Eavesdropping Detection in BB84 Quantum Key Distribution Protocols

Chankyun Lee, *Member, IEEE*, Ilkwon Sohn, and Wonhyuk Lee

***Abstract*—The nature of quantum mechanics provides us with an opportunity to statistically detect eavesdropping in quantum key distribution (QKD) protocols, which is unimaginable in classical digital communications. By utilizing Hoeffding's inequality, this study analyzes the upper bounds of the false-positive ratio (FPR) and false-negative ratio (FNR) of eavesdropping detection in the Bennett–Brassard-84 (BB84) QKD protocol, where eavesdropping is detected if the measured quantum bit error rate (QBER) is equal to or higher than a threshold. The analysis clarifies the trade-off between the accuracy of eavesdropping detection and the economy of quantum resources in the BB84 protocol. Owing to the central limit theorem, the QBER measured by 300 quantum bits (qubits) is sufficient to guarantee lower than 0.009% of the FPR and FNR of eavesdropping detection. To deal with rapidly varying quantum channel conditions, this study further introduces grouped BB84 protocol and combinatory eavesdropping detection algorithms. A polarization basis is changeable for a group of qubits, and eavesdropping is judged by a combination of criteria between QBER and group-QBER in the proposed protocol and algorithms. In our extensive simulation study, the grouped BB84 protocol with 300 qubits comparison guarantees at least 99.92% accuracy in eavesdropping detection under rapidly varying quantum channel conditions.**

***Index Terms*—Communication system security, intrusion detection, network security, quantum cryptography.**

I. Introduction

REMARKABLE developments in information and communication technology (ICT) have resulted in an explosive increase in network users and traffic [1]. Accordingly, most offline services have been migrated to online platforms, including services dealing with sensitive information, such as banking, research data transfer, and medical care. The development in ICT requires a stricter level of network security [2]–[4], which cannot be satisfied by the number theory-based state-of-the-art cryptosystems [5], especially when quantum computers become publicly available [6].

Accordingly, quantum key distribution (QKD) technologies have gained industrial and academic interest, as it has been shown that QKD can provide unconditional secure communication at the physical layer [7]–[10]. In the QKD protocol, information can be encoded into the physical states of particles, where the state is referred to as a quantum bit (qubit). The QKD protocol exchanges a sequence of qubits between two entities (from Alice to Bob) in a secure manner against the presence of an eavesdropper (Eve). The secure exchange of qubits in the QKD protocol is guaranteed by the no-cloning principle in quantum mechanics [11]. The information encoded in the qubits can be used as a secret key to encrypt/decrypt the plaintext between Alice and Bob. In this study, we use the terms eavesdropper and Eve interchangeably.

The Bennett–Brassard-84 (BB84) protocol was the first QKD protocol [7]. Because the BB84 protocol is the most well-known QKD protocol, we regard BB84 as a basic QKD model throughout this study. Interestingly, intercept-and-resend-attack from Eve in the BB84 protocol cannot avoid affecting the original qubits, and thus, causes quantum bit errors [7]. This phenomenon in BB84 provides a new perspective and intuition for engineering problems for secure communications. However, because of the imperfections in the physical implementation of QKD systems, quantum errors in practical quantum channels are inevitable, even when an eavesdropper does not exist. Unfortunately, it is impossible to deterministically distinguish between quantum errors caused by Eve and those caused by quantum channels. Accordingly, as stated in [8], the majority of prior studies on QKD over practical noisy quantum channels has been concentrated on the secret key rate performance [8]–[10], rather than on detection of the presence of an eavesdropper. Because the secret key rate is calculated with respect to the quantum bit error rate (QBER) [8], the secret key rate can be excessively limited owing to the temporary poor quantum channel, even though the channel is free from Eve. In this study, in contrast to the existing research direction in the QKD community, we investigate the fundamental research aspects in the domain including statistically distinguishing quantum errors to detect eavesdropping in QKD protocols.

Although key distribution is the purpose of the QKD protocol, this study focuses on the detectability of eavesdropping in the BB84 QKD protocols, as accurate detection of eavesdropping can help key distribution performance as well. The remainder of this paper is organized as follows: In Section II, we review the procedure of the classical BB84 protocol, define performance metrics, study related works, and clarify contributions. Section III introduces a simple QBER comparison algorithm for the BB84 protocol and evaluates the algorithm using the upper bounds of the false positive ratio (*FPR*) and false negative ratio (*FNR*) of eavesdropping

Manuscript received 15 October 2021; revised 14 February 2022; accepted 31 March 2022. Date of publication 6 April 2022; date of current version 12 October 2022. This researchwas supported by the Korea Institute of Science and Technology Information (KISTI) (1711160642). *(Corresponding author: Chankyun Lee.)*

The authors are with the Advanced Quantum KREONET Team, Korea Institute of Science and Technology Information, Daejeon 34141, South Korea (e-mail: chankyunlee@kisti.re.kr).

Digital Object Identifier 10.1109/TNSM.2022.3165202

TABLE I
EXAMPLE OF ENCODING RULE BETWEEN A BINARY BIT AND A QUBIT (A POLARIZATION OF A PHOTON) IN THE 4-STATE BB84 PROTOCOL

Basis	Bit	Polarization of photon
Rectangular (+)	0	$\leftrightarrow$
	1	$\updownarrow$
Diagonal (×)	0	$\nearrow\!\!\!\swarrow$
	1	$\nwarrow\!\!\!\searrow$

detection. Section IV proposes a novel grouped BB84 protocol and corresponding combinatory eavesdropping detection algorithms to deal with rapidly varying quantum channel conditions. In Section V, we analyze the results from our extensive simulation and compare the security performance of the proposed protocols and algorithms. Finally, Section VI concludes the paper.

II. BACKGROUND AND CONTRIBUTIONS

This section reviews the step-by-step operational procedure of the classical BB84 protocol, defines performance metrics, studies related works, and summarizes the contributions of the study.

A. BB84 Protocol

We review the classical 4-state BB84 protocol [7] by assuming an ideal quantum channel condition, where eavesdropping is the only reason behind QBER > 0. First, Alice generates N binary bits that need to be transported to Bob. To encode a binary bit into a qubit, Alice randomly selects a polarization basis between the diagonal ($\times$) or rectangular ($+$). The encoding is performed using a publicly shared encoding rule. For example, with a rectangular basis, binary information 0 and 1 can be encoded by a qubit with $\leftrightarrow$ and $\updownarrow$ polarizations, respectively. Similarly, a qubit with $\nearrow\!\!\!\swarrow$ and $\nwarrow\!\!\!\searrow$ polarizations can represent 0 and 1 in a diagonal basis, respectively. An example of the encoding rule is presented in Table I. Because Alice does not share her sending basis, Bob randomly selects a basis between diagonal or rectangular to decode a receiving qubit. If the sending basis of Alice and the receiving basis of Bob are identical for a qubit, Bob can decode an original binary bit without error. Otherwise, the qubit from Alice randomly collapses into one qubit with respect to the basis of Bob. In the aforementioned example, if Alice encodes 0 into a qubit with $\leftrightarrow$ polarization and Bob selects a diagonal basis to receive the qubit, the qubit will randomly collapse into a qubit with $\nearrow\!\!\!\swarrow$ or $\nwarrow\!\!\!\searrow$ polarizations [7].

After transporting N qubits over the quantum channel, Alice and Bob discuss over the classical channel. Bob reports to Alice about his N receiving bases and Alice shares her identical sending bases. Assume that the number of qubits, whose bases between Alice and Bob are identical, is M. Then, Bob shares his decoding results for K qubits, which are subsets of M qubits. Alice can calculate QBER as the number of disagreeing bits in K, divided by K. Without Eve, the QBER must be measured as 0, under the ideal quantum channel conditions [7], [12]–[16].

TABLE II
SUMMARY OF TERMINOLOGIES FOR EAVESDROPPING DETECTION

Eavesdropper	Judgment	Terminology
Exist	Exist	True-positive (*TP*)
	Not exist	False-negative (*FN*)
Not exist	Exist	False-positive (*FP*)
	Not exist	True-negative (*TN*)

In the case of intercept-and-resend-attack from Eve, she randomly selects a basis between diagonal or rectangular to intercept a qubit from Alice and resend it to Bob. If the bases between Alice and Eve are identical for a given qubit, the qubit will not experience an error. Otherwise, the qubit will randomly collapse into a qubit associated with the basis used by Eve. Therefore, under the eavesdropping, Alice and Bob measure an average QBER as 25% ($= 50\% \times 50\%$), as the probability of nonidentical bases between Alice and Eve is 50% and half of them causes bit mismatch.

B. Performance Metrics and Notations

To evaluate the performance of eavesdropping detection, this study adopts the terminologies and metrics used in [17], [18], which are representative measures in anomaly detection research. Table II summarizes the terminologies of true-positive (*TP*), false-negative (*FN*), false-positive (*FP*), and true-negative (*TN*). For example, *TP* represents the number of correct judgments when Eve exists.

From the terminology, *accuracy* can be defined as a performance that is the ratio of the correct judgments to the total judgments made.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

Similarly, *FNR* and *FPR* are expressed as in (2) and (3) to describe the ratios of incorrect judgments with and without the presence of an eavesdropper, respectively.

$$FNR = \frac{FN}{FN + TP} \tag{2}$$

$$FPR = \frac{FP}{FP + TN} \tag{3}$$

Table III summarizes the notations and descriptions used in this paper.

