scientific reports

Check for updates

OPEN

Analysis of quantum key distribution based on unified model of sequential state discrimination strategy

Min Namkung[1,2] & Younghun Kwon[2]✉

The quantum key distribution for multiparty is one of the essential subjects of study. Especially, without using entangled states, performing the quantum key distribution for multiparty is a critical area of research. For this purpose, sequential state discrimination, which provides multiparty quantum communication and quantum key distribution for multiple receivers, has recently been introduced. Moreover, the sequential state discrimination is applicable for the security analysis against an eavesdropper's attack. In this work, we provide the security analysis of quantum key distribution by proposing a unified model of sequential state discrimination including an eavesdropper. In this model, the success probability of eavesdropping is used as a figure of merit for the security analysis. Moreover, we obtain a non-zero secret key rate between the sender and receiver, which implies that the sender and receiver can share a secret key despite the eavesdropper's scheme that optimizing the success probability of eavesdropping. Further, we propose an experimental methodology for the proposed model, which is implementable with linear optics. We observe that the secret key between the sender and receiver can be non-zero, even with imperfections.

Quantum physics restricts perfect detection of a physical system's state, which contradicts the argument of classical physics[1–4]. This fact takes a major role of quantum state discrimination in quantum information processing. According to the optimal strategy of the quantum state discrimination required in terms of the figure of merit, there exist well-known strategies such as minimum error discrimination[5–14], unambiguous discrimination[15–23], maximal confidence[24], and a fixed rate of inconclusive results[25–33], which can be applied to two-party quantum communication.

There can be many receivers in quantum communication, and the strategy of the quantum state discrimination between two parties needs to be extended to multiple parties. In 2013, Bergou et al.[34] proposed sequential state discrimination in which many parties can participate as receivers. The sequential state discrimination is process in which the post-measurement state of a receiver is passed to the next receiver. The fact that the probability for every receiver to succeed in discriminating the given quantum states is nonzero implies that all these receivers can obtain the information of the quantum state of the sender, from the post-measurement state of the preceding receiver[35–40]. It was shown that sequential state discrimination can provide multiparty B92 protocol[41], which was implemented using quantum optical experiment[42,43]. this gives us that the sequential state discrimination can be exploited to construct a general quantum key distribution scenario and to analyze the security thereof.

When sequential state discrimination is performed, one can assume that an eavesdropper may exist. Suppose that Alice and Bob performs quantum communication and Eve tries to eavesdrop messages between them. The eavesdropper can have two ways for eavesdropping. The first situation is the case where Eve tries to eavesdrop on Alice's quantum state, which was analyzed in[40]. The second situation is where Eve tries to eavesdrop on the result of Bob. Even though the second situation as well as the first one is a major threat to secure communication, the security analysis to this case has not been done yet. We further note that lots of prepare-and-measure QKD scenarios have been proposed by numerous researchers[44–48], which includes not only high-dimensional DV-QKD protocols[49] but also CV-QKD ones[50,51], and the concern about the threat is reasonable in these scenarios. The prepare-and-measure QKD scenarios are considered to be practical since it does not require an entanglement between a sender and a receiver such as E92 and BBM92 protocols[52,53].

[1]Center for Quantum Information, Korea Institute of Science and Technology (KIST), Seoul 02792, Republic of Korea. [2]Department of Applied Physics, Hanyang University (ERICA), Ansan 15588, Republic of Korea. ✉email: yyhkwon@hanyang.ac.kr

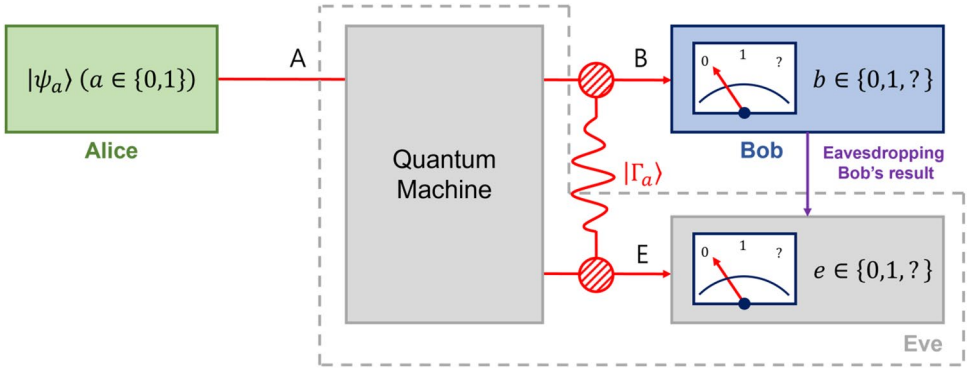

Figure 1. Type-I structure of Eve's scheme for eavesdropping Bob's measurement result. In this scheme, Eve uses a quantum machine that deterministically transforms Alice's state $|\psi_a\rangle$ to a composite system $|\Gamma_a\rangle$ written in Eq. (3) such that $\mathrm{Tr}_E(|\Gamma_a\rangle\langle\Gamma_a|) = \Lambda^{(A\to B)}(|\psi_a\rangle\langle\psi_a|)$. Then, she measures her subsystem to obtain information about Bob's measurement result. If Eve is unnoticed by Alice and Bob, then the quantum channel between Alice and Bob is described as a depolarizing channel $\Lambda^{(A\to B)}$ in Eq. (2)

In this paper, we focus on the second case, in which an intruder tries to eavesdrop on the result of a receiver. We provide a systematic security analysis from a unified model of sequential state discrimination including an eavesdropper. In this proposed model, the success probability of eavesdropping and the secret key rate[54] can be considered as a figure of merit for the security analysis. Specifically, the figure of merit for Eve is the success probability of eavesdropping, but the figure of merit for Alice and Bob is the secret key rate. Our study shows that although Eve performs an optimal measurement for the success probability of eavesdropping, the secret key rate between Alice and Bob is not zero.

In addition, we propose an experimental scheme that implements a new sequential state discrimination method composed of Alice–Eve–Bob. This scheme consists of a linear optical system similar to a Sagnac interferometer[42,55]. The experimental setup can realize optimal success probability of eavesdropping for Eve, as well as non-zero secret key rate between Alice and Bob against the Eve. In other words, the protection of quantum communication between two receiters against an eavesdropper's optimal scheme is possible with experimentally feasible setup. Further, we provide the success probability of eavesdropping and the secret key rate, considering the imperfections that can occur in the source, channel, and detector. White noise and colored noise are considered imperfections of the source[56]. The dark count rate and detection efficiency are considered imperfections of the detector[57]. We further propose that, despite these imperfections, the non-zero secret key rate between Alice and Bob is possible.

Results

Eavesdropper's strategies

For an intruder, there are two ways of eavesdropping. The first is to eavesdrop on the quantum state of sender Alice and the other is to eavesdrop on the result of receiver Bob. When the intruder Eve, eavesdrops on the quantum state of sender Alice, she can do it using unambiguous discrimination, without an error. However, from the argument of sequential state discrimination, this process can be observed by Alice and Bob[40]. Therefore, the sender and receiver can recognize the presence of an eavesdropper.

When Eve wants to eavesdrop on the result of receiver Bob, she should be in a quantum entangled state with Bob. Assuming that the existence of an eavesdropper is unnoticed, the eavesdropping can be described as a noisy quantum channel to of Alice and Bob as Fig. 1a. When Alice prepares $|\psi_a\rangle$ $(a \in \{0,1\})$

$$|\psi_a\rangle = \sqrt{\frac{1+s}{2}}|1\rangle + (-1)^a\sqrt{\frac{1-s}{2}}|2\rangle, \tag{1}$$

with prior probability q_a, the noisy quantum channel between Alice and Bob can be described as follows:

$$\Lambda^{(A\to B)}(|\psi_a\rangle\langle\psi_a|)_A = \eta_{AB}|\psi_a\rangle\langle\psi_a|_B + (1-\eta_{AB})\frac{\mathbb{I}_B}{2}. \tag{2}$$

Here, the lower indices A and B denote the systems of Alice and Bob. $\mathbb{I}_B = |1\rangle\langle 1| + |2\rangle\langle 2|$ is an identity operator defined in the system of Bob, which consists of an orthonormal basis $\{|1\rangle, |2\rangle\}$. In Eq. (2), $\eta_{AB} \in [0,1]$ denotes the channel efficiency between Alice and Bob.

Type-I structure of eavesdropper's scheme

Let us consider the eavesdropper's scheme illustrated as Fig. 1b. If quantum systems of Bob and Eve are considered, Eve uses a quantum machine to deterministically transform the Alice's state $|\psi_a\rangle$ to a composite state between Bob and Eve:

$$|\Gamma_a\rangle_{BE} = \sqrt{\eta_{AB}}|\psi_a\rangle_B \otimes |0\rangle_E + \sqrt{1-\eta_{AB}}|\phi_+\rangle_{BE}, \tag{3}$$

with an entangled state

$$|\phi_+\rangle_{BE} = \frac{1}{\sqrt{2}}(|11\rangle + |22\rangle)_{BE}, \tag{4}$$

where is the entangled state between Bob and Eve. Then, Eve performs a quantum measurement on her system to discriminate Bob's measurement result. If η_{AB} is equal to one, then the composite state in Eq. (3) is a product state. Thus, Eve cannot obtain information by measuring her subsystem. Otherwise, Eve can obtain the information about Bob's measurement result. We note that the partial state of Bob is equal to Eq. (2).

Type-II structure of eavesdropper's scheme

The drawback of the eavesdropping scheme introduced above is that it requires a quantum machine deterministically producing $|\Gamma_a\rangle$. Since designing the quantum machine can be difficult, we further propose an alternative eavesdropping scheme. In this scheme, we can consider a composite state between Bob and Eve as follows:

$$\sigma_{a,BE} = \eta_{AB}|\psi_a\rangle\langle\psi_a|_B \otimes |0\rangle\langle 0|_E + (1-\eta_{AB})|\phi_+\rangle\langle\phi_+|_{BE}, \tag{5}$$

which satisfies $\mathrm{Tr}_E\sigma_{a,BE} = \Lambda^{(A\to B)}(|\psi_a\rangle\langle\psi_a|)$. The procedure for producing the composite state in Eq. (5) is illustrated in Fig. 2. In this figure, Eve lets Alice's state be transmitted to Bob with a probability η_{AB}, or discard Alice's state and share $|\phi_+\rangle$ with Bob with a probability $1-\eta_{AB}$. Let us suppose that $|\phi_+\rangle\langle\phi_+|$ is replaced to $\frac{1}{2}|11\rangle\langle 11| + \frac{1}{2}|22\rangle\langle 22|$ in Eq. (5), which means that Bob and Eve eventually shares a fully separable state. In this case, each Kraus operator of Bob transforms $\frac{1}{2}|11\rangle\langle 11| + \frac{1}{2}|22\rangle\langle 22|$ to another rank-2 state. It leads us to that Eve fails to design a quantum measurement used in type-I and -II eavesdropping schemes. Thus, Eve needs entanglement between herself and Bob in order to obtain meaningful information about his outcome.

These two types can provide same security. That is because the joint measurement probability between Bob and Eve in the type-I structure is equal to that in the type-II structure. Particularly, the type-II structure can be easily reproduced in an experimental setup.

Sequential state discrimination including eavesdropper

For the security analysis, we propose the new sequential state discrimination for describing the two eavesdropper's schemes. We first explain the structure of sequential state discrimination, and propose the optimal success probability of eavesdropping. We further investigate the amount of the secret key rate in frame of the sequential state discrimination scenario.

