomes $N/2^N$. Note that the shifted key ratio decreases with an increase in N. One can see that there is a trade-off relation between the error tolerance bound and the shifted key ratio. However, we can find that the two-qubit case has no loss on the key ratio although secrecy increases.

IV. Proof of the Error Tolerance Bound

In this section, we first prove an error bound for secure communication in the two-qubit case when Eve's optimal incoherent attack is applied. A general proof of N-qubit case is presented in Appendix-A.

[2] The detailed explanations for intercept-and-resend attack are described in Appendix-B.

To find out an error bound, we need to compute $I_{AE} \leq I_{AB}$. For ease of calculation, we re-express Eq. (37) as follows:

$$I_{AB} = 1 + \sum_{i=0}^{2} \binom{2}{i} f\left(\frac{1}{2^2}(1+\cos c)^{2-i}(1-\cos c)^i\right). \tag{40}$$

where $f(x) = x\log_{2^2} x$. Therefore, from Eqs. (36) and (40), we need to find error probability which satisfies $\sin c \leq \cos c$ which is the same as $1 \leq 2\cos^2 c$. With Eqs. (26) and (38), we can express $\cos c$ as a function of D which is $\cos c = 2\sqrt{1-D} - 1$. Then, we can compute the final quantum symbol error bound as

$$D \leq 1 - \left(\frac{\sqrt{2}+2}{4}\right)^2 \approx 27.2\%. \tag{41}$$

V. Conclusion

Even though an incoherent attack against a QKD system will become realized in some future, understanding QKD performance against an ultimate attack is fundamentally important. The effort to enhance the secret key rate has been appreciated as well as the effort to enhance secrecy. These benefits can be brought by a multi-qubit QKD system even under Eve's incoherent attack. In this paper, we analyze rigorously a two-qubit QKD system secrecy performance, where each single photon is encoded with two different coding scheme against the Eve's incoherent attack. We assume each coding scheme uses two bases and two states per basis like the BB84 protocol. We model completely an incoherent attack by Eve with approximate quantum cloning and quantum memory for the cases of two-qubit and N-quibit QKD, following the secrecy analysis of BB84. With the result, we find the tolerable error probability in terms of quantum symbol error rate is 27.2% for the two-qubit case which is almost doubled from that of an one-qubit QKD system, while the sifted key ratio is the same as that of the one-qubit QKD system. Furthermore, the N-qubit QKD system analysis shows the trade-off relation between the error bound and the sifted key ratio, which suggests the fundamental design rule for multi-qubit QKD systems.

Appendix A
Proof of Theorem 1

A. N-Qubit QKD States

N-qubit state $|\mathbf{Q}\rangle$ can be defined as follows:

$$|\mathbf{Q}\rangle = |q_{bs}\rangle_1 \otimes |q_{bs}\rangle_2 \otimes \cdots \otimes |q_{bs}\rangle_N, \tag{A.1}$$

where $|q_{bs}\rangle_i$ represents state of the i-th qubit $(i = 1, 2, \ldots, N)$, where $b \in \{\mathrm{z}, \mathrm{x}\}$ and $s \in \{0, 1\}$ indicate indices for basis and state of the i-th qubit. State relations for each i-th qubit are as follows:

$$|q_{\mathrm{x}0}\rangle_i = \frac{1}{\sqrt{2}}\left(|q_{\mathrm{z}0}\rangle_i + |q_{\mathrm{z}1}\rangle_i\right), \tag{A.2}$$

$$|q_{\mathrm{x}1}\rangle_i = \frac{1}{\sqrt{2}}\left(|q_{\mathrm{z}0}\rangle_i - |q_{\mathrm{z}1}\rangle_i\right). \tag{A.3}$$

