Analysis on Eavesdropper Detection in BB84 Quantum Key Distribution Protocol against Partial Intercept-and-resend Attack

Chankyun Lee, Eunjoo Lee, and Wonhyuk Lee
Quantum Network Research Center
Korea Institute of Science and Technology Information (KISTI)
Daejeon, South Korea
chankyunlee@kisti.re.kr

***Abstract*—In the quantum key distribution (QKD) protocol, principles in quantum mechanics enable the detection of an eavesdropper statistically. By leveraging such principles, this research investigates the detectability of an eavesdropper in the Brassard–Bennett-1984 (BB84) QKD protocol over noisy quantum channel, against the partial intercept-and-resend attack. Based on the statistical property of quantum bit error rate (QBER), a simple eavesdropper detection algorithm with optimal threshold for the BB84 protocol is developed. By considering diverse factors such as the quantum channel condition, eavesdropping probability of an eavesdropper, and quantum resource expenditure, the optimal threshold renders flexibility to the algorithm. Through rigorous numerical analysis, the trade-off relation between the accuracy of eavesdropper detection and the secret key rate performance is investigated with respect to the eavesdropping probability in the partial intercept-and-resend attack of an eavesdropper.**

Keywords—Quantum key distribution protocol, Network security, Quantum communication systems, Intrusion detection

I. Introduction

The forthcoming quantum computer era threatens the continued existence of the number theory-based state-of-the-art cryptography system [1]. By utilizing the principles of quantum mechanics, quantum key distribution (QKD) technology can provide unconditionally secure communication, regardless of the computational evolution [2–5]. In QKD, a secret key is shared between two entities (Alice and Bob) over the quantum channel, where an eavesdropper (Eve) may be present. Accordingly, QKD encodes a binary bit information into a physical state of a particle, transmits it over the quantum channel, and decodes it. The state of the particle is defined as a quantum bit (qubit). To realize QKD technology, numerous QKD protocols have been proposed in the community [6–8], among which, the Brassard-Bennett-1984 (BB84) protocol is the first QKD protocol [6]. Because the BB84 is the most widely used protocol in practical systems, this study considers the four-state BB84 protocol as the basic model of the QKD protocol.

Intercept-and-resend attack is a simple, yet powerful eavesdropping strategy that leaks digital information without leaving trace, and thus significantly hampers security of communication. Nonetheless, owing to the principles of quantum mechanics, the intercept-and-resend attack of a qubit in QKD inevitably statistically affects the qubit and increases the quantum bit error rate (QBER) [3–6]. This phenomenon introduces a novel perspective in the security problem in classical communications. However, due to the imperfection of implementation of the QKD system, a qubit may experience QBER, despite the absence of an eavesdropper in the quantum channel. Here, we define the channel error to represent the errors due to the imperfection of implementation of the QKD system, including multiphoton generation in a pulse, attenuation in a fiber, and dark current in a photo detector. Unfortunately, deterministic distinguish between the qubit error caused due to the existence of an eavesdropper and that caused by the channel is impossible. Accordingly, the existing research on the QKD mainly focuses on the secret key rate between the involved entities, regardless of the existence of an eavesdropper [5]. However, in this paper, we suggest further investigation of eavesdropper detectability that is a non-trivial and unique property in QKD. The accurate detection of an eavesdropper can introduce a better utilization of costly quantum resource to QKD and thus eventually contribute to key sharing in QKD.

The intercept-and-resend attack is broadly assumed as a strategy of an eavesdropper in the BB84 protocol [6][9-12]. Inoue [3] and Scarani et al. [4] reviewed the partial intercept-and-resend attack as a practical eavesdropping strategy. In the partial intercept-and-resend attack, the eavesdropper launches the attack to a qubit with a probability ρ and does nothing with a probability (1-ρ). The partial intercept-and-resend attack is one of the simplest individual attack of an eavesdropper. However, this paper assumes the partial intercept-and-resend attack as a sole strategy of an eavesdropper, for the straightforward analysis on detectability of an eavesdropper in the QKD protocol. In [3][4], QBER between the involved entities under the partial intercept-and-resend attack with probability ρ in the BB84 protocol was calculated as $\rho/4$. In other words, the error due to eavesdropping was calculated independent of the channel error. However, in this study, we analyze QBER of the partial attack in the BB84 protocol as a function of channel error.