Structure of sequential state discrimination

Let us first explain how each of the eavesdropping scheme introduced in the previous section is described as a sequential state discrimination problem. It is noted that the unambiguous discrimination can be applied to the B92 protocol[3,58]. For this reason, we consider that Bob has a quantum measurement which can unambiguously discriminates Alice's states $|\psi_0\rangle$ and $|\psi_1\rangle$.

We first consider the type-I structure. We note in advance that our argument in here can also be applied to the type-II structure. Suppose that positive-operator valued measure (POVM) $\{M_0^{(B)}, M_1^{(B)}, M_?^{(B)}\}$ denotes the measurements of Bob. Then, the Kraus operator $K_b^{(B)}$ corresponding to the POVM element $M_b^{(B)}$ $(b \in \{0,1,?\})$ is given by[34,39,40]:

$$\begin{aligned} K_0^{(B)} &= \sqrt{\alpha_0}|\phi_0^{(B)}\rangle\langle\alpha_0|, \;\; K_1^{(B)} = \sqrt{\alpha_1}|\phi_1^{(B)}\rangle\langle\alpha_1|, \\ K_?^{(B)} &= \sqrt{1-\alpha_0}|\phi_0^{(B)}\rangle\langle\alpha_0| + \sqrt{1-\alpha_1}|\phi_1^{(B)}\rangle\langle\alpha_1|. \end{aligned} \tag{6}$$

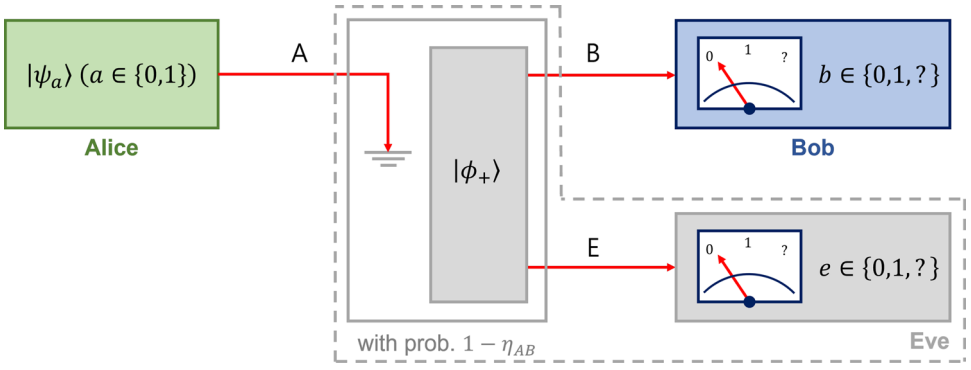

Figure 2. Type-II structure of Eve's scheme. In this scheme, Eve discards Alice's state $|\psi_a\rangle$ and shares a maximally entangled state $|\phi_+\rangle$ with Bob with a probability $1-\eta_{AB}$ as illustrated in the above figure, and lets the Alice's state be transmitted to Bob with a probability η_{AB}.

Here, α_0 and α_1 are non-negative parameters[40], and $|\alpha_0\rangle$ and $|\alpha_1\rangle$ are corresponding vectors:

$$\begin{aligned} |\alpha_0\rangle &= \frac{1}{\sqrt{2(1+s)}}|1\rangle + \frac{1}{\sqrt{2(1-s)}}|2\rangle, \\ |\alpha_1\rangle &= \frac{1}{\sqrt{2(1+s)}}|1\rangle - \frac{1}{\sqrt{2(1-s)}}|2\rangle. \end{aligned} \tag{7}$$

For $a \neq b$, the inner product between $|\alpha_b\rangle$ and $|\psi_a\rangle$ is equal to zero. It guides us to the fact that the measurement described in terms of the Kraus operators in Eq. (6) can perform the unambiguous discrimination. When Bob obtains a conclusive result $b \in \{0, 1\}$, the Kraus operator $K_b^{(B)}$ probabilistically changes the bipartite state of Eq. (3) into the following form:

$$\begin{aligned} K_0^{(B)} \otimes \mathbb{I}_E |\Gamma_0\rangle_{BE} &= |\phi_0^{(B)}\rangle_B \otimes |\gamma_{00}\rangle, \\ K_1^{(B)} \otimes \mathbb{I}_E |\Gamma_0\rangle_{BE} &= |\phi_1^{(B)}\rangle_B \otimes |\gamma_{01}\rangle, \\ K_0^{(B)} \otimes \mathbb{I}_E |\Gamma_1\rangle_{BE} &= |\phi_0^{(B)}\rangle_B \otimes |\gamma_{10}\rangle, \\ K_1^{(B)} \otimes \mathbb{I}_E |\Gamma_1\rangle_{BE} &= |\phi_1^{(B)}\rangle_B \otimes |\gamma_{11}\rangle, \end{aligned} \tag{8}$$

where $|\gamma_{ab}\rangle$ are written as

$$\begin{aligned} |\gamma_{00}\rangle &= \mathcal{N}\left\{\sqrt{\eta_{AB}\alpha_0}|0\rangle_E + \sqrt{\frac{(1-\eta_{AB})\alpha_0}{2(1-s^2)}}|\widetilde{\psi}_0\rangle_E\right\}, \\ |\gamma_{01}\rangle &= |\widetilde{\psi}_1\rangle_E, \\ |\gamma_{10}\rangle &= |\widetilde{\psi}_0\rangle_E, \\ |\gamma_{11}\rangle &= \mathcal{N}\left\{\sqrt{\eta_{AB}\alpha_1}|0\rangle_E + \sqrt{\frac{(1-\eta_{AB})\alpha_1}{2(1-s^2)}}|\widetilde{\psi}_1\rangle_E\right\}. \end{aligned} \tag{9}$$

Here, $\mathcal{N}$ is the normalization constant and

$$|\widetilde{\psi}_b\rangle = \sqrt{1-s^2}|\alpha_b\rangle \tag{10}$$

is a pure state spanned by $\{|1\rangle, |2\rangle\}$. According to Eq. (10), $|\widetilde{\psi}_b\rangle$ is orthogonal to $|0\rangle$. Moreover, the label of $|\widetilde{\psi}_b\rangle$ in Eq. (8) is equal to the measurement result of Bob. Therefore, Eve can eavesdrop the measurement result of Bob by discriminating $|\widetilde{\psi}_0\rangle$ and $|\widetilde{\psi}_1\rangle$ with her measurement described as the POVM $\{M_0^{(E)}, M_1^{(E)}, M_?^{(E)}\}$ on the subspace spanned by $\{|1\rangle, |2\rangle\}$,

$$\begin{aligned} M_0^{(E)} &= u_0 |u_0\rangle\langle u_0|, \\ M_1^{(E)} &= u_1 |u_1\rangle\langle u_1|, \\ M_?^{(E)} &= \mathbb{I}_E - M_0^{(E)} - M_1^{(E)}, \end{aligned} \tag{11}$$

where $M_e^{(E)}$ is the POVM element corresponding to the measurement result e. In Eq. (11), $\mathbb{I}_E$ is the identity operator on Eve's system, u_e is the non-negative real number, and $|u_e\rangle$ is the vector in the subspace $\{|1\rangle, |2\rangle\}$ satisfying $\langle\widetilde{\psi}_b|u_e\rangle = \delta_{be}$. We note that $|u_e\rangle$ can be constructed in the same way as Eq. (7)[40].

In the aspect of the quantum state discrimination task, the finite (but nonzero) success probability implies that a receiver can obtain an information about sender's state[3]. Thus, one of the probable figures of merit is "the success probability of eavesdropping" in case of type-I structure, which is described as (the detailed evaluation is presented in Methods)

$$P_{s,\mathrm{type-I}}^{(E)} = \sum_{a,b\in\{0,1\}} q_a \langle\Gamma_a| K_b^{(B)\dagger} K_b^{(B)} \otimes \mathbb{I}_E |\Gamma_a\rangle \langle\gamma_{ab}| M_b^{(E)} |\gamma_{ab}\rangle. \tag{12}$$

Assume that Bob performs optimal unambiguous discrimination on Alice's state. Then, $P_{s,opt}^{(E)}$, which is the optimum success probability of eavesdropping, can have a simple expression such as $P_{s,opt1}^{(E)}$ or $P_{s,opt2}^{(E)}$,

$$\begin{aligned} P_{s,opt}^{(E)} &= \frac{1-\eta_{AB}}{2(1-s^2)}(\alpha_0 + \alpha_1 - 2\sqrt{\alpha_0\alpha_1}s), \ \text{ if } \ \mathrm{f}_0(\mathrm{s}) > 0 \ \text{ and } \ \mathrm{f}_1(\mathrm{s}) > 0, \\ P_{s,opt}^{(E)} &= \frac{1-\eta_{AB}}{2}\max\{\alpha_0, \alpha_1\}, \ \text{ if } \ \mathrm{f}_0(\mathrm{s}) \leq 0 \ \text{ or } \ \mathrm{f}_1(\mathrm{s}) \leq 0, \end{aligned} \tag{13}$$

with $s := |\langle\psi_1|\psi_2\rangle|$ and

$$\begin{aligned} f_0(s) &:= q_1 s^3 - \sqrt{q_0 q_1}s^2 - q_0 s + \sqrt{q_0 q_1}, \\ f_1(s) &:= q_0 s^3 - \sqrt{q_0 q_1}s^2 - q_1 s + \sqrt{q_0 q_1}. \end{aligned} \tag{14}$$

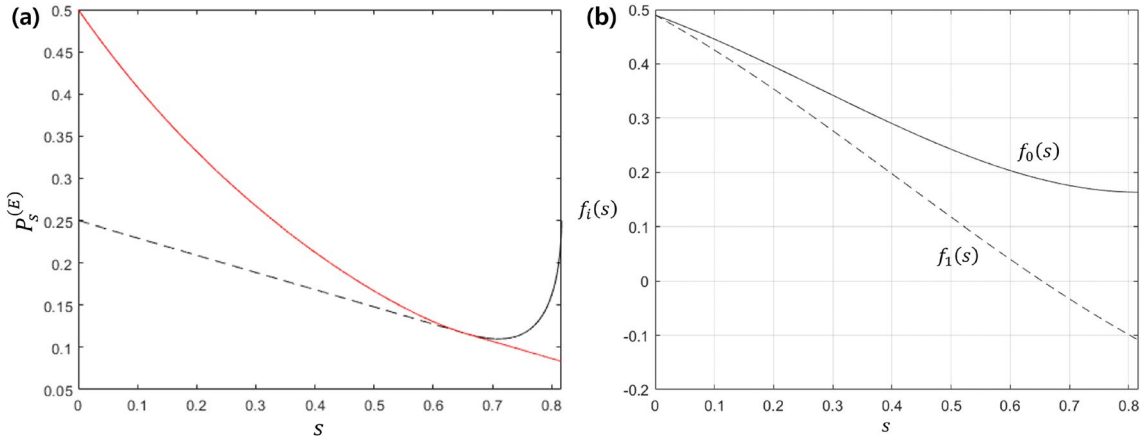

Figure 3. (**a**) Success probability of eavesdropping with respect to overlap $s = |\langle\psi_0|\psi_1\rangle|$ between two Alice's states. Solid black line and dashed black line are success probabilities of eavesdropping $P^{(E)}_{s,opt1}$ and $P^{(E)}_{s,opt2}$ in Eq. (13), respectively, and solid red line is the optimal success probability of eavesdropping. In (**b**), $f_0(s)$ and $f_1(s)$ in Eq. (14) are depicted, where these functions are used for deciding which value between $P^{(E)}_{s,opt1}$ and $P^{(E)}_{s,opt2}$ is indeed optimal, on the basis of the condition written in Eq. (13).