For N-qubit representation, each of 2^N bases make 2^N states. Therefore, total 2^{2N} states are created

$$\begin{aligned}
\text{Basis ZZ}\cdots\text{Z}: \ & |q_{\mathrm{z}0}q_{\mathrm{z}0}\cdots q_{\mathrm{z}0}\rangle, |q_{\mathrm{z}1}q_{\mathrm{z}0}\cdots q_{\mathrm{z}0}\rangle, \\
& \cdots, |q_{\mathrm{x}1}q_{\mathrm{z}1}\cdots q_{\mathrm{z}1}\rangle \\
\text{Basis XZ}\cdots\text{Z}: \ & |q_{\mathrm{x}0}q_{\mathrm{z}0}\cdots q_{\mathrm{z}0}\rangle, |q_{\mathrm{x}1}q_{\mathrm{z}0}\cdots q_{\mathrm{z}0}\rangle, \\
& \cdots, |q_{\mathrm{x}1}q_{\mathrm{z}1}\cdots q_{\mathrm{z}1}\rangle \\
& \vdots \\
\text{Basis XX}\cdots\text{X}: \ & |q_{\mathrm{x}0}q_{\mathrm{x}0}\cdots q_{\mathrm{x}0}\rangle, |q_{\mathrm{x}1}q_{\mathrm{x}0}\cdots q_{\mathrm{x}0}\rangle, \\
& \cdots, |q_{\mathrm{x}1}q_{\mathrm{x}1}\cdots q_{\mathrm{x}1}\rangle.
\end{aligned}$$

Here an i-th qubit state is indicated at the i-th position in an N-qubit state. As already defined in Section II, Eve's cloning system whose initial state $|\psi_0\rangle$ changes as it interacts with Alice's qubit by unitary operation can be represented as

$$|\mathbf{Q}\rangle \otimes |\psi_0\rangle \xrightarrow{U} \sum_{\mathbf{E}\subset\mathbb{N}} \sqrt{D_{\mathbf{E}}}|\mathbf{Q}_{\mathbf{E}}\rangle \otimes |\psi_{\mathbf{E}}^{\mathbf{Q}}\rangle, \tag{A.4}$$

where $\mathbb{N} = \{1, 2, \ldots, N\}$, $D_{\mathbf{E}}$ is probability that a group of qubits indexed by an error qubit set $\mathbf{E}$ have state errors, $|\mathbf{Q}_{\mathbf{E}}\rangle$ indicates the corresponding cloned qubit state referenced by $\mathbf{E}$, and $|\psi_{\mathbf{E}}^{\mathbf{Q}}\rangle$ represents the state of Eve's system after cloning when Alice sent $|\mathbf{Q}\rangle$ and Bob received the state with errors of $\mathbf{E}$. Through the same procedures as in Section II, parameterization of Eve's system state can be conducted as follows using $\langle\psi_{\mathbf{E}_1}^{\mathbf{Q}_1}|\psi_{\mathbf{E}_2}^{\mathbf{Q}_2}\rangle = 0$ for $\mathbf{E}_1 \neq \mathbf{E}_2$ where $\mathbf{E}_1, \mathbf{E}_2 \subset \mathbb{N}$ and $\mathbf{Q}_1, \mathbf{Q}_2$ are any arbitrary states that Alice can send

$$|\psi_{\mathbf{E}}^{\mathbf{Q}}\rangle = |\psi_{e_1}^{q_{bs}}\rangle_1 \otimes |\psi_{e_2}^{q_{bs}}\rangle_2 \otimes \cdots \otimes |\psi_{e_N}^{q_{bs}}\rangle_N, \tag{A.5}$$

where $b \in \{\mathrm{z}, \mathrm{x}\}$, $s \in \{0, 1\}$, $e_i \in \{0, 1\}$. If $i \in \mathbf{E}$, then $e_i = 1$; otherwise, $e_i = 0$. And $|\psi_{e_i}^{q_{bs}}\rangle_i$ is defined as follows:

$$\begin{aligned}
|\psi_0^{q_{b0}}\rangle &= |0\rangle|0\rangle, \\
|\psi_0^{q_{b1}}\rangle &= |a_i\rangle|0\rangle, \\
|\psi_1^{q_{b0}}\rangle &= |0\rangle|1\rangle, \\
|\psi_1^{q_{b1}}\rangle &= |b_i\rangle|1\rangle,
\end{aligned} \tag{A.6}$$

where $|a_i\rangle = \cos a_i|0\rangle + \sin a_i|1\rangle$, $|b_i\rangle = \cos b_i|0\rangle + \sin b_i|1\rangle$. Note that, for $i \in \mathbb{N}$, a_i and b_i are control parameters that characterize Eve's system. The parameterization as in Eq. (A.6) can easily be obtained by expending a parameterization used in one-qubit system [10], where Eve's system is parameterized with two qubits.