C. Related Works

In the seminal paper on the BB84 protocol [7], Bennett and Brassard assumed a perfect quantum channel and thus, stated that the quantum transmission is free from Eve if the QBER is measured to be 0. Elboukhari *et al.* [12] calculated *FNR* in the classical 4-state BB84 to be $(3/4)^K$. In [13], Subramaniam and Parakh analyzed the *FNR* of the BB84 protocol to be $(1/2)^K$, when the number of bases in BB84 reached infinity. Zamani and Verma [14] proposed a QKD protocol with a two-way quantum channel and calculated the expected QBER as a function of K, which iteratively transmits qubits back and forth between Alice and Bob. In [15], Subramaniam and

TABLE III
NOTATIONS AND DESCRIPTIONS

Notation	Description
N	Number of transported qubits in the BB84 protocols
K	Number of qubits whose decoding results are shared
$\nu_{ch,K}$	QBER measured by K qubits without the presence of Eve
$\nu_{eve,K}$	QBER measured by K qubits with the presence of Eve
μ_{ch}	Genuine QBER without the presence of Eve
μ_{eve}	Genuine QBER with the presence of Eve
$b_{A=E}$	Events of identical bases between Alice and Eve
$b_{A\neq E}$	Events of non-identical bases between Alice and Eve
μ_{AE}	Average channel error between Alice and Eve
μ_{EB}	Average channel error between Eve and Bob
q_E^c	Events that a qubit collapses into error at basis of Eve
q_B^c	Events that a qubit collapses into error at basis of Bob
θ_{QBER}	QBER threshold in eavesdropping detection algorithms
α	Balancing parameter between *FPR* and *FNR*
μ_{ch}^{thr}	Genuine QBER without the presence of Eve, when calculating optimal θ_{QBER} at time t
μ_{ch}^{alg}	Genuine QBER without the presence of Eve, when applying eavesdropping detection algorithm at time $(t+\tau)$
G_i	Group of successive qubits ($\lvert G_i \rvert = b$)
$QBER_{G_i}$	QBER measured by b qubits in G_i
θ_{G-QBER}^{l}	Low threshold for group-QBER
θ_{G-QBER}^{h}	High threshold for group-QBER
γ^l	Low threshold for group ratio
γ^h	High threshold for group ratio

Parakh developed a quantum Diffie–Hellman protocol and calculated *FNR* to be $(1/2)^K$, when the number of bases of the protocol was infinite. Parakh [16] proposed a duplication-based quantum key transfer protocol and calculated the *FNR* as $(1/2)^{(\#\ of\ dup.)\times K/4}$, where Bob will realign a sequence of bases if he detects a change of qubits between duplications.

The quantum channels in previous eavesdropping detection studies in QKD protocols were considered as ideal, which is not practical. Moreover, although *FPR* is an important measure in security [19], it has been overlooked in previous research. To the best of our knowledge, this is the first study to statistically detect eavesdropping in QKD protocols for practical quantum channel conditions.

D. Summary of Contributions

Our contributions can be summarized as follows.

- We propose a simple eavesdropping detection algorithm that is highly compatible with the classical BB84 protocol. The algorithm judges the intercept-and-resend-attack from Eve by comparing the QBER and θ_{QBER}. We suggest an optimal θ_{QBER} by considering the relative importance between *FPR* and *FNR*.
- By exploring Hoeffding's inequality, we indicate the presence of a trade-off between the accuracy of eavesdropping detection and the economy of quantum resources. The upper bounds of the *FPR* and *FNR* of eavesdropping detection in the proposed algorithm exponentially decrease with respect to the increase in *K*.
- To provide secure communications for rapidly varying quantum channel conditions, we propose a novel design of a grouped BB84 protocol that maintains a polarization basis for a group of bits. We further introduce combinatory eavesdropping detection algorithms that combine QBER and group-QBER criteria for accurate eavesdropping judgment.
- We empirically find solutions for thresholds in the proposed protocols and algorithms from extensive simulation studies. We show that the grouped BB84 protocol with optimized algorithms can guarantee a high level of security performance, whereas the classical BB84 protocol fails to do so.

III. EAVESDROPPING DETECTION IN THE CLASSICAL BB84 PROTOCOL

As described in Section II, Alice can measure the QBER by comparing K qubits with Bob in the BB84 protocol. Since a period of an individual qubit transmission is shared between Alice and Bob, study on existence of the individual qubit in signal processing is out of interest of this paper. A qubit may experience errors due to imperfections in the implementation of QKD systems, such as multiple photon generation in a pulse, attenuation in a fiber, and dark current at a photo detector [5], [8]. We define a term, channel error, to represent errors resulting from imperfections in the implementation of the QKD system. We model the channel error as a single random variable and assume independent and identically distributed (i.i.d.) channel errors for each qubit [20]. Therefore, the channel error events of each qubit can be modeled as independent Bernoulli random variables.

A. QBER Comparison Algorithm for Eavesdropping Detection

In this study, we assume that Eve launches an intercept-and-resend-attack on all qubits between Alice and Bob. Therefore, the measured QBER can be modeled by the case of either with or without the presence of Eve. Without the presence of Eve, the Bernoulli random variables $Q_{ch,1}, Q_{ch,2} \cdots Q_{ch,K}$ represent the channel error events of each qubit. $Q_{ch,i}$ is 1 if Alice and Bob disagree on the ith qubit; otherwise, it is 0. Now, Alice calculates the QBER as

$$\nu_{ch,K} = \frac{1}{K}\sum_{i=1}^{K} Q_{ch,i}. \tag{4}$$

Similarly, with the presence of Eve, the QBER measured by K qubits can be expressed as

$$\nu_{eve,K} = \frac{1}{K}\sum_{i=1}^{K} Q_{eve,i} \tag{5}$$

where $Q_{eve,i}$ is a Bernoulli random variable for the error event of an ith qubit with the presence of Eve. Notably,

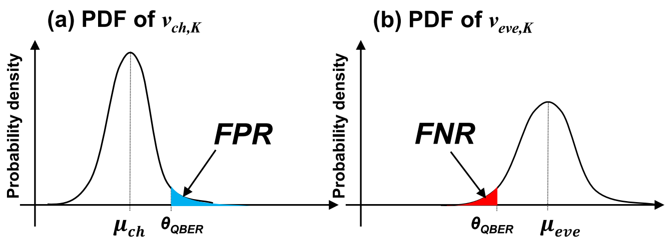

Fig. 1. PDFs of $\nu_{ch,K}$ (a) and $\nu_{eve,K}$ (b) with K qubits comparisons. *FPR* and *FNR* are illustrated with respect to θ_{QBER} in the proposed QBER comparison algorithm.

both channel error and eavesdropping affect $Q_{eve,i}$. Owing to the central limit theorem [21], both $\nu_{ch,K}$ and $\nu_{eve,K}$ can be approximated by normal distributions, if K is sufficiently large, for example, $K > 30$ [22]. Therefore, the probability density functions (PDFs) of $\nu_{ch,K}$ and $\nu_{eve,K}$ can be modeled by normal distributions represented by $N(\mu_{ch}, \sigma^2_{ch}/K)$ and $N(\mu_{eve}, \sigma^2_{eve}/K)$, as illustrated in Figs. 1 (a) and (b), respectively. Please note that μ_{ch} and μ_{eve} are genuine QBERs without and with the presence of Eve, which can be calculated using (4) and (5) with $K = \infty$, respectively.

We can categorize error event of qubit for cases of identical and non-identical bases between Alice and Eve. Please note that we omit consideration of basis of Bob, because QBER is measured only when bases between Alice and Bob are identical. Then μ_{eve} is expressed as $p(b_{A=E})p$ (qubit experience odd number of bit flip $|b_{A=E}) + p(b_{A\neq E})p$ (qubit experience odd number of bit flip $|b_{A\neq E})$. Appendix A describes all the bit flip events with associated probability. We assume that error events described at Table V in Appendix A are independent each other. Therefore, μ_{eve} can be calculated as (6), by a summation of probability of all error events in Table V.

$$\begin{aligned}\mu_{eve} = {} & p(b_{A=E})\{\mu_{AE}(1-\mu_{EB}) + (1-\mu_{AE})\mu_{EB}\} \\ & + p\big(b_{A\neq E}\big)p\big(q^c_E|b_{A\neq E}\big)\big(1 - p\big(q^c_B|b_{A\neq E}\big)\big) \\ & \times \{\mu_{AE}\mu_{EB} + (1-\mu_{AE})(1-\mu_{EB})\} \\ & + p\big(b_{A\neq E}\big)\big(1 - p\big(q^c_E|b_{A\neq E}\big)\big)p\big(q^c_B|b_{A\neq E}\big) \\ & \times \{\mu_{AE}\mu_{EB} + (1-\mu_{AE})(1-\mu_{EB})\} \\ & + p\big(b_{A\neq E}\big)p\big(q^c_E|b_{A\neq E}\big)p\big(q^c_B|b_{A\neq E}\big) \\ & \times \{\mu_{AE}(1-\mu_{EB}) + (1-\mu_{AE})\mu_{EB}\} \\ & + p\big(b_{A\neq E}\big)\big(1 - p\big(q^c_E|b_{A\neq E}\big)\big)\big(1 - p\big(q^c_B|b_{A\neq E}\big)\big) \\ & \times \{\mu_{AE}(1-\mu_{EB}) + (1-\mu_{AE})\mu_{EB}\} \end{aligned} \quad (6)$$

In (6), $p(b_{A=E})$, $p(b_{A\neq E})$, μ_{AE}, μ_{EB}, $p(q^c_E|b_{A\neq E})$, and $p(q^c_B|b_{A\neq E})$ represent the probability of identical bases between Alice and Eve, the probability of non-identical bases between Alice and Eve, the average channel error between Alice and Eve, the average channel error between Eve and Bob, the conditional probability that binary information is flipped due to a basis of Eve when $b_{A=E}$, and the conditional probability that binary information is flipped due to a basis of Bob when $b_{A=E}$, respectively.

Because the QBER in BB84 is measured by qubits whose bases are identical between Alice and Bob, $b_{A=E}$ in (6) represent events when the bases of Alice, Eve, and Bob are all identical. Similarly, $b_{A\neq E}$ in (6) represent events when the bases of Alice and Bob are identical; however, that of Eve is nonidentical. The first term in (6) calculates the probability that Alice and Eve select identical bases for a given qubit, and binary information encoded in the qubit is flipped once because of the channel error between Alice and Eve or between Eve and Bob. The remaining terms consider the events when Alice and Eve select nonidentical bases for a given qubit. For the nonidentical bases, the second and third terms in (6) calculate the probabilities that the bases of Eve or Bob flip binary information encoded in the qubit once and channel error does not flip or flips twice. Similarly, the fourth and last terms in (6) calculate the probabilities that the channel error flips a binary information encoded in the qubit once, and the bases of Eve and Bob do not flip or flip twice, for the nonidentical bases. Because Alice and Eve randomly select their bases, $p(b_{A=E}) = p(b_{A\neq E}) = 1/2$. In the 4-state BB84 model, $p(q^c_E|b_{A\neq E}) = p(q^c_B|b_{A\neq E}) = 1/2$. If we assume that the average channel error between any two entities is the same, namely $\mu_{AE} = \mu_{EB} = \mu_{ch}$, we can simplify (6) as

$$\mu_{eve} = 0.25 + \mu_{ch} - \mu^2_{ch}. \quad (7)$$

Please note that the assumption of an ideal quantum channel ($\mu_{ch} = 0$) for (7) results in μ_{eve} to be 25%, same to [7], [12]–[16].