The detailed evaluation of the optimization is presented in Methods. If $s \in [0, \sqrt{q_1/q_2}]$, we get $\alpha_0 = 1 - \sqrt{\frac{q_1}{q_0}}s$ and $\alpha_1 = 1 - \sqrt{\frac{q_0}{q_1}}s$ from Bob's optimal POVM condition[18].

Figure 3a illustrates the optimum success probability of eavesdropping($P^{(E)}_{s,opt}$) in Eq. (13). Here, we have used $q_0 = 0.4(q_1 = 0.6)$ and $\eta_{AB} = 0.5$. In Fig. 3a, the solid black line(dashed black line) indicates $P^{(E)}_{s,opt1}$ ($P^{(E)}_{s,opt2}$). According to Fig. 3a, in the region of $s < 0.6538$, $P^{(E)}_{s,opt1}$ (solid black line) is optimum. That is because, as illustrated in Fig. 3b, both $f_0(s)$ and $f_1(s)$ in Eq. (14) are non-negative in this region. Meanwhile, $P^{(E)}_{s,opt2}$ (dashed black line) is optimum in the region of $s > 0.6538$, since one of $f_1(s)$ is negative. Thus, the optimum success probability of eavesdropping is indicated by the solid red line.

We further evaluate the success probability of eavesdropping in type-II structure as

$$P^{(E)}_{s,\text{type}-\text{II}} = \sum_{a,b\in\{0,1\}} q_a \text{tr}\left[\text{K}_\text{b}^{(\text{B})} \otimes \mathbb{I}_\text{E} \sigma_{\text{a,BE}} \text{K}_\text{b}^{(\text{B})\dagger} \otimes \mathbb{I}_\text{E}\right] \text{tr}\left[\tau_{\text{ab,E}} \text{M}_\text{b}^{(\text{E})}\right], \tag{15}$$

where $\tau_{ab,E}$ are defined as

$$\begin{aligned}
\tau_{00,E} &= \frac{\eta_{AB}}{\eta_{AB} + \frac{1-\eta_{AB}}{2(1-s^2)}} |0\rangle\langle 0|_E + \frac{\frac{1-\eta_{AB}}{2(1-s^2)}}{\eta_{AB} + \frac{1-\eta_{AB}}{2(1-s^2)}} |\widetilde{\psi}_0\rangle\langle\widetilde{\psi}_0|_E, \\
\tau_{01,E} &= |\widetilde{\psi}_1\rangle\langle\widetilde{\psi}_1|_E, \\
\tau_{10,E} &= |\widetilde{\psi}_0\rangle\langle\widetilde{\psi}_0|_E, \\
\tau_{11,E} &= \frac{\eta_{AB}}{\eta_{AB} + \frac{1-\eta_{AB}}{2(1-s^2)}} |0\rangle\langle 0|_E + \frac{\frac{1-\eta_{AB}}{2(1-s^2)}}{\eta_{AB} + \frac{1-\eta_{AB}}{2(1-s^2)}} |\widetilde{\psi}_1\rangle\langle\widetilde{\psi}_1|_E.
\end{aligned} \tag{16}$$

From the straightforward calculation, the success probability of eavesdropping in Eq. (15) is equal to Eq. (12). The proof is presented in Methods. Thus, the optimal success probability of eavesdropping in type-II structure is also analytically derived as Eq. (13).

Secret key rate

In sequential state discrimination scenario among Alice, Bob, and Eve, Alice and Bob can obtain secret key as follows. Let us suppose that Eve performs the eavesdropping scheme discussed in the previous section with optimal success probability of the eavesdropping. Then, due to Eve's measurement which extracts information of Bob's measurement outcome, an event that Alice's prepared bit and Bob's outcome are not equal happens with nonzero probability. By this discrepancy between Alice and Bob, they notice the presence of Eve. This means that Alice and Bob can share the secret key even though Eve performs most efficient eavesdropping scheme. Note that Bob performs optimal unambiguous discrimination on Alice's states, he is not supposed to get error outcomes if Eve does not exist between Alice and Bob.

According to Csiszar and Korner[54], when the amount of information between a receiver and a sender is larger than that between a receiver and eavesdropper, a secret key can exist as an amount equal to the difference of information. The secret key rate is defined as

$$\begin{aligned} K_{AB:E} &= \max\{0, I(B:A) - I(B:E)\} \\ &= \max\{0, H(A) - H(B,A) - H(E) + H(B,E)\}. \end{aligned} \tag{17}$$

Here, $I(X:Y) = H(X) + H(Y) - H(X,Y)$ is Shannon mutual information. $H(X)$ denotes Shannon entropy and $H(X, Y)$ is Shannon joint entropy. If $K_{AB:E} > 0$, sender Alice and receiver Bob can share the secret key[54].

As illustrated in Fig. 4, Bob and Eve can perform the following post-processing. In case that Bob performs optimal unambiguous discrimination, he can discard the measurement result when he obtains an inconclusive result. This post-processing can enhance the amount of information shared between Alice and Bob[59]. In this way, the joint probability between Alice and Bob is

$$\widetilde{P}_{AB}(a,b) = \frac{P_{AB}(a,b)}{\sum_{a,b\in\{0,1\}} P_{AB}(a,b)}, \tag{18}$$

which constitutes the Shannon mutual information in Eq. (17). Here. $a, b \in \{0, 1, ?\}$ are the measurement results for Alice and Bob, respectively. Similarly, when Eve obtains an inconclusive result, she discards the measurement result. Thus, it seems that Eve can successfully obtain information about Bob. However, Bob and Eve are separated in space and the information leakage discussed above is not permitted. In other words, Eve cannot discard her measurement result based on whether Bob obtained an inconclusive result or not. Therefore, the joint probability between Bob and Eve should be changed as follows:

$$\widetilde{P}_{BE}(b,e) = \frac{P_{BE}(b,e)}{\sum_{b\in\{0,1,?\}}\sum_{e\in\{0,1\}} P_{BE}(b,e)}, \tag{19}$$

where $b, e \in \{0, 1, ?\}$ are the measurement results for Bob and Eve, respectively.

Figure 5 shows the secret key rate $K_{AB:E}$ written in Eq. (17), considering the marginal probability between Bob and Eve which is updated from Eq. (19). Here, $P_{AB}(a, b)$ and $P_{BE}(b, e)$ in Eqs. (18) and (19) are evaluated by considering Bob's POVM optimizing optimal unambiguous discrimination and Eve's POVM maximizing success probability of eavesdropping (For the details, see "Secret key rate" in Methods). We note that the both two types of eavesdropper's scheme provides same secret key rate (for detail, see Methods). Here, the channel efficiency is considered as $\eta_{AB} = 0.9$(solid red line), $\eta_{AB} = 0.8$(solid blue line), $\eta_{AB} = 0.7$(solid black line), and $\eta_{AB} = 0.6$(solid purple line). As shown in Fig. 5, as the overlap s increases, $K_{AB:E}$ also increases. However, from a specific overlap $K_{AB:E}$ decreases. For example, for $\eta_{AB} = 0.9$, in the region of $s < 0.4585$, $K_{AB:E}$ increases but in the region of $s > 0.4585$, $K_{AB:E}$ decreases.

The secret key rate $K_{AB:E}$ exhibits interesting behavior. When the overlap s is large, it is difficult for Bob and Eve to efficiently implement the quantum state discrimination. In this case, the mutual information between Alice and Bob, and Bob and Eve becomes small. However, when s is small, Bob and Eve can easily and efficiently implement the quantum state discrimination. In this case, the mutual information between Alice and Bob, and Bob and Eve becomes large.

Method for experimental implementation

Let us propose an experimental method for a unified model of sequential state discrimination including an eavesdropper with quantum optics. Even though the type-I structure was used previously, we will use type-II structure, because it can be easily implemented in an experimental setup. In the type-II structure, Alice prepares a quantum state

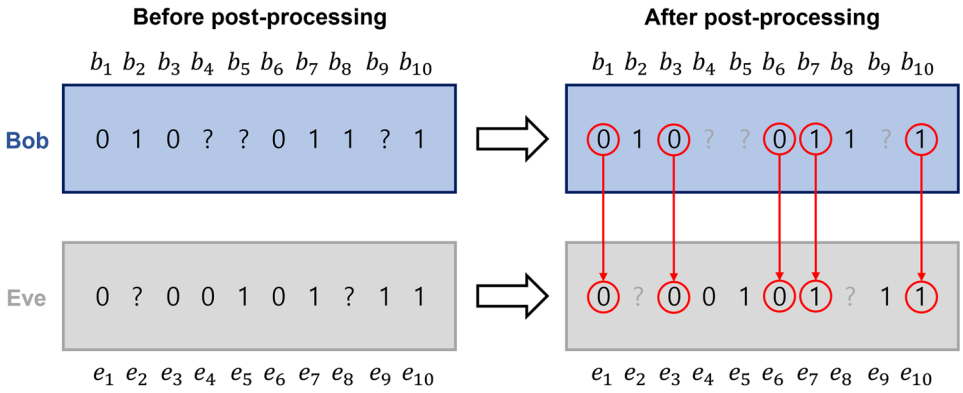

Figure 4. Post-processing performed by Bob and Eve. Let us suppose that Bob has 10 measurement results $b_1, \cdots, b_{10}$, and Eve has measurement results $e_1, \cdots, e_{10}$. Bob can discard the inconclusive results b_4, b_5, b_{10}, and Eve can also discard e_2 and e_8. We note that there may no classical communication between Bob and Eve. In other words, Eve does not have ability to discard her messages by presuming Bob's inconclusive results. This supports the reason that the joint probability needs to be considered as Eq. (19).

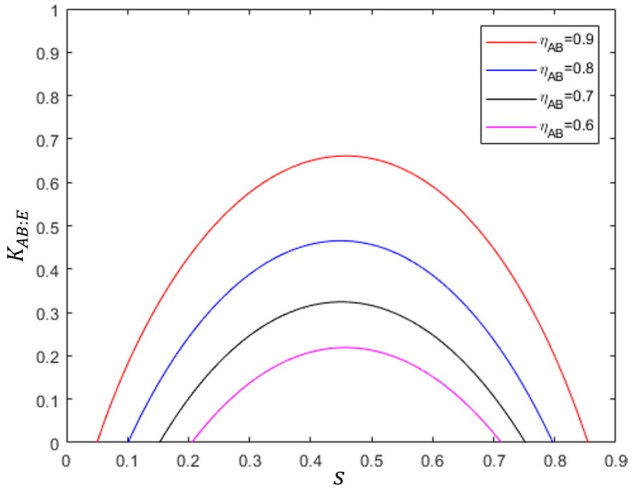

Figure 5. Secret key rate $K_{AB:E}$: red, blue, black, and purple lines correspond to $\eta_{AB} = 0.9$, $\eta_{AB} = 0.8$, $\eta_{AB} = 0.7$, and $\eta_{AB} = 0.6$, respectively. Here, s is the overlap between two Alice's states.

$$|\psi_a\rangle = \sqrt{\frac{1+s}{2}}|h\rangle + (-1)^a\sqrt{\frac{1-s}{2}}|v\rangle, \tag{20}$$

where $|h\rangle$ and $|v\rangle$ represent horizontal and vertical directions, respectively. Eve, who controls channel efficiency η_{AB}, can eavesdrop as follows: (i) With a probability of η_{AB}, Eve does not eavesdrop on the quantum state of Alice. (ii) With a probability of $1-\eta_{AB}$, Eve eliminates the quantum state of Alice and shares a maximally entangled state with Bob. (iii) After Bob's measurement, Eve performs measurement on her subsystem.