There are studies for eavesdropper detection against intercept-and-resend attack in QKD protocols. Bennett and Brassard assumed the communication to be free from eavesdropping, if the QBER measured is zero [6]. In [9], Elboukhari et al. calculated that an eavesdropper will not be detected with a probability of $(3/4)^K$ in the four-state BB84 QKD

This work was supported by the National Research Council of Science & Technology (NST) grant by the Korea government (MSIT) (CAP22051-000)

978-3-903176-54-6 © 2023 IFIP

protocol, where K is the number of qubits to calculate QBER. Subramaniam and Parakh analyzed that an eavesdropper will not be detected with a probability of $(1/2)^K$ for infinite-state BB84 and quantum Diffie–Hellman protocols [10]. In [11], Zamani and Verma proposed a two-way QKD protocol and calculated the probability that an eavesdropper will not be detected with respect to K and the number of key exchanges. The underlying assumption in the aforementioned studies is an ideal quantum channel, where eavesdropping is the only reason for QBER > 0.

Our previous work [12] was the first study on accuracy of eavesdropper detection in the BB84 QKD protocols by considering practical quantum channel conditions. However, in [12], only full intercept-and-resend attack ($\rho = 1$) was considered, and the accuracy analysis of eavesdropper detection was limited by its upper-bound. Moreover, the key share performance of QKD, such as the secret key rate, was not investigated in [12]. As a follow-up study of [12], the primary objective of this work is to investigate the eavesdropper detectability in the BB84 QKD protocol against more general attack over noisy channel. The main contributions of this study are as follows:

- By considering quantum channel condition, probability of eavesdropping in the partial intercept-and-resend attack, and quantum resource expenditure, a simple and flexible eavesdropper detection algorithm for BB84 protocol is numerically developed.
- Eavesdropper detection accuracy of the proposed algorithm is numerically evaluated against probability of eavesdropping. It is shown that the large number of qubits used for QBER calculation can increase the accuracy performance.
- A strong trade-off relation between the eavesdropper detection accuracy and secret key rate performance of the proposed algorithm with respect to probability of eavesdropping, is revealed.

II. Preliminaries

This section summarizes the notations and reviews the procedure of the classical four-state BB84 QKD protocol.

A. Notations

We adopt the terminologies of true-negative (*TN*), false-positive (*FP*), true-positive (*TP*), and false-negative (*FN*) from [13][14]. The terminologies are summarized in Table I. We evaluate the false negative ratio (*FNR*) and false positive ratio (*FPR*). *FNR* and *FPR* are the ratios of incorrect judgments in and without the existence of an eavesdropper that can be written as *FN*/(*TP*+*FN*) and *FP*/(*TN*+*FP*), respectively. Furthermore, the *accuracy* represents a ratio of correct judgments that is expressed as (*TP*+*TN*)/(*TP*+*FN*+*TN*+*FP*). Table II summarizes the notations and the associated descriptions used in this paper.

TABLE I. Terminologies for Eavesdropper 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*)

TABLE II. Notations and Descriptions

Notation	Description
K	The number of shared qubits to calculate QBER
ρ	A probability of eavesdropping for a qubit in the partial intercept-and-resend attack
$\nu_{ch,K}$	QBER measured by K qubits without existence of Eve
$\nu_{eve,K}$	QBER measured by K qubits with existence of Eve
μ_{ch}	Genuine QBER without existence of Eve
μ_{eve}	Genuine QBER with existence of Eve
θ_{QBER}	QBER threshold for eavesdropper detection algorithm
$b_{A=E}$	Events that bases of Alice and Eve are identical
$b_{A\neq E}$	Events that bases of Alice and Eve are non-identical
c^E	Events that a qubit collapses into error at a basis of Eve
c^B	Events that a qubit collapses into error at a basis of Bob
$(err.\|Att.)$	Events that a qubit collapses into error when Eve launches intercept-and-resend attack to the qubit
$(err.\|$ *no Att.*$)$	Events that a qubit collapses into error when Eve does not launch intercept-and-resend attack to the qubit

B. Procedure of Four-State BB84 Protocol

In the four-state BB84 protocol, Alice generates a random binary bit sequence as a secret key. Alice encodes a binary bit into a polarization state of a particle (a qubit), where the polarization can be generated by selecting a basis among rectangular (+) or diagonal (×). The encoding rule between a binary bit and a polarization state with respect to bases are publicly shared. For example, ↔ and ↕ polarizations can represent 1 and 0, if Alice selects a rectangular basis. Alice sends qubits to Bob over the quantum channel, and Bob decodes the qubits by the encoding rule. Please note that Bob randomly selects a basis to decode a qubit because Alice does not share the information of her encoding basis for the qubit. If the bases of Alice and Bob are non-identical for a qubit, the qubit collapses randomly into a polarization of a basis of Bob. After sending all the qubits, Alice and Bob communicate over the public channel. Bob shares the information of his decoding bases of each qubit and Alice answers which bases are identical to her encoding bases. Among the identical bases, Bob announces decoding results of randomly selected K qubits. Alice can calculate the QBER by comparing the original binary bit information and decoding results of the K qubits of Bob. The qubit is a costly resource in the QKD. Considering practical interest, we limit K to a few hundreds.