The deterministic distinction between quantum error caused by Eve and that caused by quantum channel is not achievable because of the intersection between the PDFs of $\nu_{ch,K}$ and $\nu_{eve,K}$ in Figs. 1 (a) and (b). Fortunately, owing to the central limit theorem, an increase in K effectively reduces the variances of each distribution while maintaining averages. Moreover, with a first-order approximation, the distance between μ_{ch} and μ_{eve} in (7) remains at 25%, even though we consider a practical quantum channel condition. From these observations, we propose a QBER comparison eavesdropping detection algorithm that is highly compatible with the classical BB84 protocol. The QBER comparison algorithm judges eavesdropping by comparing the measured QBER to a threshold (θ_{QBER}). In this algorithm, *FN* increases when $\nu_{eve,K}$ is lower than a given θ_{QBER} in the presence of Eve. Conversely, without the presence of Eve, *FP* increases when $\nu_{ch,K}$ is equal to or higher than θ_{QBER}. It is expected that an appropriate θ_{QBER} with a sufficiently large K in the proposed algorithm can effectively detect eavesdropping, with negligibly small *FPR* and *FNR*. We limit θ_{QBER} to a real number within the range (μ_{ch}, μ_{eve}).

B. Bounds

The *FPR* can be calculated by integrating the distribution of $\nu_{ch,K}$, from θ_{QBER} to infinity. However, to consider a diverse range of K, we calculate the upper bound of *FPR*. Using ε_{FP} to denote $\theta_{QBER} - \mu_{ch}$, *FPR* and its upper bound is expressed as (8). The upper bound is calculated by Hoeffding's inequality, which can calculate the bound of the difference between the genuine and empirical means from the K-sample [23]. The upper bound is expressed by an exponential function with

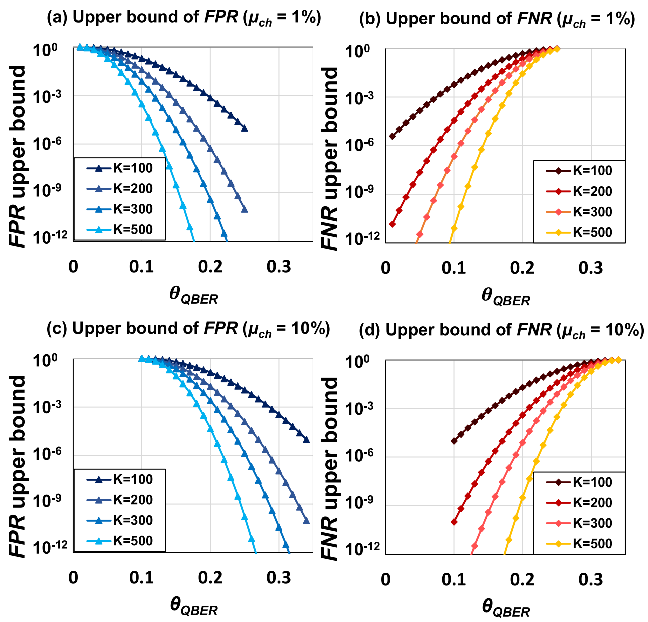

Fig. 2. Numerical analysis for upper bounds of *FPR* and *FNR* for diverse K and θ_{QBER}. ($\mu_{ch} = 1\%$ and 10%).

respect to θ_{QBER}, μ_{ch}, and K.

$$\begin{aligned} FPR &= p\left[\nu_{ch,K} \geq \theta_{QBER}\right] \\ &= p\left[\nu_{ch,K} - \mu_{ch} \geq \theta_{QBER} - \mu_{ch}\right] \\ &= p\left[\nu_{ch,K} - \mu_{ch} \geq \varepsilon_{FP}\right] \;\leq e^{-2\varepsilon_{FP}^2 K} \end{aligned} \tag{8}$$

Similarly, upper bound of *FNR* is written as

$$\begin{aligned} FNR &= p\left[\nu_{eve,K} \leq \theta_{QBER}\right] \\ &= p\left[\mu_{eve} - \nu_{eve,K} \geq \mu_{eve} - \theta_{QBER}\right] \\ &= p\left[\mu_{eve} - \nu_{eve,K} \geq \varepsilon_{FN}\right] \;\leq e^{-2\varepsilon_{FN}^2 K} \end{aligned} \tag{9}$$

where ε_{FN} is $\mu_{eve} - \theta_{QBER}$. Because μ_{eve} can be calculated by a function of μ_{ch} using (7), the upper bounds of *FNR* can be written as a function of θ_{QBER}, μ_{ch}, and K, as well.

Figure 2 depicts the upper bounds of *FPR* and *FNR* of eavesdropping detection for diverse K and θ_{QBER}, calculated by (8) and (9). We considered 1% and 10% for μ_{ch}. As expected, the increase in K exponentially reduces the upper bounds of *FPR* and *FNR*. Figure 2 clarifies the trade-off between the security performance of the algorithm and the economy of quantum resources in the BB84 protocol. Because a qubit is a costly quantum resource, careful selection of K is required by considering the security criteria of the networking service. For example, as shown in Fig. 2 (a) and (b), comparison of 300 qubits for QBER is sufficient to guarantee lower than 0.009% of *FPR* and *FNR*, if we set θ_{QBER} to 0.135. A small θ_{QBER} effectively reduces the upper bound of *FNR* at the cost of increasing the upper bound of *FPR*. Similarly, a large θ_{QBER} improves the upper bound of *FPR* by sacrificing the upper bound of *FNR*. Therefore, the selection of an appropriate θ_{QBER} is a significantly important problem in the proposed algorithm.

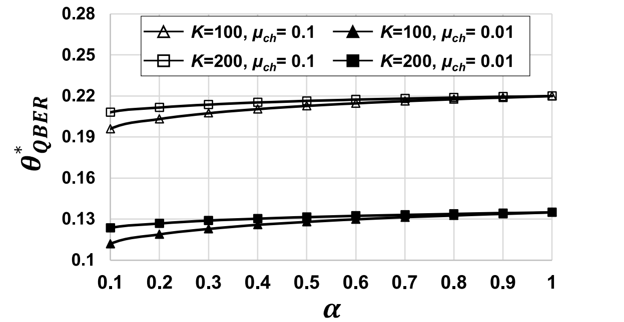

Fig. 3. Optimal θ_{QBER} for the proposed algorithm for diverse α, K, and μ_{ch}.

C. Optimal Threshold

We define an optimal θ_{QBER} that satisfies

$$\theta^*_{QBER} = \underset{\theta_{QBER}}{\arg\min} \left(e^{-2\varepsilon_{FN}^2 K} + \alpha e^{-2\varepsilon_{FP}^2 K}\right). \tag{10}$$

The objective function in (10) is a summation of the upper bound of *FNR* and the weighted upper bound of *FPR* by a balancing parameter α ($0 \leq \alpha \leq 1$), as the reduction of *FN* is practically important in security [12]–[16], [18]. Both the first and second terms in (10) are differentiable. Therefore, we can find an optimal θ_{QBER} by differentiating the objective function with respect to θ_{QBER}.

$$\begin{aligned} 0 = &\, e^{-2K\left(\theta^*_{QBER} - \mu_{ch}(1-\mu_{ch}) - 0.25\right)^2} \\ &\times 4K\left(0.25 + \mu_{ch}(1-\mu_{ch}) - \theta^*_{QBER}\right) \\ &+ \alpha e^{-2K\left(\theta^*_{QBER} - \mu_{ch}\right)^2} 4K\left(\mu_{ch} - \theta^*_{QBER}\right) \end{aligned} \tag{11}$$

According to the Appendix B, the optimal θ_{QBER} for the proposed algorithm can be expressed as (12), with respect to α, μ_{ch}, and K.

$$\theta^*_{QBER} = \frac{\ln \alpha + 2K\left\{\mu_{ch}^2(1-\mu_{ch})^2 - \mu_{ch}^2 + 0.5\mu_{ch}(1-\mu_{ch}) + 0.25^2\right\}}{K\left(1-4\mu_{ch}^2\right)}. \tag{12}$$

The optimal θ_{QBER} in (12) under the ideal quantum channel condition is calculated as $(\ln \alpha)/K + 0.125$. If we further assume equal importance between *FPR* and *FNR*, the optimal θ_{QBER} is calculated as 12.5% which is half of 25%.

Figure 3 plots optimal θ_{QBER} calculated by (12). In a small α regime, the objective function in (10) finds an optimal θ_{QBER}, which lowers the upper bound of *FNR*. Therefore, the optimal θ_{QBER} in Fig. 3 follows a monotonic decrease with respect to the decrease of α. From (8) and (9), the upper bounds of *FPR* and *FNR* for a given K are symmetric to the $\theta_{QBER} = 0.125 + \mu_{ch} - 0.5\mu_{ch}^2$. Therefore, when α is 1, the optimal θ_{QBER} in (12) is independent of K and plotted at $0.125 + \mu_{ch} - 0.5\mu_{ch}^2$ in Fig. 3. As expected, a large μ_{ch} finds a large optimal θ_{QBER}.