In Fig. 6 of the next page, we illustrate the experimental setup(for details about the description, see Supplementary information). Here, the experimental setup of Bob and Eve is based on a Sagnac-like interferometer[55]. The setup consists of a half-wave plate(HWP), polarized beam splitter(PBS), and single-photon detector(SPD). In step (ii), Eve generates a maximally entangled two-photon polarization state $|\phi_+\rangle = \frac{1}{\sqrt{2}}(|hh\rangle + |vv\rangle)$, using a type-II spontaneous parametric down conversion(SPDC)[60]. Type-II SPDC includes beta-barium borate(BBO) crystals, two birefringent crystals, HWP, and quarter-wave plate(QWP). HWP and QWP transform the entangled pure state, generated by the BBO and birefringent crystals, into one of the four Bell-states. Note that the maximally entangled two-photon polarization state is also efficiently generated by the Sagnac interferometer in which a periodically-poled KTP crystal is equipped.

According to the type-II structure, if Eve generates $|\phi_+\rangle$ with a probability of $1-\eta_{AB}$, Eve can eavesdrop on the result of Bob, based on the selection of the path of a single photon and the measurement result of two SPDs. Ideally, Bob performs an unambiguous discrimination based on a Sagnac-like interferometer, and Eve can eavesdrop with the optimum success probability of eavesdropping by constructing a Sagnac-like interferometer. It should be emphasized that despite the attack by Eve, Alice and Bob can obtain the secret key rate.

In reality, one should consider imperfections occurring in the photon state and in SPD. We consider the dark count rate($\nu > 0$) and detection efficiency($0 < \eta < 1$) for the SPD. The photon state in the setup consists of two types: a single-photon polarization state that Alice sends to Bob, and the single photon state of maximally entangled state generated by Eve. Different types of photon states suffer from different types of noises. For example, the single-photon polarization state may disappear under a noisy channel, which is called "amplitude damping"[61,62]. We assume that amplitude damping can occur between Alice and Bob and between Bob and Eve. In addition, white or colored noise can occur when Eve generates a maximally entangled quantum state[56]. Particularly, colored noise which occurs because of imperfections in experimental entangling operations is more frequent than white noise[56]. By including all the imperfections discussed above, Bob and Eve eventually shares the following quantum state:

$$\zeta_a = \eta_{AB}\Lambda_{D_0}^{(ad)}(|\psi_a\rangle\langle\psi_a|)_B \otimes |0\rangle\langle 0|_E + (1-\eta_{AB})\left(\Lambda_{D_e}^{(ad)} \otimes \Lambda_{D_e}^{(ad)}\right)(\varrho_{ent}), \tag{21}$$

for given Alice's bit $a \in \{0,1\}$. Here, η_{AB} is the channel efficiency between Alice and Bob, $\Lambda_{D_0}^{(ad)}$ is an amplitude damping channel between Alice and Bob with damping ratio D_0, and $\Lambda_D^{(ad)}$ is the amplitude damping channel between Eve and Bob with the damping ratio D_e. ϱ_{ent} is a noisy entangled state generated by Eve. If Eve's entangled state is exposed to white noise, then the noisy entangled state is written as[56]

$$\rho_{ent}^{(wh)} = \eta_{\text{ent}}|\phi_+\rangle\langle\phi_+| + (1-\eta_{\text{ent}})\frac{1}{4}(|h\rangle\langle h| + |v\rangle\langle v|) \otimes (|h\rangle\langle h| + |v\rangle\langle v|), \tag{22}$$

and if it is exposed to color noise, then[56]

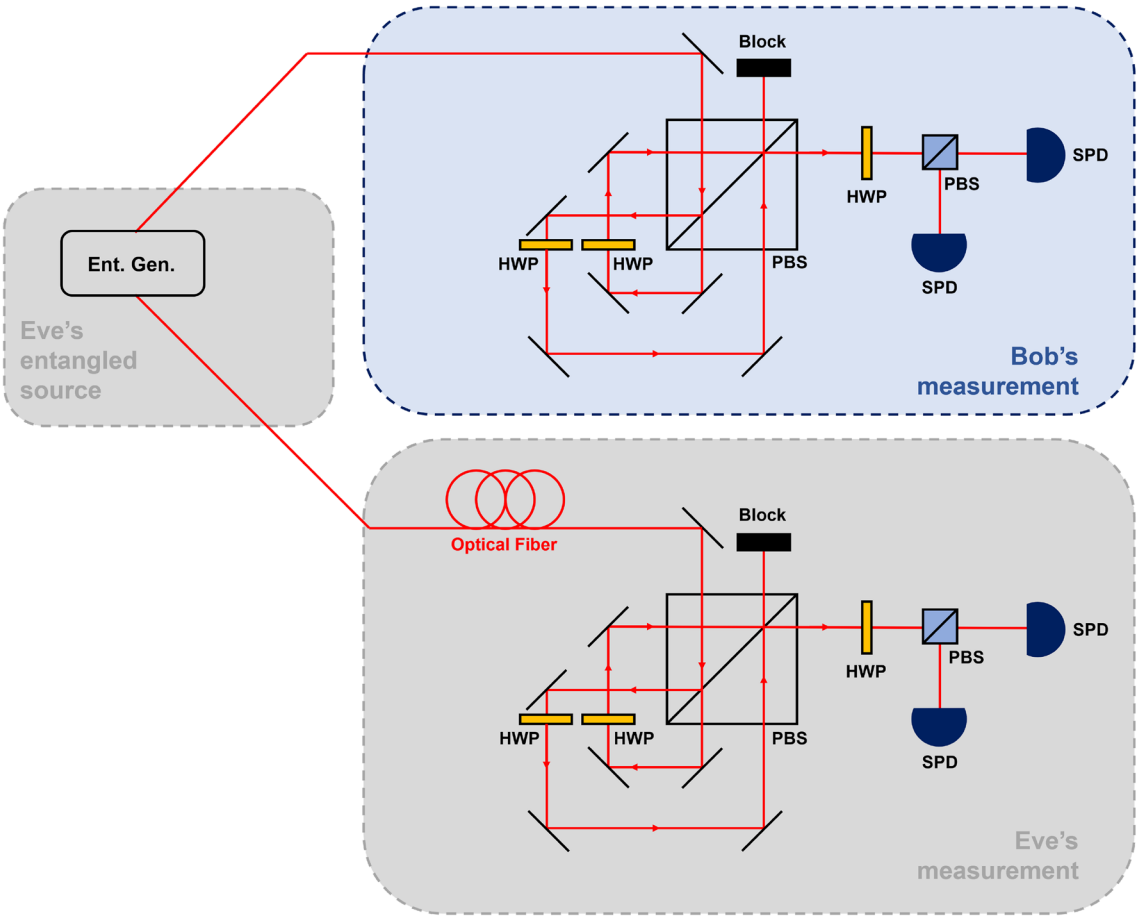

Figure 6. Experimental setting for implementing type-II structure of eavesdropping. Here, with probability $1-\eta_{AB}$, Eve discards Alice's state and prepares maximally entangled state $|\phi_+\rangle = \frac{1}{\sqrt{2}}(|hh\rangle + |vv\rangle)$ between Eve and Bob. HWP: half-wave plate, PBS: polarized beam splitter, SPD: single-photon detector, and Ent. Gen.: entanglement generator[60].

$$\rho_{ent}^{(cl)} = \eta_{ent}|\phi_+\rangle\langle\phi_+| + (1-\eta_{\text{ent}})\frac{1}{2}(|hh\rangle\langle hh| + |vv\rangle\langle vv|), \tag{23}$$

with the efficiency of entanglement η_{ent}, where $|\phi_+\rangle = (|hh\rangle + |vv\rangle)/\sqrt{2}$ is a maximally entangled state composed of horizontal and vertical states $|h\rangle$ and $|v\rangle$.

The success probability of eavesdropping under imperfections described as Eqs. (21)–(23) is displayed in Fig. 7a (for detail, see Supplementary information). In Fig. 7a, the value of $\eta_{AB} = 0.5$, $\eta_{ent} = 0.5$, and $\eta = 0.8$ are considered, where the detection efficiency $\eta = 0.8$ is the value of a commercialized superconducting nanowire single-photon detector(SNSPD) whose dark count rate is nearly zero[63]. In Fig. 7a, the solid line, dashed line, and dash-dot line correspond to the cases of decoherence parameter, $D = 0.1$, $D = 0.2$, and $D = 0.3$, respectively(a large D implies that the decoherence rate is high). Here, we assume that $D_0 = D_e = D$ for considering the relation between the secret key rate and a single decoherence parameter. The black and blue lines show the cases of white and colored noise, respectively.

In Fig. 7b, the secret key rate between Alice and Bob with the imperfections in Eqs. (21)–(23) is displayed, considering various imperfections (for detail, see Supplementary information). Here, $\eta_{AB} = 0.5$, $\eta_{ent} = 0.5$, and $\eta = 0.8$ are considered. The blue(black) line corresponds to colored(white) noise. The solid(dashed) line corresponds to $D_0 = 0.1(D_0 = 0.2)$. In every case, D_e is taken as 0.4. It should be noted that the secret key rate does not change when $D_0 = D_e$ owing to the post-processing expressed in Eq. (19). As shown in Fig. 7b, the graph of the secret key rate has one global maximum. This implies that (i) if s tends to be smaller, then the secret key rate decreases because the tendency of s makes Eve as well as Bob to easily discriminate the quantum states, and (ii) if s tends to be larger, then the secret key rate decreases because the tendency of s makes discrimination performed by Bob and Eve difficult.

Conclusion

In this paper, we have proposed a unified model of sequential state discrimination including an eavesdropper. We have shown that even though Eve uses an entanglement to eavesdrop on Bob's measurement result, Alice and Bob can have a non-zero secret key rate. Furthermore, we have proposed an experimental model for eavesdropping.