In the case of the intercept-and-resend attack, Eve randomly selects a decoding basis between rectangular or diagonal to intercept a qubit. If bases between Alice and Eve are identical, the qubit does not collapse at the basis of Eve. However, when bases are non-identical, the qubit collapses randomly to a polarization with respect to the basis of Eve. Eve resends the qubit to Bob. Assuming perfect quantum channel condition [6][9–11], the average QBER measured by Alice and Bob is calculated as 25% because the probability of non-identical bases between Alice and Eve for a qubit is 50%, and 50% of them collapse into errors. Please refer [6] for the further information.

III. Threshold-based Eavesdropper Detection in the BB84 Protocol

This section discusses the modelling of QBER distributions in the BB84 protocol in and without the existence of an eavesdropper, by considering partial intercept-and-resend attack strategy of an eavesdropper. Based on the statistical property of QBERs, a simple eavesdropper detection algorithm is developed.

A. QBER Threshold-based Eavesdropper Detection

We define the Bernoulli random variable of $Q_{ch,i}$ to model an error event of *i*-th qubit without the existence of Eve. $Q_{ch,i}$ is 1, if Alice and Bob disagree on $Q_{ch,i}$, otherwise, 0. We assume independent and identically distributed channel errors for each qubit. Accordingly, the QBER measured by *K* qubits without the existence of Eve is calculated as

$$v_{ch,K} = \frac{1}{K}\sum_{i=1}^{K} Q_{ch,i} \; . \qquad (1)$$

QBER calculated by *K* qubits in the existence of Eve is expressed as (2), where the Bernoulli random variable $Q_{eve,i}$ is 1, if Alice and Bob experience bit-mismatch on $Q_{eve,i}$, otherwise, 0.

$$v_{eve,K} = \frac{1}{K}\sum_{i=1}^{K} Q_{eve,i} \qquad (2)$$

Owing to the central limit theorem [15], if *K* is sufficiently large, for example, larger than 30 [16], then the distribution of the average of *K*-sampled variables follows the normal distribution. Accordingly, we model the normal distributions of QBERs without and in the existence of Eve as $v_{ch,K} \sim N(\mu_{ch}, \sigma_{ch}^2)$ and $v_{eve,K} \sim N(\mu_{eve}, \sigma_{eve}^2)$, respectively. Here, μ_{ch} and μ_{eve} are the genuine means of QBERs that can be calculated by (1) and (2), when *K* is infinite. From the central limit theorem, the variances of each distribution are calculated using (3) and (4) that are functions of genuine means and *K*.

$$\sigma_{ch} = \sqrt{\frac{\mu_{ch}\left(1-\mu_{ch}\right)}{K}} \qquad (3)$$

$$\sigma_{eve} = \sqrt{\frac{\mu_{eve}\left(1-\mu_{eve}\right)}{K}} \qquad (4)$$

Because this study considers partial intercept-and-resend attack, an error event of a qubit in the existence of Eve can be categorized into two cases; Eve launches an attack with probability ρ and Eve does not launch any attack with probability (1-ρ). Please note that a qubit suffers from channel error even though an attack is not launched to the qubit by Eve. Accordingly, μ_{eve} is expressed as (5).

$$\mu_{eve} = \rho \Pr(err. \mid Att.) + (1-\rho)\Pr(err. \mid no\ Att.) \qquad (5)$$

An error probability of a qubit when Eve launches an attack is further divided into two cases, when bases between Alice and Eve are identical and non-identical, as shown in (6).

$$\begin{aligned}\Pr(err. \mid Att.) = {} & \Pr(b_{A=E})\Pr(err. \mid b_{A=E}, Att.) \\ & + \Pr(b_{A\neq E})\Pr(err. \mid b_{A\neq E}, Att.)\end{aligned} \qquad (6)$$

The original binary bit becomes erroneous if a qubit experiences odd numbers of bit-flip. Under the condition of identical bases between Alice and Eve, there are two reasons of bit-flip of a qubit—channel error between Alice and Eve (μ_{AE}) and channel error between Eve and Bob (μ_{EB}). Therefore, when Eve launches an attack and the bases of Alice and Eve are identical, a probability of error is calculated as (7) that represents one bit-flip of a qubit due to the channel error. We assume independent channel error each other.

$$\Pr(err. \mid b_{A=E}, Att.) = \mu_{AE}\left(1-\mu_{EB}\right) + \left(1-\mu_{AE}\right)\mu_{EB} \qquad (7)$$

QBER in the BB84 protocol is calculated only when the bases of Alice and Bob are identical. Therefore, an event $b_{A=E}$ represents the cases when the bases of Alice, Eve, and Bob are all identical. Accordingly, (7) does not consider the error cases corresponding to the basis of Bob.