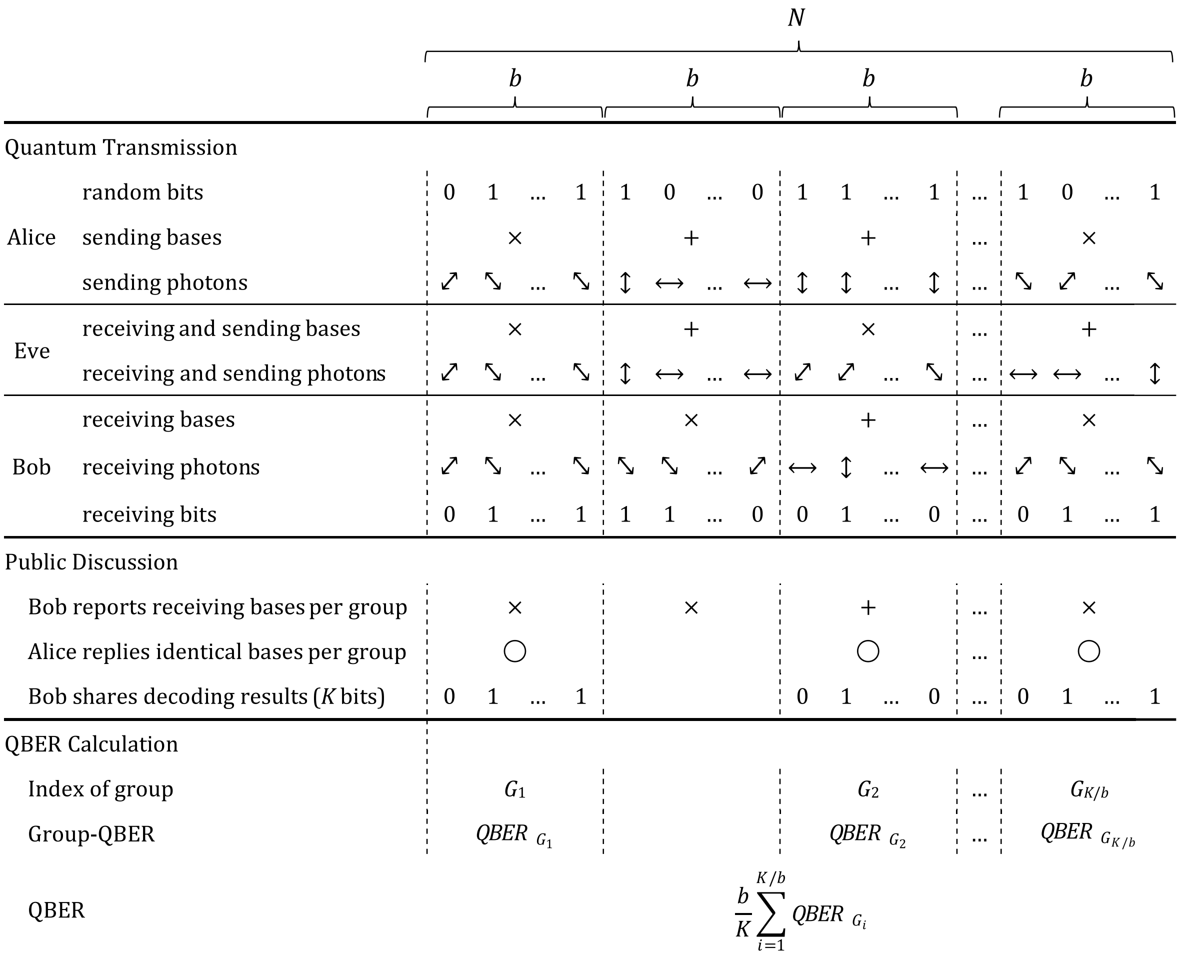

Fig. 4. Example of the grouped BB84 protocol with presence of Eve. A polarization basis is maintained during encoding b bits in a group.

IV. Eavesdropping Detection in the Grouped BB84 Protocol

The optimal θ_{QBER} in (12) requires information of μ_{ch}. However, accurate estimation of μ_{ch} is infeasible in the practical communication networks. In this paper, we assume that Alice and Bob can approximate μ_{ch} before QKD transmission. According to [24], Alice and Bob can approximately predict μ_{ch} from the quantum interference visibility, before actual QKD transmission. A gap between the predicted and measured QBERs lies within 1% in 120km QKD transmission. Moreover, it is shown that fluctuation of QBER in QKD transmission lies within 0.16% during 70-hour monitoring period [25].

The proposed QBER comparison eavesdropping detection algorithm in Section III assumes a stationary quantum channel condition where μ_{ch} does not change over time. In practical time-varying quantum channel conditions, an optimal θ_{QBER} calculated by a function of μ_{ch} at time t can be outdated when it is applied at time $t+\tau(\tau > 0)$. Moreover, if an eavesdropper has prior knowledge of our QBER comparison algorithm, the eavesdropper can degrade the security performance of the algorithm by manipulating the QKD devices and rapidly changing the quantum channel error. We define μ_{ch}^{thr} and μ_{ch}^{alg} for genuine QBERs on the quantum channel when calculating an optimal θ_{QBER} at t, and applying the eavesdropping detection algorithm at $t+\tau$, respectively. For example, the optimal θ_{QBER} is calculated to be 0.135 from (12), when $\mu_{ch}^{thr} = 1\%$, $K = 200$, and $\alpha = 1$. However, if μ_{ch}^{alg} changes to 10%, the upper bound of *FPR* is calculated as 61% from (8), which is not acceptable for a practical system. To provide highly secure communications for rapidly varying quantum channel conditions, Section IV proposes a grouped BB84 protocol with associated eavesdropping detection algorithms.

A. Grouped BB84 Protocol

As described in (8) and (9), the decreasing slopes of the upper bounds of *FPR* and *FNR* of eavesdropping detection with respect to the increase in K becomes smaller when K is large. To effectively exploit the limited qubit resources, we introduce a grouped BB84 protocol, as shown in Fig. 4. Alice generates a sequence of N random binary bits. She randomly selects a polarization basis between diagonal ($\times$) and rectangular ($+$) bases, which is maintained during encoding b bits in a row. The example in Fig. 4 assumes the encoding rule shown in Table I. We define a group to represent a set of successive b

qubits. An example of an intercept-and-resend-attack by Eve and decoding by Bob is shown in Fig. 4. A value of b can be selected as a divisor of N. Because the value of b is publicly shared, Alice and Bob can maintain a basis for a group using a counter.

We assume that Eve has prior knowledge of the grouped BB84 protocol. Under this assumption, Eve can spoil the protocol by changing her polarization basis within b qubits. Therefore, maximum size of b is limited by photon pulse interval of pulse generator of Alice, minimum required switching time of polarization switch of Eve, and dead time of photo detector of Bob. With state-of-the-art technology, we assume that Alice is with 100GHz level photon generator [26], [27], Eve is with LiNbO3 technology-based tens of MHz switch [28], and Bob is with tens of ns dead time photo detector [29], [30]. If Bob takes advantage of multiplexed single photon detector technology [31], it is sufficient to set b as thousands of qubits. For the photo detector, avalanche photodiode with a single photon counting method can detect qubits in the noisy channel. Superconducting single photon detector operated in the cryogenic environment can achieve extremely low dark counts, due to the low noise [32].

After sending all qubits over the quantum channel, Alice and Bob discuss their bases over a public channel. Bob reports his receiving bases for groups, Alice replies identical bases, and Bob shares parts of his decoding results of qubits regarding identical bases. The bases between Alice and Bob are either identical or nonidentical for b qubits in a group. If the bases of Alice and Bob are identical for a group, Bob shares the decoding results of whole or nothing of the b qubits in the group. In other words, in the proposed grouped BB84 protocol, the minimum period of basis change and the granularity of decoding results sharing are b, which is the cardinality of a group.

Bob shares his decoding results of K qubits. Alice categorizes the K qubits into groups and indexes them from G_1 to $G_{K/b}$. The grouped BB84 protocol measures two types of error statistics between Alice and Bob; group-QBER and QBER. The group-QBER is a set of measured QBERs for each group. The cardinality of the group-QBER is K/b. Because we consider an equivalent cardinality for all groups, the QBER can be calculated by averaging the group-QBER. For example, assume that K and b are 100 and 20, respectively. Bob shares the decoding results of qubits in G_1, G_2, G_3, G_4, and G_5. If the number of disagree bits between Alice and Bob in each group is 2, 11, 1, 10, and 2, the group-QBER and QBER are calculated to be $\{0.1, 0.55, 0.05, 0.5, 0.1\}$ and 0.26, respectively. Due to the identical error event assumption for each qubit, the grouped BB84 protocol does not affect QBER and secret key rate from those of the classical BB84 protocol.

B. Combinatory Eavesdropping Detection Algorithms for the Grouped BB84 Protocol

Figures 5 (a) and (b) illustrate the flow charts of the proposed combinatory eavesdropping detection algorithms for the grouped BB84 protocol. This paper suggests two types of combinatory algorithms to judge Eve; combining QBER and group-QBER criteria with "or" and "and" operations, as shown in Figs. 5 (a) and (b), respectively. In Fig. 5 (a), an eavesdropping is judged, unless both the QBER and group-QBER criteria are not satisfied. The QBER and group-QBER comparison algorithm in Fig. 5 (b) judges eavesdropping if both QBER and group-QBER criteria are satisfied. The QBER criterion is satisfied when the measured QBER is equal to or higher than a threshold, which is the same as the QBER comparison algorithm introduced in Section III. The group-QBER criterion will be met if both (13) and (14) are satisfied.

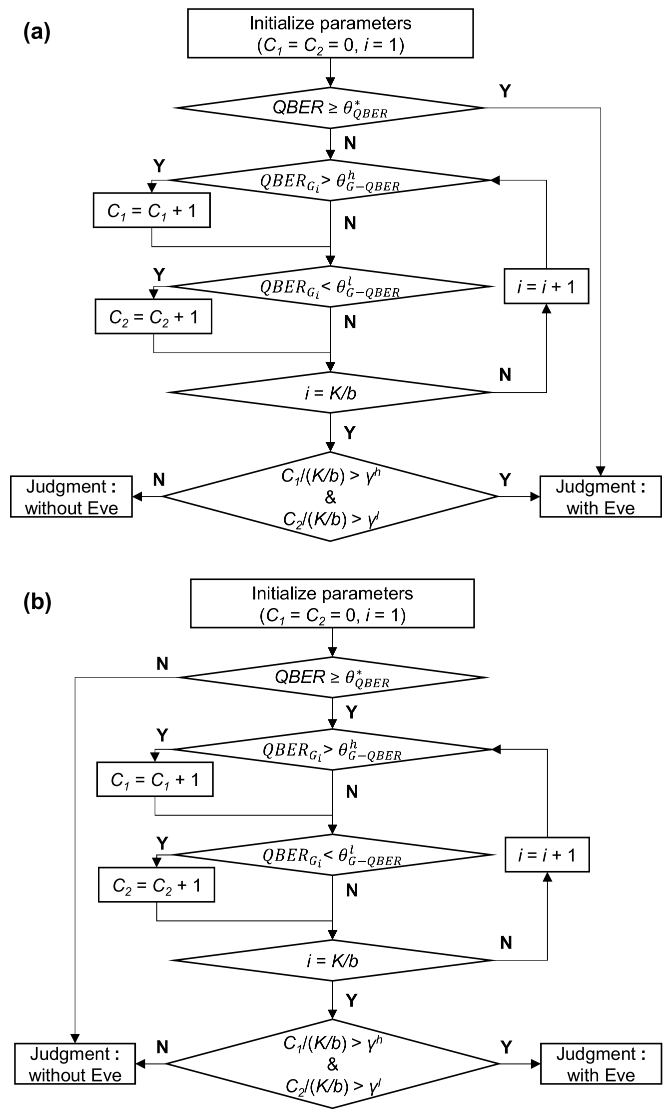

Fig. 5. Flow charts of combinatory eavesdropping detection algorithms with "or" (a) and "and" (b) operations between QBER and group-QBER to judge eavesdropping.

$$\frac{\sum_{i=1}^{K/b} I_{QBER_{G_i} > \theta^h_{G-QBER}}}{K/b} > \gamma^h \tag{13}$$

$$\frac{\sum_{i=1}^{K/b} I_{QBER_{G_i} < \theta^l_{G-QBER}}}{K/b} > \gamma^l \tag{14}$$

Here, I_x is 1 if x is true and 0 otherwise. Regarding a group-QBER set, (13) represents a condition in which the ratio of elements whose QBER is higher than θ^h_{G-QBER} is higher than γ^h. Similarly, (14) will be satisfied if the ratio of elements whose QBER is lower than θ^l_{G-QBER}, is higher than γ^l. Please note that the "or" operation in Fig. 5 (a) relaxes the criteria for eavesdropping judgment so that it can effectively reduce *FN* at the cost of *FP*, from the QBER comparison algorithm.