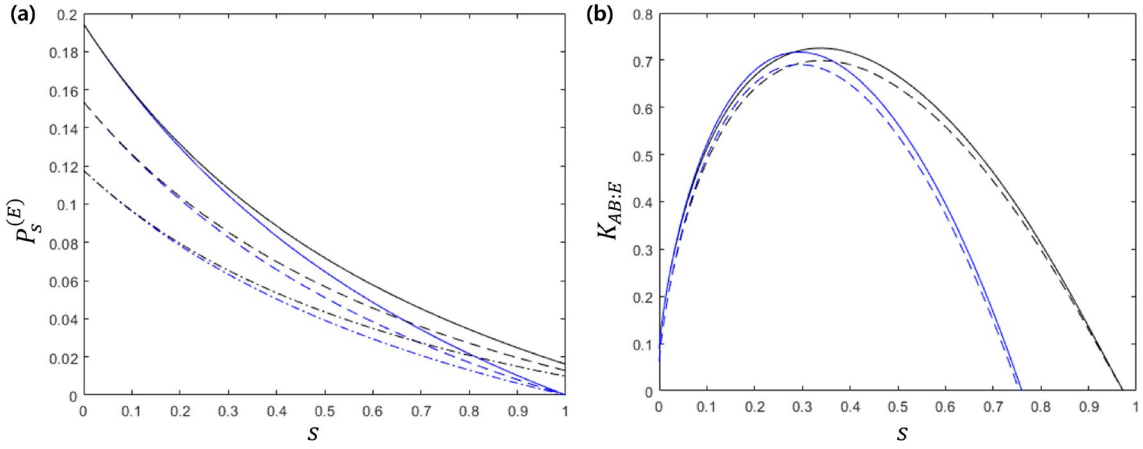

Figure 7. (**a**) Success probability of eavesdropping under imperfect quantum channel, entangled state, and single-photon detector. (**b**) Secret key rate between Alice and Bob. Here, η_{AB}, η_{ent}, and η in Eq. (21) are $\eta_{AB} = 0.5$, $\eta_{ent} = 0.5$, and $\eta = 0.8$, respectively. Blue(black) line corresponds to color(white) noise. Solid, dashed, and dash-dot lines correspond to $D = 0.1$, $D = 0.2$, and $D = 0.3$, respectively. Here, we assume that $D_0 = D_e = D$ for considering the relation between the secret key rate and a single decoherence parameter. Secret key rate under imperfect quantum channel, entangled state, and single-photon detector. Here, $\eta_{AB} = 0.5$, $\eta_{ent} = 0.5$, and $\eta = 0.8$ are considered. Blue(black) line corresponds to color(white) noise. Solid(dashed) line corresponds to $D_0 = 0.1(D_0 = 0.2)$. In every case, $D_e = 0.4$ is considered.

Because our experimental method consists of linear optical technologies, the implementation of our method is practical. Ideally, our experiment can achieve optimum success probability of eavesdropping. Beyond the ideal case, we have investigated possible imperfections including quantum channels between Alice and Bob, entanglement between Bob and Eve, and the inefficiency of Bob's SPD. It is interesting that the non-zero secret key rate is possible even under such the imperfections.

In this paper, we have focused on security analysis of the B92 protocol in view of the sequential state discrimination scheme. That is because the security analysis can be performed with the simple mathematical structure of the unambiguous discrimination[22,40]. We emphasize that our methodology based on the sequential state discrimination can be applied to the various kinds of quantum communication[64] as well as quantum key distribution[45,65] designed in prepare-and-measure way. Moreover, our scheme can be applied to quantum communication or key distribution task utilizing the continuous variable quantum systems[57,66]. We further emphasize that our research propose a novel theoretical way to unify the secure quantum communication tasks in terms of the quantum state discrimination.

It also should be noted that our sequential state discrimination model can be extended to the case of unambiguously discriminating N pure states[1,22]. This extension is important since large N guarantees large amount of transmitted bits per a signal pulse. Moreover, our experimental idea can also be applied to the continuous variable version. That is because sequential measurement that unambiguously discriminates two coherent states can be designed with linear optics[41].

Methods

Success probability of eavesdropping

In this section, we derive and optimize the success probability of eavesdropping by considering both types of eavesdropping strategies.

Describing type-I structure of eavesdropper

In this structure, the following entangled state between Bob and Eve is considered:

$$|\Gamma_a\rangle_{BE} = \sqrt{\eta_{AB}}|\psi_a\rangle_B \otimes |0\rangle_E + \sqrt{\frac{1-\eta_{AB}}{2}}(|11\rangle + |22\rangle)_{BE}. \tag{24}$$

Then, each $K_b^{(B)} \otimes \mathbb{I}_E|\Gamma_a\rangle$ are obtained by

$$
\begin{aligned}
K_0^{(B)} \otimes \mathbb{I}_E|\Gamma_0\rangle =& \sqrt{\eta_{AB}\alpha_0}|\phi_0^{(B)}\rangle_B \otimes |0\rangle_E + \sqrt{\frac{(1-\eta_{AB})\alpha_0}{2}}\left\{(|\phi_0^{(B)}\rangle\langle\alpha_0| \otimes \mathbb{I}_E)|11\rangle + (|\phi_0^{(B)}\rangle\langle\alpha_0| \otimes \mathbb{I}_E)|22\rangle\right\}_{BE},\\
K_1^{(B)} \otimes \mathbb{I}_E|\Gamma_0\rangle =& \sqrt{\frac{(1-\eta_{AB})\alpha_1}{2}}\left\{(|\phi_1^{(B)}\rangle\langle\alpha_1| \otimes \mathbb{I}_E)|11\rangle + (|\phi_1^{(B)}\rangle\langle\alpha_1| \otimes \mathbb{I}_E)|22\rangle\right\}_{BE},\\
K_0^{(B)} \otimes \mathbb{I}_E|\Gamma_1\rangle =& \sqrt{\frac{(1-\eta_{AB})\alpha_0}{2}}\left\{(|\phi_0^{(B)}\rangle\langle\alpha_0| \otimes \mathbb{I}_E)|11\rangle + (|\phi_0^{(B)}\rangle\langle\alpha_0| \otimes \mathbb{I}_E)|22\rangle\right\}_{BE},\\
K_1^{(B)} \otimes \mathbb{I}_E|\Gamma_1\rangle =& \sqrt{\eta_{AB}\alpha_1}|\phi_1^{(B)}\rangle_B \otimes |0\rangle_E + \sqrt{\frac{(1-\eta_{AB})\alpha_1}{2}}\left\{(|\phi_1^{(B)}\rangle\langle\alpha_1| \otimes \mathbb{I}_E)|11\rangle + (|\phi_1^{(B)}\rangle\langle\alpha_1| \otimes \mathbb{I}_E)|22\rangle\right\}_{BE}.
\end{aligned}
\tag{25}
$$

Without loss of generality, we write pure states $|\psi_a\rangle$ as

$$
\begin{aligned}
|\psi_0\rangle_E =& \sqrt{\frac{1+s}{2}}|1\rangle_E + \sqrt{\frac{1-s}{2}}|2\rangle_E,\\
|\psi_1\rangle_E =& \sqrt{\frac{1+s}{2}}|1\rangle_E - \sqrt{\frac{1-s}{2}}|2\rangle_E,
\end{aligned}
\tag{26}
$$

and vectors $|\alpha_b\rangle$ in the Kraus operators as

$$
\begin{aligned}
|\alpha_0\rangle_E =& \frac{1}{\sqrt{2(1+s)}}|1\rangle_E + \frac{1}{\sqrt{2(1-s)}}|2\rangle_E,\\
|\alpha_1\rangle_E =& \frac{1}{\sqrt{2(1+s)}}|1\rangle_E - \frac{1}{\sqrt{2(1-s)}}|2\rangle_E,
\end{aligned}
\tag{27}
$$

such that $\langle\psi_a|\alpha_b\rangle = \delta_{ab}$ for every $a, b \in \{0,1\}$. Substituting Eqs. (26) and (27) into Eq. (25), we obtain

$$
\begin{aligned}
K_0^{(B)} \otimes \mathbb{I}_E|\Gamma_0\rangle =& \sqrt{\eta_{AB}\alpha_0}|\phi_0^{(B)}\rangle_B \otimes |0\rangle_E + \sqrt{\frac{(1-\eta_{AB})\alpha_0}{2}}|\phi_0^{(B)}\rangle_B \otimes |\alpha_0\rangle_E,\\
K_1^{(B)} \otimes \mathbb{I}_E|\Gamma_0\rangle =& \sqrt{\frac{(1-\eta_{AB})\alpha_1}{2}}|\phi_1^{(B)}\rangle_B \otimes |\alpha_1\rangle_E,\\
K_0^{(B)} \otimes \mathbb{I}_E|\Gamma_1\rangle =& \sqrt{\frac{(1-\eta_{AB})\alpha_0}{2}}|\phi_0^{(B)}\rangle_B \otimes |\alpha_0\rangle_E,\\
K_1^{(B)} \otimes \mathbb{I}_E|\Gamma_1\rangle =& \sqrt{\eta_{AB}\alpha_1}|\phi_1^{(B)}\rangle_B \otimes |0\rangle_E + \sqrt{\frac{(1-\eta_{AB})\alpha_1}{2}}|\phi_1^{(B)}\rangle_B \otimes |\alpha_1\rangle_E.
\end{aligned}
\tag{28}
$$

We define (normalized) pure states by

$$
|\widetilde{\psi}_a\rangle_E = \sqrt{1-s^2}|\alpha_a\rangle_E. \tag{29}
$$

Substituting Eq. (29) into Eq. (28), we obtain the representation of Eq. (6) in the letter with $|\gamma_{ab}\rangle$ defined by

$$
\begin{aligned}
|\gamma_{00}\rangle_E =& \frac{1}{\sqrt{\eta_{AB} + \frac{(1-\eta_{AB})}{2(1-s^2)}}}\left\{\sqrt{\eta_{AB}}|0\rangle + \sqrt{\frac{(1-\eta_{AB})}{2(1-s^2)}}|\widetilde{\psi}_0\rangle\right\}_E,\\
|\gamma_{01}\rangle_E =& |\widetilde{\psi}_1\rangle_E,\\
|\gamma_{10}\rangle_E =& |\widetilde{\psi}_0\rangle_E,\\
|\gamma_{11}\rangle_E =& \frac{1}{\sqrt{\eta_{AB} + \frac{(1-\eta_{AB})}{2(1-s^2)}}}\left\{\sqrt{\eta_{AB}}|0\rangle + \sqrt{\frac{(1-\eta_{AB})}{2(1-s^2)}}|\widetilde{\psi}_1\rangle\right\}_E.
\end{aligned}
\tag{30}
$$

Consider Eve's POVM as $\{M_0^{(E)}, M_1^{(E)}, M_?^{(E)}\}$ where each POVM element is given by

$$
M_0^{(E)} = u_0|u_0\rangle\langle u_0|,\ \ M_1^{(E)} = u_1|u_1\rangle\langle u_1|,\ \ M_?^{(E)} = \mathbb{I}_E - M_0^{(E)} - M_1^{(E)}, \tag{31}
$$

where u_0 and u_1 are non-negative real numbers, and $|u_0\rangle$ and $|u_1\rangle$ are vectors orthogonal to $|0\rangle_E$ and satisfying $\langle u_b|\widetilde{\psi}_a\rangle = \delta_{ab}$ for every $a, b \in \{0,1\}$.