For a case of non-identical bases between Alice and Eve, an error probability Pr(*err.*|$b_{A\neq E}$,*Att.*) is calculated in (8) by a summation of the probabilities of all possible cases of odd numbers (once and three times) of bit-flips of a qubit. Refer to [12] for the detailed description of each event in (8). In (8), the channel errors and errors due to non-identical bases between any two entities are assumed as independent. We further assume each error event in (8) to be independent of each other.

$$\begin{aligned}&\Pr(err. \mid b_{A\neq E}, Att.) \\ &= \Pr(c^E \mid b_{A\neq E})\{1-\Pr(c^B \mid b_{A\neq E})\}\{\mu_{AE}\mu_{EB} + (1-\mu_{AE})(1-\mu_{EB})\} \\ &+\{1-\Pr(c^E \mid b_{A\neq E})\}\Pr(c^B \mid b_{A\neq E})\{\mu_{AE}\mu_{EB} + (1-\mu_{AE})(1-\mu_{EB})\} \\ &+\Pr(c^E \mid b_{A\neq E})\Pr(c^B \mid b_{A\neq E})\{\mu_{AE}(1-\mu_{EB}) + (1-\mu_{AE})\mu_{EB}\} \\ &+\{1-\Pr(c^E \mid b_{A\neq E})\}\{1-\Pr(c^B \mid b_{A\neq E})\} \\ &\quad \{\mu_{AE}(1-\mu_{EB}) + (1-\mu_{AE})\mu_{EB}\}\end{aligned} \qquad (8)$$

Pr(*err.*|*no Att.*) in (5) can be simply expressed as μ_{AB}.

In the four-state BB84 protocol, a qubit randomly collapses at a basis of Eve when the bases between Alice and Eve are non-identical. Therefore, Pr(c^E|$b_{A\neq E}$) = Pr(c^B|$b_{A\neq E}$) = 0.5. We assume that Alice, Eve, and Bob select their bases randomly, Pr($b_{A=E}$) = Pr($b_{A\neq E}$) = 0.5. We further assume that imperfections of a single photon generator at a sender and a photodetector at a receiver are the major reasons for channel error. Accordingly, we can simplify the channel error between any two entities to the same, $\mu_{AB} = \mu_{AE} = \mu_{EB} = \mu_{ch}$, because all they undergo one single photon generator and one photodetector. Consider altogether, we can simplify (5) as (9), as a function of ρ and μ_{ch}.

$$\mu_{eve} = 0.25\rho + \mu_{ch} - \rho\mu_{ch}^2 \qquad (9)$$

Accordingly, the distance between μ_{eve} and μ_{ch} is expressed as

$$\rho(0.25 - \mu_{ch}^2)\,. \qquad (10)$$

Under an ideal quantum channel condition (μ_{ch} = 0), μ_{eve} calculated using (9) is 0.25ρ that is in line with the calculations in [3][4]. If we further consider full intercept-and-resend attack (ρ = 1), μ_{eve} becomes 25%, as regarded in [6][9–11]. If we consider full intercept-and-resend attack (ρ = 1) in (10), the distance becomes $0.25 - \mu_{ch}^2$, equivalent to that in [12].

We suggest an eavesdropper detection algorithm for BB84 protocol. The algorithm makes judgment of the existence of an eavesdropper, if QBER measured by *K* qubits is larger than a threshold (θ_{QBER}). In this algorithm, *FP* increases if $v_{ch,k}$ is larger than θ_{QBER}. Similarly, *FN* increases when $v_{eve,k}$ is equal to or smaller than θ_{QBER}. With sufficiently large *K* (a few hundreds) the *FPR* is calculated by the integration of the distribution of $v_{ch,k}$ from θ_{QBER} to infinite, as shown by (11).

$$FPR = \int_{\theta_{QBER}}^{\infty} \frac{1}{\sigma_{ch}\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{x-\mu_{ch}}{\sigma_{ch}}\right)^2} dx = 1-\Phi\left(\frac{\theta_{QBER}-\mu_{ch}}{\sigma_{ch}}\right) \quad (11)$$

Here, the Φ function represents the cumulative distribution function of the standard normal distribution and is defined as $\Phi(x) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{-t^2/2} dt$ [17]. Similarly, (12) calculate *FNR*.