C. Thresholds and Group Size

The security performance of the proposed algorithms highly depends on the thresholds ($\theta_{QBER}, \theta^h_{G-QBER}, \theta^l_{G-QBER}, \gamma^h, \gamma^l$) and group size b. We first calculate and fix an optimal θ_{QBER} using (12) for a given K, α, and μ^{thr}_{ch}. Then, using (15), we find a solution for thresholds ($\theta^h_{G-QBER}, \theta^l_{G-QBER}, \gamma^h, \gamma^l$) and a group size b, for a given K, α, and the optimal θ_{QBER}.

$$\underset{\left(\theta^h_{G-QBER},\theta^l_{G-QBER},\gamma^h,\gamma^l,b\right)}{\arg\min} \left[\sum_{a=1}^{a_{\max}} \left\{ FNR\left(\frac{a}{100}, K, \theta^*_{QBER}, \theta^h_{G-QBER}, \theta^l_{G-QBER}, \gamma^h, \gamma^l, b\right) + \alpha FPR\left(\frac{a}{100}, K, \theta^*_{QBER}, \theta^h_{G-QBER}, \theta^l_{G-QBER}, \gamma^h, \gamma^l, b\right)\right\}\right] \tag{15}$$

Because our purpose is to provide secure communications through the rapidly varying quantum channel conditions, (15) aims to minimize the summation of *FNR* and weighted *FPR* by assuming $\mu^{thr}_{ch} \neq \mu^{alg}_{ch}$ conditions. In (15), we assume that μ^{alg}_{ch} is independent of μ^{thr}_{ch} and distributed uniformly from 1% to $a_{max}\%$. By considering the relative importance between *FPR* and *FNP*, the *FPR* is weighted by a balancing parameter α, where $0 \leq \alpha \leq 1$.

For a given K, α, and optimal θ_{QBER}, we empirically solve (15) using an extensive simulation study over searching spaces of the variables ($\theta^h_{G-QBER}, \theta^l_{G-QBER}, \gamma^h, \gamma^l, b$). The search space of b is the divisors of K. Similarly, the search spaces of $\theta^h_{G-QBER}, \theta^l_{G-QBER}, \gamma^h$, and γ^l in the simulation span [0.3, 0.8], [0, 0.4], [0.1, 0.5], and [0.1, 0.5], respectively. A step-size in the simulation is 0.01 for $\theta^h_{G-QBER}, \theta^l_{G-QBER}, \gamma^h$, and γ^l. Table VI in the Appendix C summarizes the empirical solutions of ($\theta^h_{G-QBER}, \theta^l_{G-QBER}, \gamma^h, \gamma^l, b$) for $K = \{100, 200, 300\}$, $\alpha = \{0.1, 0.5, 1\}$, and $\mu^{thr}_{ch} = \{0.01, 0.05, 0.1\}$. The value of a_{max} is assumed to be 10.

V. Performance Evaluations

Table IV summarizes cases of combination between QKD protocol and eavesdropping detection algorithm investigated in this paper. We define Case 1 for the QBER comparison algorithm over classical BB84 protocol. Similarly, Case 2 and Case 3 represent algorithms illustrated in Fig. 5 (a) and Fig. 5 (b) with the grouped BB84 protocol, respectively. From the protocol perspective, one can regard Case 1 as a conventional method, since it runs over the classical BB84 protocol. We evaluate the security performance (*FPR*, *FNR*, and *accuracy*) of Cases from extensive simulation studies. Figures 6–8 and 9–11 summarize the simulation results of *FPR*, *FNR*, and *accuracy* for $K = 100$ and 300, respectively. In each figure, the subfigures (a), (b), (c), and (d) depict the security performance for ($\alpha = 0.1, \mu^{alg}_{ch} = 1\%$), ($\alpha = 1, \mu^{alg}_{ch} = 1\%$), ($\alpha = 0.1, \mu^{alg}_{ch} = 10\%$), and ($\alpha = 1, \mu^{alg}_{ch} = 10\%$), respectively. The curve with black circular data points indicates the performance of the Case 1, which judges eavesdropping by comparing QBER and θ^*_{QBER}. Red triangle and blue rectangular curves represent the performance of the Case 2 and Case 3, respectively. For the Cases, the thresholds and group sizes summarized at Table VI in Appendix C are used for the simulations. The performance is plotted by averaging 10,000 iterations of simulations. We consider $N =$ 10,000 for each iteration and randomly select 100 and 300 qubits for K to calculate the QBER.

TABLE IV
Cases of Combination Between QKD Protocol and Algorithm

Notation	QKD protocol	Eve detection algorithm
Case 1	Classical BB84 [7]	QBER comparison (Sect. III. A)
Case 2	Grouped BB84 (Sect. IV. A)	QBER or group-QBER (Fig. 5 (a))
Case 3	Grouped BB84 (Sect. IV. A)	QBER and group-QBER (Fig. 5 (b))

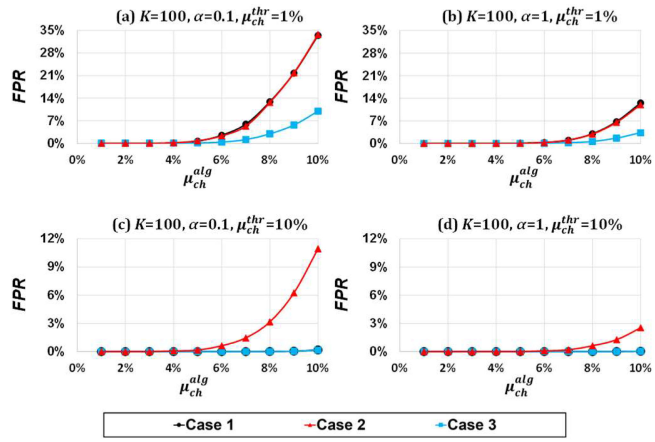

Fig. 6. *FPR* comparisons between Cases with $K = 100$.

A. FPR

When $\mu^{thr}_{ch} < \mu^{alg}_{ch}$, all Cases cause a number of *FPs*, because the optimal θ_{QBER} calculated by μ^{thr}_{ch} becomes too small for actual operation μ^{alg}_{ch}. Conversely, when μ^{alg}_{ch} is small, all Cases show negligibly small *FPRs*, as shown in Figs. 6 and 9, regardless of μ^{thr}_{ch}. The Case 1 finds an optimal θ_{QBER} by assuming that $\mu^{thr}_{ch} = \mu^{alg}_{ch}$. Therefore, as shown in Figs. 6 (a), 6 (b), 9 (a), and 9 (b), when $\mu^{thr}_{ch} < \mu^{alg}_{ch}$, the Case 1 suffers from severe *FPR*. The Case 2 shows similar *FPR* performance to those of the Case 1 in these realms. However, strict criteria for judgment of eavesdropping in the Case 3 can effectively reduce the *FPR* for $\mu^{thr}_{ch} < \mu^{alg}_{ch}$ cases.

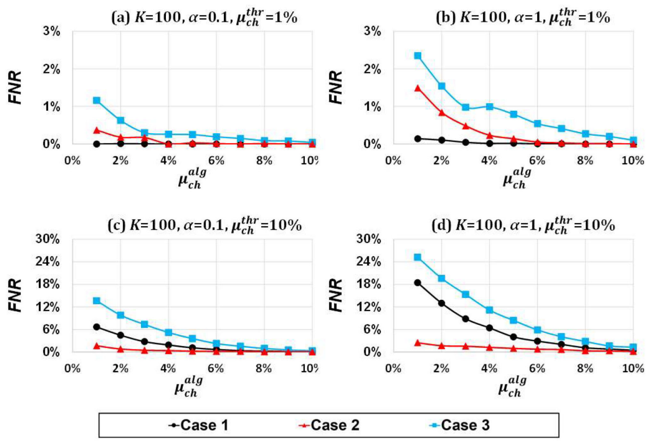

Fig. 7. *FNR* comparisons between Cases with $K = 100$.

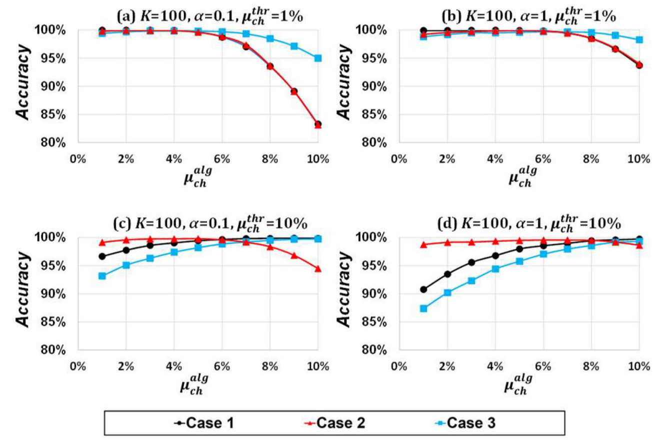

Fig. 8. *Accuracy* comparisons between Cases with $K = 100$.

For large μ_{ch}^{thr} and μ_{ch}^{alg}, as shown in Figs. 6 (c), 6 (d), 9 (c), and 9 (d), both the Case 1 and Case 3 achieve negligibly small *FPR*. However, owing to the relaxation of criteria for judgment of eavesdropping in the algorithm, Case 2 shows poor *FPR* performance. A small α results in poor *FPR* performance for all Cases, because the importance of *FPR* weakens when α is small.

B. FNR

When $\mu_{ch}^{thr} > \mu_{ch}^{alg}$, the optimal value for θ_{QBER} in the Case 1 becomes unnecessarily large for actual μ_{ch}^{alg}, and thus may cause a number of *FNs*, as shown in Figs. 7 (c), 7 (d), 10 (c), and 10 (d). The Case 3 suffers from the worst *FNR* in these areas owing to the strict criteria for judgment of eavesdropping. However, owing to the relaxation of criteria for judgment of eavesdropping, the Case 2 effectively achieves the best *FNR* performance for the cases $\mu_{ch}^{thr} > \mu_{ch}^{alg}$. As shown in Figs. 7 (a) and (b), when both μ_{ch}^{thr} and μ_{ch}^{alg} are small and *K* is small, the Case 2 and Case 3 show relatively poor *FNR* performance because the combinatory algorithms divide *K* into groups to judge eavesdropping, which degrades the accuracy of eavesdropping detection. However, when *K* is sufficiently large, as shown in Figs. 10 (a) and (b), dividing *K* into groups rarely affects accuracy. As expected, a small α improves the *FNR* performance of all Cases.