B. Mutual Information Between Alice and Bob

Disturbances of one-qubit QKD system, where a and b are Eve's system parameters, are

$$D_{\emptyset} = \frac{f}{1+f}, \quad D_{\{1\}} = \frac{1}{1+f}, \tag{A.7}$$

where $f = \frac{1+\cos b}{1-\cos a}$. For two-qubit QKD system, we can get disturbances as in Eq. (26). Similarly, N-qubit QKD system can be derived by the same pattern.

$$D_{\mathbf{E}} = \prod_{i=0}^{N} \frac{f_i}{1+f_i} \prod_{j \in \mathbf{E}} \frac{1}{f_j}, \tag{A.8}$$

where $f_i = \frac{1+\cos b_i}{1-\cos a_i}$, and $\mathbf{E} \subset \mathbb{N}$. Note that a_i's and b_i's are Eve's system parameters for $i \in \mathbb{N}$. Using Eq. (A.8), we can compute I_{AB} as follows:

$$I_{AB} = 1 + \sum_{\mathbf{E} \subset \mathbb{N}} D_{\mathbf{E}} \log_{2^N} D_{\mathbf{E}}. \tag{A.9}$$

C. Mutual Information Between Alice and Eve

In order to find out the probability $Pr(\mathbf{C}|\mathbf{E})$ for correct guess $\mathbf{C}$ of Alice's qubits by Eve under $|\mathbf{Q_E}\rangle$ in an N-qubit QKD system, we investigate $Pr(\mathbf{C}|\mathbf{E})$ in a one-qubit case first. Similarly to the aforementioned two-qubit QKD system, $Pr(\mathbf{C}|\mathbf{E})$ in one-qubit QKD system, i.e. for $\mathbf{C}, \mathbf{E} \subset \{1\}$, is obtained

$$Pr(\{1\}|\emptyset) = \frac{1}{2}(1+\sin a), \tag{A.10}$$

$$Pr(\emptyset|\emptyset) = \frac{1}{2}(1-\sin a), \tag{A.11}$$

$$Pr(\{1\}|\{1\}) = \frac{1}{2}(1+\sin b), \tag{A.12}$$

$$Pr(\emptyset|\{1\}) = \frac{1}{2}(1-\sin b), \tag{A.13}$$

where a and b are Eve's system parameters in the one-qubit QKD system. From the results of $Pr(\mathbf{C}|\mathbf{E})$ in one-qubit and two-qubit QKD systems, we find that $Pr(\mathbf{C}|\mathbf{E})$ in multi-qubit QKD system can be expressed as multiplication of $Pr(\mathbf{C}|\mathbf{E})$ in the one-qubit QKD system, because we assume the multiple independent coding scheme is applied in a single photon. Thus, for $\mathbf{C}, \mathbf{E} \subset \mathbb{N}$, we can easily find $Pr(\mathbf{C}|\mathbf{E})$ in N-qubit QKD system

$$\begin{aligned} Pr(\mathbf{C}|\mathbf{E}) = \frac{1}{2^N} &\prod_{i \in \mathbf{C}, i \notin \mathbf{E}} (1+\sin a_i) \prod_{i \in \mathbf{C}, i \in \mathbf{E}} (1+\sin b_i) \\ &\prod_{i \notin \mathbf{C}, i \notin \mathbf{E}} (1-\sin a_i) \prod_{i \notin \mathbf{C}, i \in \mathbf{E}} (1-\sin b_i). \end{aligned} \tag{A.14}$$