$$FNR = \int_{0}^{\theta_{QBER}} \frac{1}{\sigma_{eve}\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{y-\mu_{eve}}{\sigma_{eve}}\right)^2} dy = \Phi\left(\frac{\theta_{QBER}-\mu_{eve}}{\sigma_{eve}}\right) \quad (12)$$

A large θ_{QBER} can reduce *FPR* at a cost of the increase in *FNR*. The proposed algorithm with an appropriate threshold can achieve acceptable *accuracy* performance, if the intersection between distributions of $v_{ch,k}$ and $v_{eve,k}$ is sufficiently small. We highlight following observations:

- Owing to the central limit theorem, a large *K* reduces the variances of distributions of $v_{ch,k}$ and $v_{eve,k}$. Therefore, a large *K* can effectively reduce *FPR* and *FNR* with an appropriate threshold in the proposed algorithm.
- A small ρ in the partial intercept-and-resend attack reduces the distance between μ_{eve} and μ_{ch}, which may degrade *accuracy* performance of the proposed algorithm. However, a small ρ simultaneously reduces the variance of distribution of $v_{eve,k}$, which can improve *FPR* and *FNR* of the proposed algorithm.

B. Optimal Threshold

We calculate the optimal threshold θ^*_{QBER} using (13) that minimizes the summation of *FPR* and *FNR*.

$$\theta^*_{QBER} = \underset{\theta_{QBER}}{\arg\min}\left(FPR + FNR\right) \quad (13)$$

Because both *FPR* and *FNR* shown in (11) and (12) are differentiable, the optimal threshold satisfies

$$\frac{1}{\sigma_{eve}\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{\theta^*_{QBER}-\mu_{eve}}{\sigma_{eve}}\right)^2} = \frac{1}{\sigma_{ch}\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{\theta^*_{QBER}-\mu_{ch}}{\sigma_{ch}}\right)^2}. \quad (14)$$

By taking logarithm and organizing terms, we rewrite (14) as

$$2\ln\frac{\sigma_{ch}}{\sigma_{eve}} = \left(\frac{\theta^*_{QBER}-\mu_{eve}}{\sigma_{eve}}\right)^2 - \left(\frac{\theta^*_{QBER}-\mu_{ch}}{\sigma_{ch}}\right)^2. \quad (15)$$

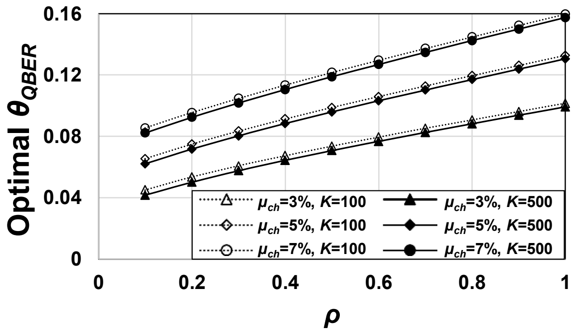

Fig. 1. Optimal θ_{QBER} for the eavesdropper detection algorithm.

From the quadratic formula, we determine a feasible solution of θ^*_{QBER} as (16). The optimal threshold can be written as a function of *K*, μ_{ch}, and ρ, by substituting (3), (4), and (9) into (16).

Figure 1 illustrates θ^*_{QBER} calculated by (16) for various conditions of *K*, μ_{ch}, and ρ. A larger μ_{ch} requires a larger optimal threshold because it changes μ_{eve} to a large value. As shown in Fig. 1, a large *K* results in a small optimal threshold under all conditions. However, the increase in *K* does not significantly affect the optimal threshold because a few hundreds of *K* is sufficiently large. For example, the largest difference between the optimal solutions with respect to *K* is 0.3% for μ_{ch} = 3% and ρ = 10%. Partial intercept-and-resend attack with a small ρ results in a small optimal threshold because a small ρ significantly decreases the distance between μ_{eve} and μ_{ch}. Please note that the optimal threshold in (16) considers both average and variance information of QBER distribution, whereas that in [12] considered average information only.

C. Assumptions and Discussion for the Optimal Threshold

The optimal threshold in (16) requires information on *K*, μ_{ch}, and ρ. Information on *K* is easily obtained because it is selected by Alice and Bob. However, accurate knowledge of μ_{ch} is impossible under the time-varying quantum channel condition. According to [18], we assume that Alice and Bob can approximate μ_{ch} from a quantum interference visibility measure, before actual QKD transmission. Authors in [18] report that the difference between the estimated and measured QBERs lies within 1% for 122 km of standard telecom fiber QKD transmission. Moreover in [19], the fluctuation of QBER in QKD transmission lies within 0.16% during 70-h monitoring. Please refer [12] to handle the cases when Eve manually varies quantum channel conditions to spoil the algorithm. Unfavorably, the parameter ρ is decided by the eavesdropper, which can mislead the optimal threshold. In this study, we assume that Eve maintains ρ as a constant. This assumption is practical if Eve is equipped with a passive optical device for partial intercept-and-resend attack. For example, Eve can use an optical coupler with 50:50 coupling ratio for partial intercept-and-resend attack with probability ρ = 50%, similar to the eavesdropping system shown in [20]. Accordingly, Alice and Bob can analyze the statistics of QBER and estimate ρ using (9).