We calculate the optimal θ_{QBER} from upper bounds of *FPR* and *FNR*, which lacks the consideration of variance of $\nu_{eve,K}$ and $\nu_{ch,K}$. In the practical condition $(0 < \mu_{ch} < \mu_{eve} < 0.5)$, variance of $\nu_{eve,K}$ is larger than that of $\nu_{ch,K}$. Therefore, as shown in Figs. 6 (b), 6 (d), 7 (b), and 7 (d), Case 1 shows *FPR*-favorable performance, even though $\alpha = 1$. As shown in Figs. 9 (b), 9 (d), 10 (b), and 10 (d), a large *K* reduces the gap between *FPR* and *FNR* of Case 1.

C. Accuracy

As defined by (1), *FP* and *FN* directly affect *accuracy*. In the proposed eavesdropping detection algorithms, the majority of *FP* and *FN* are produced when $\mu_{ch}^{thr} < \mu_{ch}^{alg}$ and $\mu_{ch}^{thr} > \mu_{ch}^{alg}$, respectively. When $\mu_{ch}^{thr} \approx \mu_{ch}^{alg}$, the Case 1

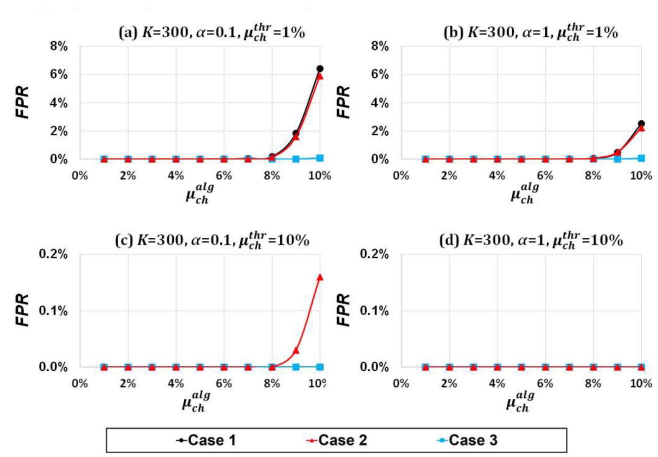

Fig. 9. *FPR* comparisons between Cases with $K = 300$.

shows good *accuracy* performance in Figs. 8 and 11, because it calculates an optimal θ_{QBER} by assuming $\mu_{ch}^{thr} = \mu_{ch}^{alg}$. In our simulation study for $\mu_{ch}^{thr} = \mu_{ch}^{alg}$ conditions, the worst *accuracy* of the Case 1 is 99.75%, as shown at $\mu_{ch}^{alg} = 10\%$ in Fig. 8 (d). However, increase of *FP* at $\mu_{ch}^{thr} < \mu_{ch}^{alg}$ and increase of *FN* at $\mu_{ch}^{thr} > \mu_{ch}^{alg}$ critically degrade *accuracy* performance of the Case 1. For example, the worst *accuracies* of the Case 1 over the entire simulation conditions are 83.28% ($\mu_{ch}^{alg} = 10\%$ in Fig. 8 (a)) and 96.79% ($\mu_{ch}^{alg} = 10\%$ in Fig. 11 (a)), when $K = 100$ and 300, respectively.

The strict criteria for judgment of eavesdropping in the Case 3 effectively lowers *FP*, and thus introduces a high level of *accuracy* in cases of $\mu_{ch}^{thr} < \mu_{ch}^{alg}$, as shown in Figs. 8 (a), 8 (b), 11 (a), and 11 (b). The Case 3 achieves a maximum of 12% higher *accuracy* than that of the Case 1, as shown at $\mu_{ch}^{alg} = 10\%$ in Fig. 8 (a). With a large *K*, the Case 3 achieves 99.98% *accuracy* at $\mu_{ch}^{alg} = 10\%$ in Fig. 11 (a) and 99.97% *accuracy* at $\mu_{ch}^{alg} = 10\%$ in Fig. 11 (b), whereas others fail. However, an increase in *FN* due to the strict criteria degrades *accuracy* when $\mu_{ch}^{thr} > \mu_{ch}^{alg}$. Based on the observations, we can highlight that the Case 3 can be an appropriate solution when the value of μ_{ch}^{thr} is small.

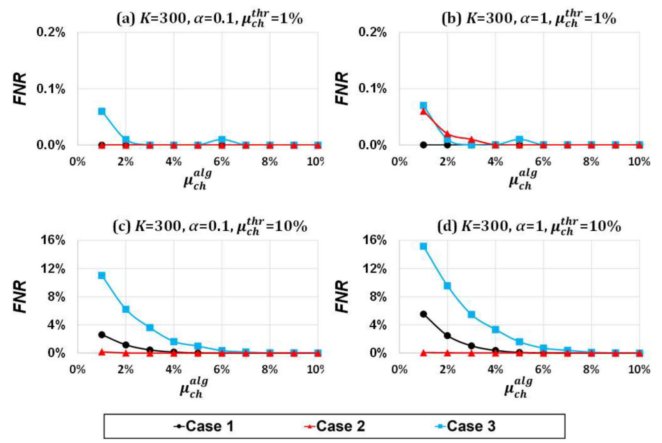

Fig. 10. *FNR* comparisons between Cases with $K = 300$.

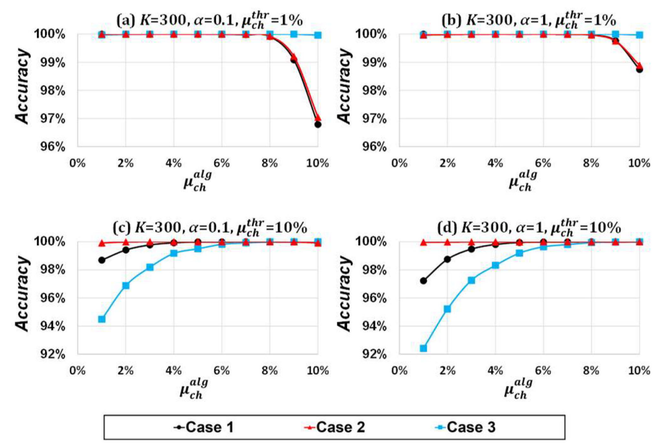

Fig. 11. *Accuracy* comparisons between Cases with $K = 300$.

The relaxation of criteria for judgment of eavesdropping in the Case 2 effectively reduces *FN* with a small *FP* overhead for cases of $\mu_{ch}^{thr} > \mu_{ch}^{alg}$. Therefore, the *accuracy* of the Case 2 outperforms the other Cases in this condition. For example, as shown at $\mu_{ch}^{alg} = 1\%$ in Fig. 8 (d), the Case 2 achieves 98.77% of *accuracy*, whereas those of Case 1 and Case 3 are limited to 90.79% and 87.40%, respectively. However, if K is small, α is small, and both μ_{ch}^{thr} and μ_{ch}^{alg} are large, the Case 2 shows 94.51% *accuracy*, which is the worst among the Cases, as shown in Fig. 8 (c). There may be two reasons for this observation. First, the Case 2 causes many *FPs* to minimize *FN* when α is small. Second, dividing K into groups significantly degrades accuracy, especially when K is small. Accordingly, as shown in Fig. 11 (c), the Case 2 effectively achieves 99.92% *accuracy* at $\mu_{ch}^{alg} = 10\%$ when K is 300. The extensive simulation study reveals that the Case 2 can be a solution for highly secure networking when K and μ_{ch}^{thr} are large.

A comparison between (a) and (b) in Figs. 8 and 11 shows that a large α effectively enhances the *accuracy* performance of all Cases when $\mu_{ch}^{thr} < \mu_{ch}^{alg}$, because the *accuracy* highly depends on *FP* in this area. Conversely, a large α degrades the *accuracies* of the Case 1 and Case 3 when $\mu_{ch}^{thr} = 10\%$. This is because a large α attempts to reduce *FP* by sacrificing *FN*, where the *accuracy* is highly affected by *FN*, when μ_{ch}^{thr} is large. Value of b significantly affects *accuracy* performance of Case 2 and Case 3. For example, when $K = 300$, $\mu_{ch}^{thr} = 10\%$, $\mu_{ch}^{thr} = 1\%$, and $\alpha = 0.1$, Case 2 with $b = 60$ suffers from 73.34% of *accuracy*, whereas $b = 6$ in Fig. 11 (c) achieves 99.92% of *accuracy*. As shown in Appendix C, the extensive simulation study reveals that the optimal b is calculated as much smaller then K/b, regardless of specific conditions. Therefore, as described at Section IV, limitation of range of b due to the hardware technology of QKD rarely affects the performance of the proposed protocol and algorithms.

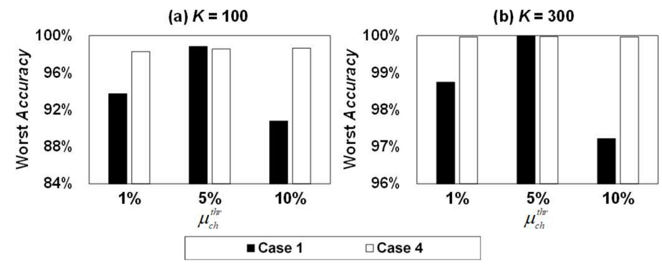

Fig. 12. Worst *accuracy* comparisons between Cases 1 and 4, when $\alpha = 1$.

From the simulation results, one can dynamically combine Case 2 and Case 3 with respect toμ_{ch}^{thr}. We empirically propose Case 4. The Case 4 works as Case 2, if $\mu_{ch}^{thr} \geq 5\%$, otherwise, Case 3. Figure 12 compares the worst *accuracy* of Cases 1 and 4 for $\mu_{ch}^{thr} = 1\%$, 5%, and 10%. The value of α is limited to as 1. The worst *accuracy* is calculated by the minimum *accuracy* among simulation results for all μ_{ch}^{alg}. As shown in Fig. 12, the Case 4 can guarantee at least 98.29% and 99.97% of *accuracies* for $K = 100$ and 300, respectively.