In a similar way as in Section II, the probability that Eve correctly guesses the i-th qubit sent by Alice for $i \in \mathbf{C} \subset \mathbb{N}$ is calculated as follows:

$$Pr\big(\mathbf{C}\big) = \sum_{\mathbf{E} \subset \mathbb{N}} D_{\mathbf{E}} Pr\big(\mathbf{C}|\mathbf{E}\big). \tag{A.15}$$

Mutual information between Alice and Eve depends on how much information is leaked to Eve from Alice. That is, I_{AE} only depends on $Pr(\mathbf{C})$. Therefore,

$$\begin{aligned} I_{AE} &= 1 + \sum_{\mathbf{C} \subset \mathbb{N}} Pr(\mathbf{C}) \log_{2^N} Pr(\mathbf{C}), \\ &= 1 + \sum_{\mathbf{C} \subset \mathbb{N}} \Big(\sum_{\mathbf{E} \subset \mathbb{N}} D_{\mathbf{E}} Pr(\mathbf{C}|\mathbf{E}) \Big) \log_{2^N} \Big(\sum_{\mathbf{E} \subset \mathbb{N}} D_{\mathbf{E}} Pr(\mathbf{C}|\mathbf{E}) \Big), \\ &\le 1 + \sum_{\mathbf{C} \subset \mathbb{N}} \sum_{\mathbf{E} \subset \mathbb{N}} D_{\mathbf{E}} Pr\big(\mathbf{C}|\mathbf{E}\big) \log_{2^N} Pr\,(\mathbf{C}|\mathbf{E}). \end{aligned} \tag{A.16}$$

The inequality in Eq. (A.16) is obtained by using Jensen's inequality and convexity of $x \log_{2^N} x$. And the equality holds iff the following condition is satisfied:

$$Pr\big(\mathbf{C}|\emptyset\big) = Pr\big(\mathbf{C}|\{1\}\big) = \cdots = Pr\big(\mathbf{C}|\{1,2,\ldots,N\}\big). \tag{A.17}$$

Eq. (A.17) implies $a_1 = a_2 = \cdots = a_N = b_1 = b_2 = \cdots = b_N = c$, where c is constant. Using Eqs. (A.14) and (A.17), mutual information between Alice and Eve is calculated as

$$I_{AE} = 1 + \sum_{i=0}^{N} \binom{N}{i} f\left(\frac{1}{2^N} \big(1+\sin c\big)^{N-i} \big(1-\sin c\big)^{i} \right), \tag{A.18}$$

where $f(x) = x \log_{2^N} x$.

D. Error Tolerance Bound for Secure Communication

Using Eqs. (A.9) and (A.17), I_{AB} can be calculated as

$$I_{AB} = 1 + \sum_{i=0}^{N} \binom{N}{i} f_N \left(\frac{1}{2^N} \big(1+\cos c\big)^{N-i} \big(1-\cos c\big)^{i} \right), \tag{A.19}$$

where $f(x) = x \log_{2^N} x$. According to the theorem in [24], $I_{AE} \le I_{AB}$ should be satisfied for secure communication. For an N-qubit QKD system, $I_{AE} \le I_{AB}$ is satisfied iff $\sin c \le \cos c$ which is obtained from Eqs. (A.18) and (A.19). Finally, by $\cos c = 2(1-D)^{\frac{1}{N}} - 1$ from Eq. (A.8), we can derive the error tolerance bound as follows:

$$D \le 1 - \left(\frac{\sqrt{2}+2}{4} \right)^{N}. \tag{A.20}$$

Appendix B

Intercept-and-Resend Attack

Intercept-and-resend attack is a sort of eavesdropping strategy, where Eve captures and measures a qubit with a randomly chosen basis and resends a new qubit in the measured state over a quantum channel to Bob, e.g., via an optical fiber. This may cause errors in qubits received by Bob. Therefore, even in an ideal case where the channel and apparatuses are perfect, the error probability on Bob's qubit is nonzero so that it can be an indicator of Eve's existence. In order to calculate the symbol error probability that Eve causes errors, one ought to consider two probabilities: The first probability is with respect to the event that a basis chosen by Eve is different from that of Alice. When N coding schemes are used on a single photon, the probability that Eve and Alice choose different bases is as follows:

$$Pr\{X_{A \neq E} = i\} = \binom{N}{i} \frac{1}{2^N}, \tag{B.1}$$

where $X_{A \neq E}$ indicates the number of differently chosen bases between Alice and Eve. The second probability is that the state of a resent photon has at least one error given $X_{A \neq E} = i$. Since each coding scheme has two orthonormal states per basis, the error probability for each basis in a coding scheme is $\frac{1}{2}$. Since we assume coding schemes are independent, the probability that there are at least one error in the resent photon given $X_{A \neq E} = i$ is as follows:

$$Pr\{\text{error}|X_{A \neq E} = i\} = 1 - \frac{1}{2^i}. \tag{B.2}$$

With the two probabilities, we can compute the average error probability due to Eve as follows:

$$\begin{aligned} Pr\{\text{error}\} &= \sum_{i=1}^{N} Pr\{\text{error}|X_{A \neq E} = i\} Pr\{X_{A \neq E} = i\} \\ &= \frac{1}{2^N} \sum_{i=1}^{N} \binom{N}{i} \left(1 - \frac{1}{2^i}\right). \end{aligned} \tag{B.3}$$

References

[1] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. Dynes *et al.*, "The SECOQC quantum key distribution network in vienna," *New J. Phys.*, vol. 11, no. 7, p. 075001, 2009.

[2] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka *et al.*, "Field test of quantum key distribution in the tokyo QKD network," *Opt. Exp.*, vol. 19, no. 11, pp. 10-387–10-409, 2011.

[3] K. Patel, J. Dynes, M. Lucamarini, I. Choi, A. Sharpe, Z. Yuan, R. Penty, and A. Shields, "Quantum key distribution for 10 gb/s dense wavelength division multiplexing networks," *Appl. Phys. Lett.*, vol. 104, no. 5, p. 051123, 2014.

[4] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li *et al.*, "Experimental measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 111, no. 13, p. 130502, 2013.

[5] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," *Nature Photon.*, vol. 7, no. 5, pp. 378–381, 2013.

[6] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, "Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution," *Phys. Rev. Lett*, vol. 112, no. 19, p. 190503, 2014.

[7] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," presented at the IEEE Int. Conf. Computers, Systems Signal Processing, New York, NY, USA, 1984, vol. 175.

[8] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, "Quantum privacy amplification and the security of quantum cryptography over noisy channels," *Phys. Rev. Lett.*, vol. 77, no. 13, p. 2818, 1996.

[9] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, "Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy," *Phys. Rev. A*, vol. 56, no. 2, p. 1163, 1997.

[10] H. Bechmann-Pasquinucci and N. Gisin, "Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography," *Phys. Rev. A*, vol. 59, no. 6, p. 4238, 1999.

[11] J.-D. Wang, Z.-J. Wei, H. Zhang, X.-J. Qin, X.-B. Liu, Z.-M. Zhang, C.-J. Liao, and S.-H. Liu, "Efficient quantum key distribution via single-photon two-qubit states," *J. Phys. B, Atomic, Mol. Opt. Phys.*, vol. 43, no. 9, p. 095504, 2010.

[12] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, "Security of quantum key distribution using d-level systems," *Phys. Rev. Lett.*, vol. 88, no. 12, p. 127902, 2002.

[13] E. Knill, R. Laflamme, and G. J. Milburn, "A scheme for efficient quantum computation with linear optics," *Nature*, vol. 409, no. 6816, pp. 46–52, 2001.

[14] J. Cirac and N. Gisin, "Coherent eavesdropping strategies for the four state quantum cryptography protocol," *Phys. Lett. A*, vol. 229, no. 1, pp. 1–7, 1997.

[15] D. Bruß, M. Cinchetti, G. M. DAriano, and C. Macchiavello, "Phase-covariant quantum cloning," *Phys. Rev. A*, vol. 62, no. 1, p. 012302, 2000.