$$\frac{1}{\sigma_{ch}^2-\sigma_{eve}^2}\left\{\left(\sigma_{ch}^2\mu_{eve}-\sigma_{eve}^2\mu_{ch}\right)-\sigma_{ch}\sigma_{eve}\sqrt{\left(\mu_{eve}-\mu_{ch}\right)^2+2\left(\sigma_{ch}^2-\sigma_{eve}^2\right)\ln\frac{\sigma_{ch}}{\sigma_{eve}}}\right\} \quad (16)$$

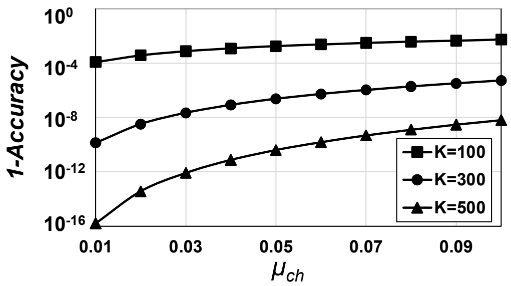

Fig. 2. *accuracy* of eavesdropper detection (ρ = 0.7).

IV. Performance Evaluation

We evaluate the *accuracy* of eavesdropper detection and the trade-off relation between the *accuracy* and secret key rate.

A. Accuracy of Eavesdropper Detection

From (11) and (12), Fig. 2 numerically analyzes 1-*accuracy* performance of eavesdropper detection capability of the proposed algorithm with the optimal thresholds for various conditions of K and μ_{ch}. ρ is fixed as 0.7. Please note that we plot 1-*accuracy* performance in the logarithm scale, for better presentation and clear comparisons. The larger the value of K, the higher the *accuracy* of eavesdropper detection that can be explained by the central limit theorem. Both σ_{ch} and σ_{eve} in (3) and (4) increase with respect to the increase in μ_{ch} that degrade the eavesdropper detectability in the proposed algorithm. Simultaneously, as shown in (10), a larger μ_{ch} results in a shorter distance between μ_{eve} and μ_{ch}. Therefore, a large μ_{ch} degrades the *accuracy* performance over the entire regimes of K. As shown in Fig. 2, more than 100 qubits comparisons for QBER calculation are required to guarantee 99.9% *accuracy*, if ρ and μ_{ch} are estimated as 0.7 and 3%, respectively.

Figure 3 numerically compares 1-*accuracy* performance of eavesdropper detection between the proposed algorithm in this paper and a reference algorithm in [12], with respect to ρ. In the comparison, a range of K is {100, 300, 500} and a value of μ_{ch} is 3%. In [12], the optimal QBER threshold for detection of an eavesdropper is proposed, where the threshold is approximated by Hoeffding's inequality under the full intercept-and-resend attack assumption. For a fair comparison, we assume an equal priority between *FPR* and *FNR* for the reference algorithm in [12]. For the entire regimes of ρ and K, the proposed algorithm achieves dramatic improvement in *accuracy* performances from those of the reference algorithm. The main reason behind this observation is explained as follows; With sufficiently large K, the optimal threshold in (16) is calculated by average and variance information of normal distributions for QBER. However, the optimal threshold in [12] is approximated by upperbounds of *FPR* and *FNR*, which lacks consideration of variance information of QBER distributions. Therefore, in our interested area for K (a few hundreds), the proposed algorithm shows much better *accuracy* performance. For all K condition, the decrease in ρ results in a degradation of the *accuracy* in the proposed algorithm, because a small ρ decreases the distance between μ_{eve} and μ_{ch}. As expected, a larger K effectively achieves higher *accuracy* performance of the algorithms. The same performance trends were observed for different μ_{ch}.