D. Impact of K

Based on the comparison between Figs. 6–8 and 9–11, it is clear that an increase in K improves the security performance of all Cases, which can be explained by the central limit theorem. When K is large, the performance gain from the combinatory criteria is much higher than the performance loss from dividing K into groups in the combinatory algorithms. In our extensive simulation study for $K = 300$ and $\mu_{ch}^{thr} = 1\%$, the Case 3 shows at least 99.97% *accuracy* ($\mu_{ch}^{alg} = 10\%$ in Fig. 11 (b)) in eavesdropping detection. As shown at $\mu_{ch}^{alg} = 1\%$ in Fig. 11 (c), the Case 2 guarantees 99.92% *accuracy* in eavesdropping detection, when $K = 300$ and $\mu_{ch}^{thr} = 10\%$.

To provide straightforward comparisons between the Cases, this study evaluates the security performance for $K = 100$ and 300. However, as it is clear that a larger K can introduce a much higher degree of *accuracy* in eavesdropping detection, we expect a significantly high level of security in the ICT with the proposed Cases. For example, in our 10,000 iterations of simulations, the Case 1 shows 100% *accuracy* for all conditions of μ_{ch}^{thr}, μ_{ch}^{alg}, and α, when K reaches 2,000.

VI. Conclusion

Because it is not feasible to deterministically distinguish between quantum error from eavesdropping and intrinsic

TABLE V
BIT FLIP EVENTS OF THE ORIGINAL BINARY INFORMATION

Bases between Alice and Eve	Bit flip by				Probability
	basis of Eve	basis of Bob	channel btw Alice and Eve	channel btw Eve and Bob	
Identical	N	N	Y	N	$p(b_{A=E})\mu_{AE}(1-\mu_{EB})$
Identical	N	N	N	Y	$p(b_{A=E})(1-\mu_{AE})\mu_{EB}$
Non-identical	Y	N	Y	Y	$p(b_{A\neq E})p(q_E^c \mid b_{A\neq E})(1-p(q_B^c \mid b_{A\neq E}))\mu_{AE}\mu_{EB}$
Non-identical	Y	N	N	N	$p(b_{A\neq E})p(q_E^c \mid b_{A\neq E})(1-p(q_B^c \mid b_{A\neq E}))(1-\mu_{AE})(1-\mu_{EB})$
Non-identical	N	Y	Y	Y	$p(b_{A\neq E})(1-p(q_E^c \mid b_{A\neq E}))p(q_B^c \mid b_{A\neq E})\mu_{AE}\mu_{EB}$
Non-identical	N	Y	N	N	$p(b_{A\neq E})(1-p(q_E^c \mid b_{A\neq E}))p(q_B^c \mid b_{A\neq E})(1-\mu_{AE})(1-\mu_{EB})$
Non-identical	Y	Y	Y	N	$p(b_{A\neq E})p(q_E^c \mid b_{A\neq E})p(q_B^c \mid b_{A\neq E})\mu_{AE}(1-\mu_{EB})$
Non-identical	Y	Y	N	Y	$p(b_{A\neq E})p(q_E^c \mid b_{A\neq E})p(q_B^c \mid b_{A\neq E})(1-\mu_{AE})\mu_{EB}$
Non-identical	N	N	Y	N	$p(b_{A\neq E})(1-p(q_E^c \mid b_{A\neq E}))(1-p(q_B^c \mid b_{A\neq E}))\mu_{AE}(1-\mu_{EB})$
Non-identical	N	N	N	Y	$p(b_{A\neq E})(1-p(q_E^c \mid b_{A\neq E}))(1-p(q_B^c \mid b_{A\neq E}))(1-\mu_{AE})\mu_{EB}$

quantum channels, most studies on the security of QKD have concentrated on the secret key rate performance rather than the detection of eavesdropping. Motivated by the central limit theorem, this study investigates the statistical detection of eavesdropping in the BB84 protocols as a function of the number of qubits used. Hoeffding's inequality manifests a tradeoff between the accuracy of eavesdropping detection and the economy of quantum resources by means of *FPR* and *FNR* analyses. The QBER calculated by 300 qubits guarantees *FPR* and *FNR* lower than 0.009% simultaneously. To provide secure communications against the rapidly varying quantum channel conditions, we propose a grouped BB84 protocol, where the period of basis changing, and the granularity of decoding result sharing are a group of qubits. Inspired by the predictability of the distributions of QBER and group-QBER statistics in the grouped BB84 protocol, this study introduces combinatory eavesdropping detection algorithms. From the extensive simulation study, an optimal combinatory algorithm with respect to a channel condition guarantees 99.97% *accuracy* of eavesdropping detection, when the number of qubits used to calculate the QBER is 300 and importance between *FPR* and *FNR* is equal. In this paper, numerical analysis of *FPR* and *FNR* for BB84 is limited to their upper bounds. We leave evaluation of exact *FPR* and *FNR* for the future study, which requires accurate variance information of distributions.

In this study, we have simplified models and assumptions to provide straightforward analysis and intuition. For example, we abstracted the quantum channel errors for diverse reasons into a single variable. In future studies, we will consider eavesdropping detection in QKD protocols for further practical conditions. Moreover, this study does not consider intercept-and-resend-attack to a part of qubits between Alice and Bob. The Intercept-and-resend-attack to a part of qubits can degrade the eavesdropping detection performance of the proposed protocol and algorithm, by lowering QBER with the presence of Eve. On the other hand, Alice and Bob can take advantage of higher secret key rate which is calculated as a function of QBER. We leave investigation of the tradeoff between eavesdropping detection performance and secret key rate for the future study.

APPENDIX A

Table V describes bit flip events of the original binary information. The error events between Alice and Eve and the error events between Eve and Bob are assumed to be independent. We assume that the channel errors and errors from non-identical bases between two entities are independent. An original binary information generated by Alice does not coincide with a decoding result of Bob, if a qubit experiences odd number of bit flip events by basis of Eve, basis of Bob, channel error between Alice and Eve, and channel error between Eve and Bob. For example, the first event in Table V represents when bases between Alice and Eve are identical with a probability $p(b_{A=E})$, a qubit experiences channel error between Alice and Eve with a probability μ_{AE}, and the qubit does not undergo channel error between Eve and Bob with a probability $(1-\mu_{EB})$. Please note that a qubit does not collapse at bases of Eve and Bob, if bases between Alice and Eve are identical, namely, $p(q_E^c|b_{A=E}) = p(q_B^c|b_{A=E}) = 0$. Therefore, the original binary information encoded in the qubit is flipped once with a probability of $p(b_{A=E})\mu_{AE}(1-\mu_{EB})$, as shown at the first event in Table V.

APPENDIX B

By organizing terms, we can rewrite (11) to as

$$\alpha \frac{e^{-2K\left(\theta^*_{QBER}-\mu_{ch}\right)^2}}{e^{-2K\left(\theta^*_{QBER}-\mu_{ch}(1-\mu_{ch})-0.25\right)^2}}$$

TABLE VI
EMPIRICAL SOLUTIONS OF θ^*_{QBER} AND (θ^h_{G-QBER}, θ^l_{G-QBER}, γ^h, γ^l, b) WITH RESPECT TO THE DIVERSE K, α, AND μ^{thr}_{ch}

K	α	μ^{thr}_{ch}	θ^*_{QBER}	Empirical solution of (θ^h_{G-QBER}, θ^l_{G-QBER}, γ^h, γ^l, b)	
				QBER and group-QBER comparison algorithm	QBER or group-QBER comparison algorithm
100	0.1	0.01	0.112	(0.52, 0.11, 0.17, 0.38, 4)	(0.72, 0.08, 0.11, 0.27, 4)
		0.05	0.150	(0.7, 0.15, 0.12, 0.34, 4)	(0.71, 0.12, 0.03, 0.37, 4)
		0.1	0.196	(0.71, 0.15, 0.11, 0.28, 4)	(0.71, 0.04, 0.1, 0.29, 4)
	0.5	0.01	0.128	(0.65, 0.05, 0.25, 0.31, 4)	(0.71, 0.11, 0.13, 0.33, 4)
		0.05	0.167	(0.7, 0.14, 0.15, 0.36, 4)	(0.71, 0.14, 0.14, 0.24, 4)
		0.1	0.213	(0.72, 0.1, 0.13, 0.37, 5)	(0.64, 0.05, 0.09, 0.41, 4)
	1	0.01	0.135	(0.54, 0.1, 0.23, 0.27, 4)	(0.72, 0.05, 0.14, 0.3, 4)
		0.05	0.174	(0.71, 0.1, 0.16, 0.34, 5)	(0.69, 0.13, 0.09, 0.29, 4)
		0.1	0.22	(0.72, 0.1, 0.15, 0.34, 4)	(0.64, 0.11, 0.15, 0.25, 4)
200	0.1	0.01	0.123	(0.62, 0.14, 0.18, 0.37, 5)	(0.72, 0.11, 0.18, 0.21, 5)
		0.05	0.162	(0.7, 0.12, 0.19, 0.22, 5)	(0.71, 0.12, 0.03, 0.27, 5)
		0.1	0.208	(0.71, 0.04, 0.13, 0.27, 8)	(0.71, 0.14, 0.05, 0.23, 5)
	0.5	0.01	0.131	(0.67, 0.06, 0.23, 0.31, 5)	(0.7, 0.16, 0.2, 0.22, 5)
		0.05	0.170	(0.7, 0.1, 0.21, 0.34, 5)	(0.68, 0.07, 0.17, 0.19, 5)
		0.1	0.216	(0.7, 0.16, 0.2, 0.28, 5)	(0.7, 0.13, 0.19, 0.28, 5)
	1	0.01	0.135	(0.53, 0.08, 0.23, 0.38, 5)	(0.72, 0.12, 0.2, 0.23, 5)
		0.05	0.174	(0.7, 0.04, 0.21, 0.24, 5)	(0.67, 0.13, 0.11, 0.2, 5)
		0.1	0.22	(0.7, 0.16, 0.2, 0.4, 5)	(0.66, 0.04, 0.16, 0.26, 5)
300	0.1	0.01	0.127	(0.64, 0.1, 0.16, 0.37, 6)	(0.67, 0.06, 0.1, 0.35, 6)
		0.05	0.166	(0.71, 0.05, 0.12, 0.3, 10)	(0.67, 0.06, 0.04, 0.18, 6)
		0.1	0.212	(0.65, 0.05, 0.09, 0.38, 6)	(0.61, 0.12, 0.09, 0.28, 6)
	0.5	0.01	0.133	(0.49, 0.07, 0.27, 0.39, 6)	(0.71, 0.04, 0.09, 0.34, 6)
		0.05	0.171	(0.7, 0.06, 0.12, 0.3, 10)	(0.69, 0.05, 0.22, 0.23, 6)
		0.1	0.218	(0.71, 0.05, 0.1, 0.36, 6)	(0.62, 0.08, 0.07, 0.35, 6)
	1	0.01	0.135	(0.6, 0.07, 0.17, 0.34, 6)	(0.67, 0.05, 0.09, 0.35, 6)
		0.05	0.174	(0.68, 0.05, 0.11, 0.36, 6)	(0.66, 0.08, 0.04, 0.26, 6)
		0.1	0.22	(0.7, 0.05, 0.11, 0.36, 6)	(0.61, 0.15, 0.14, 0.32, 6)

$$= \frac{\left(0.25 + \mu_{ch}(1-\mu_{ch}) - \theta^*_{QBER}\right)}{\left(\theta^*_{QBER} - \mu_{ch}\right)} \tag{B.1}$$