From Eqs. (28)–(31), the success probability of eavesdropping is obtained by

$$
P_s^{(E)} = \frac{1-\eta_{AB}}{2(1-s^2)}(\alpha_0 u_0 + \alpha_1 u_1). \tag{32}
$$

Optimization

According to Eq. (29), inner product $\langle\widetilde{\psi}_0|\widetilde{\psi}_1\rangle$ is obtained by

$$\langle\widetilde{\psi}_0|\widetilde{\psi}_1\rangle = -s. \tag{33}$$

Since $|u_0\rangle\perp|0\rangle_E$ and $|u_1\rangle\perp|0\rangle_E$, supports of $M_0^{(E)}$ and $M_1^{(E)}$ are also orthogonal to $|0\rangle_E$. This implies that Eve's POVM is designed to discriminate $|\widetilde{\psi}_0\rangle$ and $|\widetilde{\psi}_1\rangle$. Therefore, the constraint of Eve's POVM is given by[39]

$$(1-u_0)(1-u_1) \geq s^2. \tag{34}$$

Therefore, we obtain the following optimization problem:

$$\begin{aligned} &\text{maximize } P_s^{(E)} = \frac{1-\eta_{AB}}{2(1-s^2)}(\alpha_0 u_0 + \alpha_1 u_1), \\ &\text{subject to } (1-u_0)(1-u_1) \geq s^2. \end{aligned} \tag{35}$$

For fixed parameters α_0 and α_1, an optimal point (u_0, u_1) satisfies

$$(1-u_0)(1-u_1) = s^2. \tag{36}$$

Also, for the optimal point, there exists a non-zero real number λ satisfying

$$\overrightarrow{\nabla} P_s^{(E)} = \lambda \overrightarrow{\nabla}\left\{(1-u_0)(1-u_1) - s^2\right\}, \tag{37}$$

where $\overrightarrow{\nabla}$ is a gradient such that $\overrightarrow{\nabla} f = \left(\frac{\partial f}{\partial u_0}, \frac{\partial f}{\partial u_1}\right)$. We note that Eq. (37) is equivalent to[39]

$$\frac{\partial P_s^{(E)}/\partial u_0}{\partial P_s^{(E)}/\partial u_1} = \frac{\partial\left\{(1-u_0)(1-u_1) - s^2\right\}/\partial u_0}{\partial\left\{(1-u_0)(1-u_1) - s^2\right\}/\partial u_1}. \tag{38}$$

Combining Eqs. (36) and (38), we obtain the optimal point by

$$u_0 = 1 - \sqrt{\frac{\alpha_1}{\alpha_0}}s, \;\; u_1 = 1 - \sqrt{\frac{\alpha_0}{\alpha_1}}s. \tag{39}$$

Since the optimal point (u_0, u_1) is on the surface of Eq. (34), both u_0 and u_1 in Eq. (39) should be non-negative. For this reason, the overlap s also should be

$$s < \sqrt{\frac{\alpha_0}{\alpha_1}} \;\wedge\; s < \sqrt{\frac{\alpha_1}{\alpha_0}}. \tag{40}$$

Considering s in the region of Eq. (40), the optimal success probability of eavesdropping is analytically given by

$$P_{s,opt1}^{(E)} = \frac{1-\eta_{AB}}{2(1-s^2)}(\alpha_0 + \alpha_1 - 2\sqrt{\alpha_0\alpha_1}s). \tag{41}$$

Suppose that Bob performs optimal unambiguous discrimination between two pure states $|\psi_0\rangle$ and $|\psi_1\rangle$. Then, α_0 and α_1 are given by[18]

$$\alpha_0 = 1 - \sqrt{\frac{q_1}{q_0}}s, \;\; \alpha_1 = 1 - \sqrt{\frac{q_0}{q_1}}s, \tag{42}$$

if

$$s < \sqrt{\frac{q_1}{q_0}} \;\wedge\; s < \sqrt{\frac{q_0}{q_1}}. \tag{43}$$

Substituting Eq. (42) with α_0 and α_1 in Eq. (40), we obtain

$$\begin{aligned} f_0(s) &:= q_1 s^3 - \sqrt{q_0 q_1}s^2 - q_0 s + \sqrt{q_0 q_1} > 0, \\ f_1(s) &:= q_0 s^3 - \sqrt{q_0 q_1}s^2 - q_1 s + \sqrt{q_0 q_1} > 0. \end{aligned} \tag{44}$$

We note that if one of inequalities in Eq. (44) does not hold, then the optimal point (u_0, u_1) is given by

$$(u_0, u_1) \in \{(1,0), (0,1)\}. \tag{45}$$

Substituting this optimal point into Eq. (32), we obtain the optimal success probability of eavesdropping:

$$P_{s,opt2}^{(E)} = \frac{1-\eta_{AB}}{2}\max\{\alpha_0, \alpha_1\}. \tag{46}$$

Describing type-II structure of eavesdropper's scheme
In this structure, the following bipartite state between Bob and Eve is considered:

$$\sigma_{a,BE} = \eta_{AB}|\psi_a\rangle\langle\psi_a|_B \otimes |0\rangle\langle 0|_E + (1-\eta_{AB})|\phi_+\rangle\langle\phi_+|_{BE}. \tag{47}$$

Then, each $K_b^{(B)} \otimes \mathbb{I}_E \sigma_{a,AB} K_b^{(B)\dagger} \otimes \mathbb{I}_E$ is obtained by

$$\begin{aligned}
K_0 \otimes \mathbb{I}_E \sigma_{0,BE} K_0^\dagger \otimes \mathbb{I}_E &= \eta_{AB}\alpha_0 |\phi_0^{(B)}\rangle\langle\phi_0^{(B)}| \otimes |0\rangle\langle 0|_E + \frac{(1-\eta_{AB})\alpha_0}{2(1-s^2)} |\phi_0^{(B)}\rangle\langle\phi_0^{(B)}| \otimes |\widetilde{\psi}_0\rangle\langle\widetilde{\psi}_0|_E, \\
K_1 \otimes \mathbb{I}_E \sigma_{0,BE} K_1^\dagger \otimes \mathbb{I}_E &= \frac{(1-\eta_{AB})\alpha_1}{2(1-s^2)} |\phi_1^{(B)}\rangle\langle\phi_1^{(B)}| \otimes |\widetilde{\psi}_1\rangle\langle\widetilde{\psi}_1|_E, \\
K_0 \otimes \mathbb{I}_E \sigma_{1,BE} K_0^\dagger \otimes \mathbb{I}_E &= \frac{(1-\eta_{AB})\alpha_0}{2(1-s^2)} |\phi_0^{(B)}\rangle\langle\phi_0^{(B)}| \otimes |\widetilde{\psi}_0\rangle\langle\widetilde{\psi}_0|_E, \\
K_1 \otimes \mathbb{I}_E \sigma_{1,BE} K_1^\dagger \otimes \mathbb{I}_E &= \eta_{AB}\alpha_1 |\phi_1^{(B)}\rangle\langle\phi_1^{(B)}| \otimes |0\rangle\langle 0|_E + \frac{(1-\eta_{AB})\alpha_1}{2(1-s^2)} |\phi_1^{(B)}\rangle\langle\phi_1^{(B)}| \otimes |\widetilde{\psi}_1\rangle\langle\widetilde{\psi}_1|_E.
\end{aligned} \tag{48}$$

We derive the success probability of eavesdropping as

$$P_s^{(E)} = \sum_{a,b\in\{0,1\}} q_a \mathrm{tr}\left[\mathrm{K_b^{(B)}} \otimes \mathbb{I}_\mathrm{E} \sigma_{\mathrm{a,BE}} \mathrm{K_b^{(B)\dagger}} \otimes \mathbb{I}_\mathrm{E}\right] \mathrm{tr}\left[\tau_{\mathrm{ab,E}} \mathrm{M_b^{(E)}}\right], \tag{49}$$

where $\tau_{ab,E}$ are defined as

$$\begin{aligned}
\tau_{00,E} &= \frac{\eta_{AB}}{\eta_{AB} + \frac{1-\eta_{AB}}{2(1-s^2)}} |0\rangle\langle 0|_E + \frac{\frac{1-\eta_{AB}}{2(1-s^2)}}{\eta_{AB} + \frac{1-\eta_{AB}}{2(1-s^2)}} |\widetilde{\psi}_0\rangle\langle\widetilde{\psi}_0|_E, \\
\tau_{01,E} &= |\widetilde{\psi}_1\rangle\langle\widetilde{\psi}_1|_E, \\
\tau_{10,E} &= |\widetilde{\psi}_0\rangle\langle\widetilde{\psi}_0|_E, \\
\tau_{11,E} &= \frac{\eta_{AB}}{\eta_{AB} + \frac{1-\eta_{AB}}{2(1-s^2)}} |0\rangle\langle 0|_E + \frac{\frac{1-\eta_{AB}}{2(1-s^2)}}{\eta_{AB} + \frac{1-\eta_{AB}}{2(1-s^2)}} |\widetilde{\psi}_1\rangle\langle\widetilde{\psi}_1|_E.
\end{aligned} \tag{50}$$

From Eqs. (48) and (50), the success probability of eavesdropping in Eq. (49) is obtained by Eq. (32).

Secret key rate

In this section, we derive the secret key rate when Eve's POVM optimizes the success probability of eavesdropping.

Secret key rate of type-I eavesdropping structure
To derive the secret key rate, we need to evaluate entropies $H(A)$, $H(B, A)$, $H(E)$ and $H(B, E)$. For equal prior probabilities (*i.e.*, $q_0 = q_1$), $H(A)$ is given by

$$H(A) = -q_0 \log_2 q_0 - q_1 \log_2 q_1 = 1. \tag{51}$$

Also, $H(B, A)$ is given by

$$H(B,A) = -\sum_{a,b\in\{0,1\}} \widetilde{P}_{AB}(a,b) \log_2 \widetilde{P}_{AB}(a,b), \tag{52}$$

where $\widetilde{P}_{AB}(a, b)$ is a post-processed joint probability between Alice and Bob after Bob discards his inconclusive result:

$$\widetilde{P}_{AB}(a,b) = \frac{P_{AB}(a,b)}{\sum_{a,b\in\{0,1\}} P_{AB}(a,b)}, \tag{53}$$

and $P_{AB}(a, b)$ is a pre-processed joint probability

$$P_{AB}(a,b) = q_a \mathrm{tr}\left\{\Lambda^{(\mathrm{A}\to\mathrm{B})}(|\psi_\mathrm{a}\rangle\langle\psi_\mathrm{a}|)\mathrm{K_b^{(B)\dagger}}\mathrm{K_b^{(B)}}\right\} = \frac{1}{2}\left\{\eta_{\mathrm{AB}}\alpha_\mathrm{b}\delta_{\mathrm{ab}} + \frac{(1-\eta_{\mathrm{AB}})\alpha_\mathrm{b}}{2(1-\mathrm{s}^2)}\right\}. \tag{54}$$

Here, we consider the post-processing that Bob discard his inconclusive result, since this post-processing can enhance unambiguous quantum communication protocol[59].

Since $q_0 = q_1$ implies $u_0 = u_1 = 1 - s$ according to Eqs. (39) and (42), the joint probability of Eq. (54) is rewritten by

$$P_{AB}(a,b) = \frac{1}{2}\left\{\eta_{AB}(1-s) + \frac{1-\eta_{AB}}{2(1+s)}\right\}, \quad \text{if} \quad (\mathrm{a},\mathrm{b}) \in \{(0,0),(1,1)\}, \tag{55}$$

$$P_{AB}(a,b) = \frac{1-\eta_{AB}}{4(1+s)}, \text{ if } (a,b) \in \{(0,1),(1,0)\}. \tag{56}$$

To evaluate $H(B,E)$ and $H(E)$, we first consider a joint probability $P_{ABE}(a,b,e)$ among Alice, Bob and Eve:

$$P_{ABE}(a,b,e) = P_{AB}(a,b)P_{E|AB}(e|a,b) = q_a P_{B|A}(b|a)P_{E|AB}(e|a,b), \tag{57}$$

where $P_{B|A}(b|a)$ and $P_{E|AB}(e|a,b)$ are conditional probabilities.