[16] H. Fan, K. Matsumoto, X.-B. Wang, and M. Wadati, "Quantum cloning machines for equatorial qubits," *Phys. Rev. A*, vol. 65, no. 1, p. 012304, 2001.

[17] J. Fiurášek, "Optical implementations of the optimal phase-covariant quantum cloning machine," *Phys. Rev. A*, vol. 67, no. 5, p. 052314, 2003.

[18] C.-Y. Li, Z.-R. Zhang, S.-H. Sun, M.-S. Jiang, and L.-M. Liang, "Optimal symmetric quantum cloning machine with nonlinear optics," *JOSA B*, vol. 30, no. 1, pp. 123–126, 2013.

[19] X.-Y. Pan, G.-Q. Liu, L.-L. Yang, and H. Fan, "Solid-state optimal phase-covariant quantum cloning machine," *Appl. Phys. Lett.*, vol. 99, no. 5, p. 051113, 2011.

[20] J. Du, T. Durt, P. Zou, H. Li, L. Kwek, C. Lai, C. Oh, and A. Ekert, "Experimental quantum cloning with prior partial information," *Phys. Rev. Lett.*, vol. 94, no. 4, p. 040505, 2005.

[21] H. Chen, X. Zhou, D. Suter, and J. Du, "Experimental realization of 12 asymmetric phase-covariant quantum cloning," *Phys. Rev. A*, vol. 75, no. 1, p. 012317, 2007.

[22] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[23] A. Peres, *Quantum Theory: Concepts and Methods*. New York, NY, USA: Springer, 1995, vol. 57.

[24] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, 2002.

Kyongchun Lim received the B.E. degree in electronic and electrical engineering from Sungkyunkwan University, Seoul, Korea, in 2012, and the M.S. degree in electrical engineering from the Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Korea, in 2014, where he is currently working toward the Ph.D. degree. His current research interests include quantum key distribution and quantum information.

Heasin Ko received the B.E. degree in electrical engineering from the Korea Advanced Institute of Science and Technology, Daejeon, Korea, in 2014, where he is currently working toward the M.S. degree. His current research interests include quantum cryptography and quantum computation.

Kiung Kim received the B.E. degree in electrical engineering from the Korea Advanced Institute of Science and Technology, Daejeon, Korea, in 2014 where he is currently working toward the M.S. degree. His current research interests include quantum information theory and quantum key distribution.

Changho Suh (S'10–M'12) received the B.S. and M.S. degrees in electrical engineering from the Korea Advanced Institute of Science and Technology (KAIST) in 2000 and 2002, respectively, and the Ph.D. degree in electrical engineering and computer sciences from UC-Berkeley, Berkeley, CA, USA, in 2011. From 2002 to 2006, he had been with the Telecommunication R&D Center, Samsung Electronics. From 2011 to 2012, he was a Postdoctoral Associate at the Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA, USA. He is an Assistant Professor with the Department of Electrical Engineering, KAIST, since 2012.

Dr. Suh received the 2013 Stephen O. Rice Prize from the IEEE Communications Society, the David J. Sakrison Memorial Prize for outstanding doctoral research from the UC-Berkeley EECS Department in 2011, and the Best Student Paper Award of the IEEE International Symposium on Information Theory in 2009. He also received the Vodafone U.S. Foundation Fellowship in 2006 and 2007, and the Kwanjeong Educational Foundation Fellowship in 2009.

June-Koo Kevin Rhee (S'92–M'95) received the B.E. and M.Sc degrees from Seoul National University, Seoul, Korea, in 1988 and 1990, respectively, and the Ph.D. degree from the University of Michigan, Ann Arbor, MI, USA, in 1995. He is currently a Professor in electrical engineering, Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Korea, since 2009. Prior to KAIST, he was affiliated with KAIST-ICU, Samsung Electronics, Corning Incorporation, NEC Research Institute, and Princeton University. His research interests include the areas of quantum optics, quantum information systems, optical communication, and networking. He has authored and coauthored more than 160 technical journal and conference papers, which received more than 1500 citations. He received the Ministry Certification of Commendation 2013 from the Korea Ministry of Science, ICT and Future Planning.