The left term in (B.1) is expressed as

$$\frac{\alpha}{e^{\theta^*_{QBER}K\left(1-4\mu^2_{ch}\right)}e^{-2K\left\{\mu^2_{ch}(1-\mu_{ch})^2-\mu^2_{ch}+0.5\mu_{ch}(1-\mu_{ch})+0.25^2\right\}}} \tag{B.2}$$

Then, we can put θ^*_{QBER} related terms to the right side of (B.1) to as

$$\left(\frac{\alpha}{e^{-2K\left\{\mu^2_{ch}(1-\mu_{ch})^2-\mu^2_{ch}+0.5\mu_{ch}(1-\mu_{ch})+0.25^2\right\}}}\right) = e^{\theta^*_{QBER}K\left(1-4\mu^2_{ch}\right)}\left(\frac{\left(0.25 + \mu_{ch}(1-\mu_{ch}) - \theta^*_{QBER}\right)}{\left(\theta^*_{QBER} - \mu_{ch}\right)}\right) \tag{B.3}$$

One can rewrite (B.3) to as

$$\left(\frac{\alpha}{e^{-2K\{\mu^2_{ch}(1-\mu_{ch})^2-\mu^2_{ch}+0.5\mu_{ch}(1-\mu_{ch})+0.25^2\}}}\right)^{\frac{1}{K(1-4\mu^2_{ch})}} = e^{\theta^*_{QBER}}\underbrace{\underbrace{\left(\frac{(0.25 + \mu_{ch}(1-\mu_{ch}) - \theta^*_{QBER})}{(\theta^*_{QBER} - \mu_{ch})}\right)}_{A>0}{}^{\frac{1}{K(1-4\mu^2_{ch})}}}_{B\approx 1} \tag{B.4}$$

We limit the range of θ_{QBER} to (μ_{ch}, μ_{eve}), where μ_{eve} can be expressed as $0.25 + \mu_{ch} - \mu^2_{ch}$ by (7). Accordingly, both the numerator and denominator in term A in (B.4) are greater than 0. Because the area of interest for μ_{ch} is much smaller than 1, we can approximate the term B in (B.4) to 1. Therefore, the optimal θ_{QBER} for the proposed algorithm can be expressed as

$$\theta^*_{QBER} = \frac{\ln\alpha + 2K\{\mu^2_{ch}(1-\mu_{ch})^2-\mu^2_{ch}+0.5\mu_{ch}(1-\mu_{ch})+0.25^2\}}{K\left(1-4\mu^2_{ch}\right)}. \tag{B.5}$$

APPENDIX C

Table VI summarizes the empirical solutions for thresholds and group sizes for the proposed protocol and algorithms. To find solutions, we iteratively run simulations 10,000 times for each candidate in the entire search space and find the best solution for each condition.

References

[1] "Cisco annual Internet report (2018–2023)," CISCO, San Jose, CA, USA, Rep. C11-741490-01, 2020. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11–741490.html

[2] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 131–143, Jan. 2013.

[3] K. Hole, V. Moen, and T. Tjostheim, "Case study: Online banking security," *IEEE Security Privacy*, vol. 4, no. 2, pp. 14–20, Mar.-Apr. 2006.

[4] C. Lee, M. Jang, M. Noh, and W. Seok, "Scalable design and algorithm for science DMZ by considering the nature of research traffic," *Springer J. Supercomput.*, vol. 77, pp. 2979–2997, Jul. 2020.

[5] K. Inoue, "Quantum key distribution technologies," *IEEE J. Sel. Topics Quantum Electron.*, vol. 12, no. 4, pp. 888–896, Jul./Aug. 2006.

[6] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, Oct. 1997.

[7] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. Int. Conf. Comput. Syst. Signal Process.*, Bangalore, India, 1984, pp. 175–179.

[8] S. Pirandola *et al.*, "Advances in quantum cryptography," *Adv. Opt. Photon.*, vol. 12, no. 4, pp. 1012–1236, 2020.

[9] B. Kraus, N. Gisin, and R. Renner, "Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication," *Phys. Rev. Lett.*, vol. 95, Aug. 2005, Art. no. 080501.

[10] P. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, no. 2, pp. 441–444, Jul. 2000.

[11] W. Wootters and W. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, pp. 802–803, Oct. 1982.

[12] M. Elboukhari, M. Azizi, and A. Azizi, "Quantum key distribution protocol: A survey," *Int. J. Univ. Comput. Sci.*, vol. 1, no. 2, pp. 59–67, 2010.

[13] P. Subramaniam and A. Parakh, "Limits on detecting eavesdropper in QKD protocols," in *Proc. IEEE ANTS*, New Delhi, India, 2014, pp. 1–3.

[14] F. Zamani and P. K. Verma, "A QKD protocol with a two-way quantum channel," in *Proc. IEEE ANTS*, Bangalore, India, 2011, pp. 1–6.

[15] P. Subramaniam and A. Parakh, "A quantum Diffie-Hellman protocol using commuting transformations," in *Proc. IEEE ANTS*, New Delhi, India, 2014, pp. 1–6.

[16] A. Parakh, "A probabilistic quantum key transfer protocol," *Secur. Commun. Netw.*, vol. 6, no. 11, pp. 1389–1395, Nov. 2013.

[17] I. Siniosoglou, P. Radoglou-Grammatikis, G. Efstathopoulos, P. Fouliras, and P. Sarigiannidis, "A unified deep learning anomaly detection and classification approach for smart grid environments," *IEEE Trans. IEEE Trans. Netw. Service Manag.*, vol. 18, no. 2, pp. 1137–1151, Jun. 2021.

[18] M. J. Kang and J.-W. Kang, "A novel intrusion detection method using deep neural network for in-vehicle network security," in *Proc. IEEE VTC Spring*, Nanjing, China, 2016, pp. 1–5.

[19] D. Narsingyani and O. Kale, "Optimizing false positive in anomaly based intrusion detection using genetic algorithm," in *Proc. IEEE MITE*, Amritsar, India, 2015, pp. 72–77.

[20] H. Chau, "Practical scheme to share a secret key through a quantum channel with a 27.6% bit error rate," *Phys. Rev. A*, vol. 66, pp. 1–4, Dec. 2002.

[21] O. Johnson, *Information Theory and the Central Limit Theorem*. London, U.K.: Imperial College Press, 2004.

[22] S. G. Kwak and J. H. Kim, "Central limit theorem: The cornerstone of modern statistics," *Korean J. Anesthesiol.*, vol. 70, no. 2, pp. 144–156, Apr. 2017.

[23] W. Hoeffding, "Probability inequalities for sums of bounded random variables," *J. Amer. Statist. Assoc.*, vol. 58, no. 301, pp. 13–30, 1963.

[24] C. Gobby, Z. L. Yuan, and A. J. Shields, "Quantum Key distribution over 122 km of standard telecom fiber," *Appl. Phys. Lett.*, vol. 84, no. 19, pp. 3762–3764, 2004.

[25] B. Korzh *et al.*, "Provably secure and practical quantum key distribution over 307 km of optical fibre," *Nat. Photon.*, vol. 9, pp. 163–168, Feb. 2015.

[26] X. Tan *et al.*, "Tunable and switchable dual-waveband ultrafast fiber laser with 100 GHz repetition-rate," *Opt. Exp.*, vol. 25, no. 14, pp. 16291–16299, 2017.

[27] Z. Jiao *et al.*, "A C-band InAs/InP quantum dot semiconductor mode-locked laser emitting 403-GHz repetition rate pulses," *IEEE Photon. Technol. Lett.*, vol. 23, no. 9, pp. 543–545, May 2011.

[28] B. Koch and R. Noé, "PMD-tolerant 20 krad/s endless polarization and phase control for BB84-based QKD with TDM pilot signals," in *Proc. Photon. Netw. 21th ITG-Symp.*, 2020, pp. 37–39.

[29] A. E. Lita, A. J. Miller, and S. W. Nam, "Counting near-infrared single-photons with 95% efficiency," *OSA Opt. Exp.*, vol. 16, no. 5, pp. 3032–3040, 2008.

[30] M. Ghioni, A. Giudice, S. Cova, and F. Zappa, "High-rate quantum key distribution at short wavelength: Performance analysis and evaluation of silicon single photon avalanche diodes," *J. Mod. Opt.*, vol. 50, no. 14, pp. 2251–2269, 2003.

[31] M. Fitch, B. C. Jacobs, T. B. Pittman, and J. D. Franson, "Photon-number resolution using time-multiplexed single-photon detectors," *Phys. Rev. A*, vol. 68, pp. 1–6, Oct. 2003.

[32] H. Takesue *et al.*, "Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors," *Nat. Photon.*, vol. 1, pp. 343–348, Jun. 2007.

Chankyun Lee (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in electrical engineering from the Korea Institute of Science and Technology Information (KAIST), South Korea, in 2009, 2011, and 2016, respectively. He is a Senior Researcher with the Advanced Quantum KREONET Team, KISTI. Prior to joining KISTI, he held a senior research positions with the Next Generation Business Team from 2016 to 2018 and Network Business Team from 2018 to 2019, Samsung Electronics. His current research interests include quantum key distribution, network algorithms, and 5G air algorithms.

Ilkwon Sohn received the B.S. and unified M.S. and Ph.D. degrees in electrical engineering from Korea University, South Korea, in 2011 and 2018, respectively. He is a Senior Researcher with the Advanced Quantum KREONET Team, Korea Institute of Science and Technology Information. His current research interests include quantum error correction, quantum computation, and quantum communication.

Wonhyuk Lee received the B.S., M.S., and Ph.D. degrees from the School of Electrical, Electronic and Computer Engineering, Sungkyunkwan University, South Korea, in 2001, 2003, and 2010, respectively. He is a Principal Researcher with the Korea Institute of Science and Technology Information, Daejeon, South Korea. His research interests include quantum network management, network performance enhancement, and QKD networks.