1. In case of $b \neq ?$, every $|\gamma_{ab}\rangle$ in Eq. (30) is rewritten by

$$|\gamma_{ab}\rangle_E = \frac{1}{\sqrt{P_{B|A}(b|a)}}\left\{\sqrt{\eta_{AB}\alpha_b}\delta_{ab}|0\rangle + \sqrt{\frac{(1-\eta_{AB})\alpha_b}{2(1-s^2)}}|\widetilde{\psi}_b\rangle\right\}_E, \tag{58}$$

where

$$P_{B|A}(b|a) = \eta_{AB}\alpha_b\delta_{ab} + \frac{(1-\eta_{AB})\alpha_b}{2(1-s^2)}. \tag{59}$$

Therefore, $P_{E|AB}(e|a,b)$ is given by

$$P_{E|AB}(e|a,b) = \langle\gamma_{ab}|M_e^{(E)}|\gamma_{ab}\rangle = \frac{1}{P_{B|A}(b|a)}\frac{(1-\eta_{AB})\alpha_b}{2(1-s^2)}u_e\delta_{be}. \tag{60}$$

Substituting Eq. (60) into $P_{E|AB}(e|a,b)$ of Eq. (57), we obtain

$$P_{ABE}(a,b,e) = q_a\frac{(1-\eta_{AB})\alpha_b}{2(1-s^2)}u_e\delta_{be}, \tag{61}$$

and

$$P_{BE}(b,e) = \sum_{a=0}^{1}P_{ABE}(a,b,e) = \frac{(1-\eta_{AB})\alpha_b}{2(1-s^2)}u_e\delta_{be}, \tag{62}$$

2. in case of $b = ?$, we provide following equality:

$$\begin{aligned} K_?^{(B)}\otimes\mathbb{I}_E|\Gamma_a\rangle =& \sqrt{\eta_{AB}(1-\alpha_0)}\delta_{a0}|\phi_0^{(B)}\rangle_B\otimes|0\rangle_E + \sqrt{\frac{(1-\eta_{AB})(1-\alpha_0)}{2(1-s^2)}}|\phi_0^{(B)}\rangle_B\otimes|\widetilde{\psi}_0\rangle_E, \\ &+ \sqrt{\eta_{AB}(1-\alpha_1)}\delta_{a1}|\phi_1^{(B)}\rangle_B\otimes|0\rangle_E + \sqrt{\frac{(1-\eta_{AB})(1-\alpha_1)}{2(1-s^2)}}|\phi_1^{(B)}\rangle_B\otimes|\widetilde{\psi}_1\rangle_E. \end{aligned} \tag{63}$$

In the same way as Eq. (30), we obtain

$$|\gamma_{a?}\rangle_E = \frac{1}{P_{B|A}(?|a)}\sum_{x\in\{0,1\}}\left\{\sqrt{\eta_{AB}(1-\alpha_x)}\delta_{ax}|0\rangle + \sqrt{\frac{(1-\eta_{AB})(1-\alpha_x)}{2(1-s^2)}}|\widetilde{\psi}_x\rangle\right\}_E. \tag{64}$$

(Since $P_{B|A}(?|a)$ is too complicated, we do not describe it in detail.) Therefore, $P_{E|AB}(e|a,?)$ is given by

$$P_{E|AB}(e|a,?) = \frac{1}{P_{B|A}(?|a)}\left\{\frac{(1-\eta_{AB})(1-\alpha_0)}{2(1-s^2)}u_e\delta_{e0} + \frac{(1-\eta_{AB})(1-\alpha_1)}{2(1-s^2)}u_e\delta_{e1}\right\}. \tag{65}$$

Substituting Eq. () into $P_{E|AB}(e|a,b)$ of Eq. (57), we obtain

$$P_{ABE}(a,b,e) = q_a\left\{\frac{(1-\eta_{AB})(1-\alpha_0)}{2(1-s^2)}u_e\delta_{0e} + \frac{(1-\eta_{AB})(1-\alpha_1)}{2(1-s^2)}u_e\delta_{1e}\right\}, \tag{66}$$

and

$$P_{BE}(?,e) = \sum_{a\in\{0,1\}}P_{ABE}(a,?,e) = \frac{(1-\eta_{AB})(1-\alpha_0)}{2(1-s^2)}u_e\delta_{0e} + \frac{(1-\eta_{AB})(1-\alpha_1)}{2(1-s^2)}u_e\delta_{1e}, \tag{67}$$

Since $q_0 = q_1$ implies $u_0 = u_1 = 1-s$ according to Eqs. (39) and (42), the joint probability $P_{BE}(b,e)$ of Eqs. (62) and (67) are rewritten by

$$\begin{aligned} P_{BE}(b,e) =& \frac{(1-\eta_{AB})(1-s)}{2(1+s)}, \ \text{ if } \ (\mathrm{b},\mathrm{e}) \in \{(0,0),(1,1)\}, \\ P_{BE}(b,e) =& 0, \ \text{ if } \ (\mathrm{b},\mathrm{e}) \in \{(0,1),(1,0)\}, \\ P_{BE}(b,e) =& \frac{(1-\eta_{AB})s}{2(1+s)}, \ \text{ if } \ (\mathrm{b},\mathrm{e}) \in \{(0,?),(1,?)\}. \end{aligned} \tag{68}$$

If Eve discard her inconclusive result, the post-processed joint probability is given by

$$\widetilde{P}_{BE}(b,e) = \frac{P_{BE}(b,e)}{\sum_{b\in\{0,1,?\}}\sum_{e\in\{0,1\}} P_{BE}(b,e)}, \tag{69}$$

and a marginal probability $\widetilde{P}_E(e)$ is given by

$$\widetilde{P}_E(e) = \sum_{b\in\{0,1,?\}} \widetilde{P}_{BE}(b,e). \tag{70}$$

Finally, $H(E)$ and $H(B,E)$ are evaluated as

$$\begin{aligned} H(E) =& -\sum_{e\in\{0,1\}} \widetilde{P}_E(e)\log_2 \widetilde{P}_E(e), \\ H(B,E) =& -\sum_{b\in\{0,1,?\}}\sum_{e\in\{0,1\}} \widetilde{P}_{BE}(b,e)\log_2 \widetilde{P}_{BE}(b,e). \end{aligned} \tag{71}$$

Secret key rate of type-II eavesdropping structure

We first note that the prior probabilities and the quantum channel $\Lambda^{(A\to B)}$ are invariant under the choice of structure. Therefore, $H(A)$ and $H(B,A)$ are evaluated as Eqs. (51) and (52) in the type-I structure.

1. In case of $b \neq ?$, every $\tau_{ab,E}$ in Eq. (50) is rewritten by

$$\tau_{ab,E} = \frac{1}{P_{B|A}(b|a)}\left\{\eta_{AB}\alpha_b\delta_{ab}|0\rangle\langle 0| + \frac{(1-\eta_{AB})\alpha_b}{2(1-s^2)}|\widetilde{\psi}_b\rangle\langle\widetilde{\psi}_b|\right\}, \tag{72}$$

where $P_{B|A}(b|a)$ is given by Eq. (59). Moreover, $P_{E|AB}(e|a,b)$ is given by

$$P_{E|AB}(e|a,b) = \mathrm{tr}\left\{\tau_{\mathrm{ab,E}}\mathrm{M}_{\mathrm{e}}^{(\mathrm{E})}\right\} = \frac{1}{\mathrm{P_{B|A}(b|a)}}\frac{(1-\eta_{\mathrm{AB}})\alpha_{\mathrm{b}}}{2(1-\mathrm{s}^2)}\mathrm{u_e}\delta_{\mathrm{be}}, \tag{73}$$

which is equal to Eq. (60). Therefore, according to Eq. (57), $P_{ABE}(a,b,e)$ *is equal to the case of type-I structure.*

2. In case of $b = ?$, we consider

$$\begin{aligned} K_?^{(B)}\otimes\mathbb{I}_E\sigma_{a,BE}K_?^{(B)}\otimes\mathbb{I}_E =& \eta_{AB}\Gamma(\sqrt{1-\alpha_0}\delta_{a0}|\phi_0^{(B)}\rangle + \sqrt{1-\alpha_1}\delta_{a1}|\phi_1^{(B)}\rangle)\otimes|0\rangle\langle 0|_E \\ &+(1-\eta_{AB})\Gamma\left(\sqrt{\frac{1-\alpha_0}{2(1-s^2)}}|\phi_0^{(B)}\rangle\otimes|\widetilde{\psi}_0\rangle + \sqrt{\frac{1-\alpha_1}{2(1-s^2)}}|\phi_1^{(B)}\rangle\otimes|\widetilde{\psi}_1\rangle\right), \end{aligned} \tag{74}$$

where we define $\Gamma(|v\rangle) := |v\rangle\langle v|$ for convenience. From the above representation, we define a bipartite mixed state shared by Bob and Eve:

$$\begin{aligned} \tau_{a?,BE} = \frac{1}{P_{B|A}(b|a)}\Big[&\eta_{AB}\Gamma(\sqrt{1-\alpha_0}\delta_{a0}|\phi_0^{(B)}\rangle + \sqrt{1-\alpha_1}\delta_{a1}|\phi_1^{(B)}\rangle)\otimes|0\rangle\langle 0|_E \\ &+(1-\eta_{AB})\Gamma\left(\sqrt{\frac{1-\alpha_0}{2(1-s^2)}}|\phi_0^{(B)}\rangle\otimes|\widetilde{\psi}_0\rangle + \sqrt{\frac{1-\alpha_1}{2(1-s^2)}}|\phi_1^{(B)}\rangle\otimes|\widetilde{\psi}_1\rangle\right)\Big]. \end{aligned} \tag{75}$$

Then, $P_{E|AB}(e|a,?)$ is given by

$$\begin{aligned} P_{E|AB}(e|a,?) =& \mathrm{tr}\left\{\tau_{\mathrm{a?,BE}}\left(\mathbb{I}_{\mathrm{B}}\otimes\mathrm{M}_{\mathrm{e}}^{(\mathrm{E})}\right)\right\} \\ =& \frac{1}{P_{B|A}(?|a)}\left\{\frac{(1-\eta_{AB})(1-\alpha_0)}{2(1-s^2)}u_e\delta_{e0} + \frac{(1-\eta_{AB})(1-\alpha_1)}{2(1-s^2)}u_e\delta_{e1}\right\}. \end{aligned} \tag{76}$$

This is equal to Eq. (65), which implies that $P_{A,B,E}(a,b,?)$ *is also equal to the case of type-I structure.*

From the above calculation, we confirm that $H(B,E)$ and $H(E)$ in this structure is equal to these in the type-I structure, respectively. This leads us to the result that both structures provide same secret key rate.

It is noted that the formalism of the joint probabilities discussed above can also provide the success probability of eavesdropping. This will be further explained in the next section.

Revisiting success probability of eavesdropping in terms of joint probabilities
In the scenario of the new sequential discrimination, Bob's measurement result b depends on the input a prepared by Alice, and Eve's measurement result e depends on a and b. From these facts, the joint probability between three parties $P_{ABE}(a,b,e)$ is easily derived by

$$P_{ABE}(a,b,e) = q_a P_{B|A}(b|a) P_{E|AB}(e|a,b) = q_a P_{BE|A}(b,e|a), \tag{77}$$

where q_a is the prior probability that Alice prepares a, $P_{B|A}(b|a)$ is the conditional probability that Bob obtains b if Alice prepares a, $P_{E|AB(e|a,b}$ is the conditional probability that Eve obtains e if Alice prepares a and Bob obtains b, $P_{BE|A}(b,e|a$ is the conditional joint probability that Bob and Eve obtain b and e if Alice prepares a, and $P_{BE}(b,e)$ is the joint probability that Bob and Eve obtain b and e. Also, the success probability of eavesdropping is derived by

$$P_s^{(E)} = \sum_{a,b} q_a P_{B|A}(b|a) P_{E|AB}(e=b|a,b) = \sum_{a,b} q_a P_{BE|A}(b,e=b|a) = \sum_b P_{BE}(b,e=b). \tag{78}$$

It is noted that the expression of the success probability of eavesdropping in Eq. (78) is used for deriving the success probability of eavesdropping when Alice, Bob, and Eve performs the scenario by using the imperfect linear optical technologies.