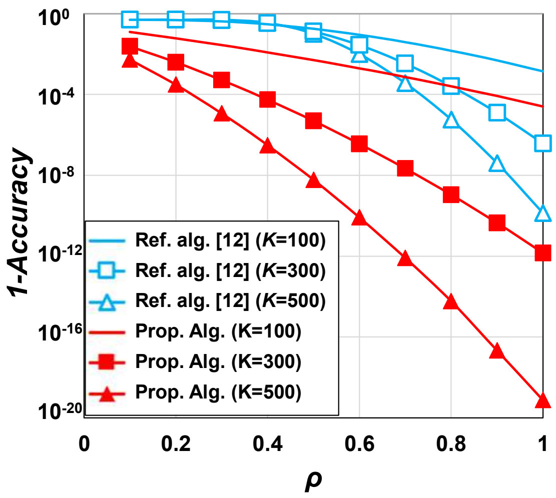

Fig. 3. Numerical comparisons for the eavesdropper detection *accuracy* between algorithms for various ρ. (μ_{ch} = 3% and K = {100, 300, 500})

B. Secret Key Rate

Secret key rate is a representative performance measure in QKD that is rate of unconditionally secure key between the involved entities against an eavesdropper. Even though the security proof in the QKD is beyond of scope of this paper, in order to understand the secret key rate performance of BB84 protocol against the partial intercept-and-resend attack, we review and calculate the secret key rate for our specific model. From [4], the secret key rate under the intercept-and-resend attack in BB84 protocol is expressed as

$$\max[I(A{:}B) - I_E, 0], \tag{17}$$

where $I(A{:}B)$ is the mutual information of raw key between Alice and Bob. I_E denotes Eve's information. Because it is impossible to generate a secret key when Eve has more information than the involved entities, the max function is used in (17) that returns the larger one. By assuming equal probability of bit values, from [4], we rewrite $I(A{:}B)$ as $1 - h(q)$, where h and q are the binary entropy function and QBER, respectively. In the partial intercept-and-resend attack with probability ρ, I_E is calculated as $\rho/2$ [4]. Therefore, the secret key rate is expressed by (18), as a function of QBER and ρ.

$$\max[1 + q\log_2 q + (1 - q)\log_2(1 - q) - \rho/2, 0] \tag{18}$$

Figure 4 compares the secret key rate of the BB84 protocol against partial intercept-and-resend attack. By assuming infinite K, we calculate the secret key rate from (18) using $q = \mu_{ch}$ and μ_{eve} for in and without the existence of an eavesdropper, respectively. In Fig. 4, the solid and dashed lines represent the secret key rates in and without the existence of the eavesdropper, respectively. When the eavesdropper is present, the increase in ρ results in an increase in QBER. Therefore, the solid lines in Fig. 4 monotonically decrease and reach zero, with the increase in ρ. Because μ_{ch} is independent of ρ, the dashed lines in Fig. 4 show constant values with respect to ρ. A large μ_{ch} results in a large μ_{eve}. Therefore, a smaller μ_{ch} shows a higher secret key rate, for both in and without the existence of the eavesdropper. We omit comparison of secret key rate performance as a function of K, because it is negligible in our interested area of K.

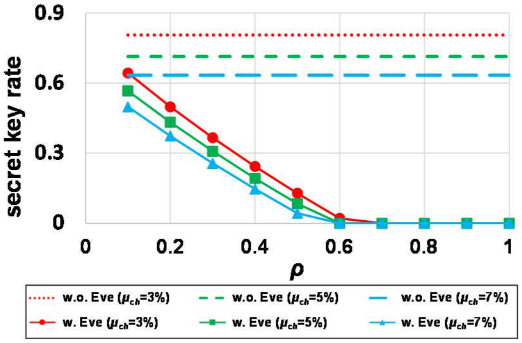

Fig. 4. secret key rate comparison in the BB84 QKD protocol over noisy quantum channel under partial intercept-and-resend attack.

The performance evaluation manifests a strong trade-off relation between the eavesdropper detection *accuracy* and secret key rate, with respect to ρ. If Eve selects a small ρ to reduce the detection probability against the threshold-based eavesdropper detection algorithm, Alice and Bob can take advantage of a higher secret key rate of the BB84 QKD protocol. On the other hand, if Eve launches partial intercept-and-resend attack with a large ρ for more information acquisition, the proposed eavesdropper detection algorithm will enable an extremely high-*accuracy* performance for eavesdropper detection. Because the proposed algorithm operates by considering a combination of the quantum channel condition, eavesdropping probability, and quantum resource expenditure, the algorithm can improve the BB84 protocol by ensuring flexibility in operation and efficiency when utilizing the costly quantum resource.

V. Conclusions

In addition to the classical secret key rate analysis, this study explores the eavesdropping detectability in BB84 QKD protocol by means of representative performance measures in the intrusion detection engineering problem, such as *accuracy*. Based on the central limit theorem, we develop a threshold-based eavesdropper detection algorithm against partial intercept-and-resend attack. The algorithm operates flexibly with respect to the quantum channel condition, the number of used quantum resource for the calculation of QBER, and the eavesdropping probability of an eavesdropper. Numerical analysis reveals a trade-off relation between the economy of quantum resource and eavesdropper detection *accuracy*. This study further investigates the trade-off relation between the eavesdropper detection *accuracy* and secret key rate in the QKD with respect to the eavesdropping probability of an eavesdropper.