Data availability

Te datsets used and analysed during the current study available from the corresponding author on reasonable request.

Received: 2 February 2024; Accepted: 17 April 2024
Published online: 04 May 2024

References

1. Chefles, A. Quantum state discrimination. *Contemp. Phys.* **41**, 401 (2000).
2. Barnett, S. M. & Croke, S. Quantum state discrimination. *Adv. Opt. Photon.* **1**, 238 (2009).
3. Bergou, J. A. Discrimination of quantum states. *J. Mod. Opt.* **57**, 160 (2010).
4. Bae, J. & Kwek, L. C. Quantum state discrimination and its application. *J. Phys. A: Math. Theor.* **48**, 083001 (2015).
5. Helstrom, C. W. *Quantum Detection and Estimation* (Academic Press, New York, 1976).
6. Holevo, A. S. *Probabilistic and Statistical Aspects of Quantum Theory* (Springer, Cham, 1979).
7. Yuen, H. P., Kennedy, R. S. & Lax, M. Optimum testing of multiple hypotheses in quantum detection theory. *IEEE Trans. Inf. Theory* **21**, 125 (1975).
8. Chou, C. L. & Hsu, L. Y. Minimum-error discrimination between symmetric mixed quantum states. *Phys. Rev. A* **68**, 042305 (2003).
9. Herzog, U. Minimum-error discrimination between a pure and a mixed two-qubit state. *J. Opt. B: Quantum Semiclass. Opt.* **6**, S24 (2004).
10. Bae, J. Structure of minimum-error quantum state discrimination. *New J. Phys.* **15**, 073037 (2013).
11. Ha, D. & Kwon, Y. Complete analysis for three-qubit mixed-state discrimination. *Phys. Rev. A* **87**, 062302 (2013).
12. Ha, D. & Kwon, Y. Discriminating N-qudit states using geometric structure. *Phys. Rev. A* **90**, 022330 (2014).
13. Ha, D. & Kwon, Y. Quantum nonlocality without entanglement: explicit dependence on prior probabilities of nonorthogonal mirror-symmetric states. *NPJ Quant. Inf.* **7**, 81 (2021).
14. Ha, D. & Kwon, Y. Complete analysis to minimum-error discrimination of four mixed qubit states with arbitrary prior probabilities. *Quant. Inf. Process.* **22**, 67 (2023).
15. Ivanovic, I. D. How to differentiate between non-orthogonal states. *Phys. Lett. A* **123**, 257 (1984).
16. Dieks, D. Overlap and distinguishability of quantum states. *Phys. Lett. A* **126**, 303 (1988).
17. Peres, A. How to differentiate between non-orthogonal states. *Phys. Lett. A* **128**, 19 (1988).
18. Jaeger, G. & Shimony, A. Optimal distinction between two non-orthogonal quantum states. *Phys. Lett. A* **197**, 83 (1995).
19. Rudolph, T., Spekken, R. W. & Turner, P. S. Unambiguous discrimination of mixed states. *Phys. Lett. A* **68**, 050301(R) (2005).
20. Herzog, U. Optimum unambiguous discrimination of two mixed states and application to a class of similar states. *Phys. Rev. A* **75**, 052309 (2007).
21. Pang, S. & Wu, S. Optimum unambiguous discrimination of linearly independent pure states. *Phys. Rev. A* **80**, 052320 (2005).
22. Bergou, J. A., Futschik, U. & Feldman, E. Optimal Unambiguous Discrimination of Pure Quantum States Phys. *Rev. Lett.* **108**, 250502 (2012).
23. Ha, D. & Kwon, Y. Analysis of optimal unambiguous discrimination of three pure quantum states. *Phys. Rev. A* **91**, 062312 (2015).
24. Croke, S., Andersson, E., Barnett, S. M., Gilson, C. R. & Jeffers, J. Maximum confidence quantum measurements Phys. *Rev. Lett.* **96**, 070401 (2006).
25. Chefles, A. & Barnett, S. M. Strategies for discriminating between non-orthogonal quantum states. *J. Mod. Opt.* **45**, 1295 (1998).
26. Zhang, C. W., Li, C. F. & Guo, G. C. General strategies for discrimination of quantum states. *Phys. Lett. A* **261**, 25 (1999).
27. Fiurasek, J. & Jezek, M. Optimal discrimination of mixed quantum states involving inconclusive results. *Phys. Rev. A* **67**, 012321 (2003).
28. Eldar, Y. C. Mixed-quantum-state detection with inconclusive results. *Phys. Rev. A* **67**, 042309 (2003).
29. Herzog, U. Optimal state discrimination with a fixed rate of inconclusive results: Analytical solutions and relation to state discrimination with a fixed error rate. *Phys. Rev. A* **86**, 032314 (2012).
30. Bagan, E., Munoz-Tapia, R., Olivares-Renteria, G. A. & Bergou, J. A. Optimal discrimination of quantum states with a fixed rate of inconclusive results. *Phys. Rev. A* **86**, 040303(R) (2012).
31. Nakahira, K., Usuda, T. S. & Kato, K. Finding optimal measurements with inconclusive results using the problem of minimum error discrimination. *Phys. Rev. A* **91**, 022331 (2015).
32. Herzog, U. Optimal measurements for the discrimination of quantum states with a fixed rate of inconclusive results. *Phys. Rev. A* **91**, 042338 (2015).
33. Ha, D. & Kwon, Y. An optimal discrimination of two mixed qubit states with a fixed rate of inconclusive results. *Quant. Inf. Process.* **16**, 273 (2017).
34. Bergou, J. A., Feldman, E. & Hillery, M. Extracting information from a qubit by multiple observers: Toward a theory of sequential state discrimination. *Phys. Rev. Lett.* **111**, 100501 (2013).
35. Rapcan, P., Calsamiglia, J., Munoz-Tapia, R., Bagan, E. & Buzek, V. Scavenging quantum information: Multiple observations of quantum systems. *Phys. Rev. A* **84**, 032326 (2011).

36. Pang, C.-Q., Zhang, F.-L., Xu, L.-F., Liang, M.-L. & Chen, J.-L. Sequential state discrimination and requirement of quantum dissonance. *Phys. Rev. A* **88**, 052331 (2013).
37. Zhang, Z.-H., Zhang, F.-L. & Liang, M.-L. Sequential state discrimination with quantum correlation. *Quant. Inf. Process.* **17**, 260 (2018).
38. Hillery, M. & Mimih, J. Sequential discrimination of qudits by multiple observers. *J. Phys. A: Math. Theor.* **50**, 455301 (2017).
39. Namkung, M. & Kwon, Y. Optimal sequential state discrimination between two mixed quantum states. *Phys. Rev. A* **96**, 022318 (2017).
40. Namkung, M. & Kwon, Y. Analysis of optimal sequential state discrimination for linearly independent pure quantum states. *Sci. Rep.* **8**, 6515 (2018).
41. Namkung, M. & Kwon, Y. Generalized sequential state discrimination for multiparty QKD and its optical implementation. *Sci. Rep.* **10**, 8247 (2020).
42. Solis-Prosser, M. A. *et al.* Experimental multiparty sequential state discrimination. *Phys. Rev. A* **94**, 042309 (2016).
43. Namkung, M. & Kwon, Y. Sequential state discrimination of coherent states. *Sci. Rep.* **8**, 16915 (2018).
44. Bennett, C. H., Brassard, G. Quantum cryptography: Public key distribution and coin tossing, Int. Conf. on Computers, Systems, & Signal Processing, Bangalore, India (1984).
45. Bennett, C. H., & Brassard, G. Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Vol. 175, pp. 8 (New York, 1984).
46. Bruss, D. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.* **81**, 3018 (1998).
47. Scarani, V., Acin, A., Ribordy, G. & Gisin, N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.* **92**, 057901 (2004).
48. Bennett, C. H., Bessette, F., Brassard, G., Salvail, L. & Smolin, J. Experimental quantum cryptography. *J. Crypt.* **5**, 3 (1992).
49. Yuan, Z. *et al.* 10-Mb/s quantum key distribution. *J. Lightwave Tech.* **36**, 3427 (2018).
50. Grosshans, F. & Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **88**, 057902 (2002).
51. Papanastasiou, P., Weedbrook, C. & Pirandona, S. Continuous-variable quantum key distribution in fast fading channels. *Phys. Rev. A* **97**, 032011 (2018).
52. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661 (1991).
53. Bennett, C. H., Brassard, G. & Mermin, N. D. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.* **68**, 557 (1992).
54. Csiszar, I. & Korner, J. Broadcast channel with confidential messages. *IEEE Trans. Inf. Theory* **24**, 339 (1978).
55. Torres-Ruiz, F. A. *et al.* Unambiguous modification of nonorthogonal single- and two-photon polarization states. *Phys. Rev. A* **79**, 052113 (2009).
56. Cabello, A., Feito, A. & Lamas-Linares, A. Bell's inequalities with realistic noise for polarization-entangled photons. *Phys. Rev. A* **72**, 052112 (2005).
57. Cariolaro, G. *Quantum Communications* (Springer, Switzerland, 2015).
58. Bennett, C. H. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **68**, 3121 (1992).
59. Fields, D., Han, R., Hillery, M. & Bergou, J. A. Extracting unambiguous information from a single qubit by sequential observers. *Phys. Rev. A* **101**, 012118 (2020).
60. Kwait, P. G. *et al.* New high-intensity source of polarization-entangled photon pairs. *Phys. Rev. Lett.* **75**, 4337 (1995).
61. Nielson, M. A. & Chuang, I. *Quantum Computation and Quantum Information* (Cambridge University Press, Cham, 2020).
62. Kim, Y.-S., Lee, J.-C., Kwon, O. & Kim, Y.-H. Protecting entanglement from decoherence using weak measurement and quantum measurement reversal. *Nat. Phys.* **8**, 117–120 (2012).
63. For detail, see the data sheet written in https://singlequantum.com/products/.
64. Burenkov, I. A., Jabir, M. V. & Polyakov, S. V. Practical quantum-enhanced receivers for classical communication. *AVS Quantum Sci.* **3**, 025301 (2021).
65. Notarnicola, M. N., Jarzyna, M., Olivares, S. & Banaszek, K. Optimizing state-discrimination receivers for continuous-variable quantum key distribution over a wiretap channel. *New J. Phys.* **25**, 103014 (2023).
66. Serafini, A. *Quantum Continuous Variables: A Primer for Theoretical Methods* (CRC Press, Cham, 2017).

Acknowledgements

This work is supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (NRF2020M3E4A1080088 and NRF2022R1F1A1064459) and and Creation of the Quantum Information Science RD Ecosystem (Grant No. 2022M3H3A106307411) through the National Research Foundation of Korea (NRF) funded by the Korean government (Ministry of Science and ICT).

Author contributions

M.N. and Y.K. conceived the main idea and wrote this manuscript. M.N. performed main calculation in this manuscript and analyzed the theoretical results. Y.K. discussed the analyzed results and improved this manuscript. All authors read and approved the final manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to Y.K.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

© The Author(s) 2024