Detectability of an eavesdropper in the QKD protocol is initial research stage. For the straightforward analysis on the detectability, this study could not avoid a number of assumptions. A partial intercept-and-resend attack, one of the simplest individual attacks, was fixed to as a specific strategy of an eavesdropper. We further assumed that the statistical property of quantum channel and attack strategy of an eavesdropper are known in prior. As future study, we plan to evaluate the detectability of an eavesdropper in the QKD protocol with realistic assumptions including side channel attack of an eavesdropper.

By incorporating the QKD protocol, we hope that this study can contribute to quantum secure communications and networking. We further believe that the investigations on eavesdropper detection of QKD in this study can contribute to enhance the understanding of QKD, by revealing a fundamental aspect of QKD protocol.

References

[1] P. 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.

[2] 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, July 2000.

[3] K. Inoue, “Quantum key distribution technologies,” IEEE J. Sel. Top. in Quantum Electron., vol. 12, no. 4, pp. 888-896, Aug. 2006.

[4] V. Scarani, H. Pasquinucci, N. Cerf, M. Dušek, N. Lűtkenhaus, and M. Peev, “The security of practical quantum key distribution,” Rev. Mod. Phys., vol. 81, pp. 1301-1350, July-Sept. 2009.

[5] S. Pirandola et al., “Advances in quantum cryptography,” Adv. Opt. Photon., vol. 12, iss. 4, pp. 1012-1236, 2020.

[6] C. H. Bennett and G. Brassard, “Quantum cryptography: public key distribution and coin tossing,” in Proc. IEEE Int. Conf. Comput. Syst. Signal Process, 1984.

[7] A. Ekert, “Quantum cryptography based on bell’s theorem,” Phys. Rev. Lett., vol. 67, pp. 661-663, Aug. 1991.

[8] C. Bennett, “Quantum cryptography using any two nonorthogonal states,” Phys. Rev. Lett., vol. 68. no. 21, pp. 3121-3124, May 1992.

[9] M. Elboukhari, M. Azizi, and A. Azizi, “Quantum key distribution protocol: A survey,” Int. J. Univ. Comput. Sci., vol. 1, iss. 2, pp. 59-67, Mar. 2010.

[10] P. Subramaniam and A. Parakh, “Limits on detecting eavesdropper in QKD protocols,” in Proc. IEEE Int. Conf. Adv. Netw. Telecomm. Syst. (ANTS), 2014.

[11] F. Zamani and P. K. Verma, “A QKD protocol with a two-way quantum channel,” in Proc. IEEE Int. Conf. Adv. Netw. Telecomm. Syst. (ANTS), 2011.

[12] C. Lee, I. Son, and W. Lee, “Eavesdropping detection in BB84 quantum key distribution protocols,” IEEE Trans. Netw. Service Manage., vol. 19, no. 3, pp. 2689-2701, Sept. 2022.

[13] I. Siniosoglou, P. R-Grammatikis, G. Efstathopoulos, P. Fouliras, and P. Sarigiannidis, “A unified deep learning anomaly detection and classification approach for smart grid environments,” IEEE Trans. Netw. Service Manage., vol. 18, no. 2, pp. 1137-1151, May 2021.

[14] M. Kang and J. Kang, “A novel intrusion detection method using deep neural network for in-vehicle network security,” in Proc. IEEE Veh. Technol. Conf. (VTC Spring), 2016.

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

[16] S. Kwak and J. Kim, “Central limit theorem: the cornerstone of modern statistics,” Korean J. Anesthesiol., vol. 70, no. 2, pp. 144-156, April 2017.

[17] G. Marsaglia, “Evaluating the Normal distribution,” J. Stat. Soft., vol. 11, iss. 4, pp. 1-11, July 2004.

[18] C. Gobby, Z. Yuan, and A. Shields, “Quantum Key distribution over 122 km of standard telecom fiber,” Appl. Phys. Lett., vol. 84, no. 19, pp. 3762-3764, May 2004.

[19] B. Korzh, C. Lim, R. Houlmann, N. Gisin, M. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, “Provably secure and practical quantum key distribution over 307 km of optical fibre,” Nat. Photon., vol. 9, pp. 163-168, Feb. 2015.

[20] S. Sun, M. Jiang, X. Ma, C. Li, and L. Liang, “Hacking on decoy-state quantum key distribution system with partial phase randomization,” Sci. Rep., vol. 4, April 2014.