SCIENTIFIC REPORTS
nature research

OPEN

Generalized sequential state discrimination for multiparty QKD and its optical implementation

Min Namkung & Younghun Kwon

Sequential state discrimination is a strategy for *N* separated receivers. As sequential state discrimination can be applied to multiparty quantum key distribution (QKD), it has become one of the relevant research fields in quantum information theory. Up to now, the analysis of sequential state discrimination has been confined to special cases. In this report, we consider a generalization of sequential state discrimination. Here, we do not limit the prior probabilities and the number of quantum states and receivers. We show that the generalized sequential state discrimination can be expressed as an optimization problem. Moreover, we investigate a structure of generalized sequential state discrimination for two quantum states and apply it to multiparty QKD. We demonstrate that when the number of receivers is not too many, generalized sequential state discrimination for two pure states can be suitable for multiparty QKD. In addition, we show that generalized sequential state discrimination for two mixed states can be performed with high optimal success probability. This optimal success probability is even higher than those of quantum reproducing and quantum broadcasting strategy. Thus, generalized sequential state discrimination of mixed states is adequate for performing multiparty QKD. Furthermore, we prove that generalized sequential state discrimination can be implemented experimentally by using linear optics. Finally, we analyze the security of multiparty QKD provided by optimal sequential state discrimination. Our analysis shows that the multiparty QKD guarantees nonzero secret key rate even in low channel efficiency.

In quantum mechanics, one cannot always discriminate quantum states that are non-orthogonal to each other. Therefore, a strategy to discriminate these quantum states is required. Investigation of the strategy for quantum state discrimination is one of the fundamental research fields in quantum information processing. The concept of quantum state discrimination can be understood as a game consisting of a sender Alice and a receiver Bob. In this game, Alice prepares a quantum state out of two or more than two quantum states, with a prior probability. It is assumed that Alice has informed Bob about the prior probabilities before Bob performs a measurement for quantum state discrimination. With the information, Bob measures Alice's quantum state. Bob's measurement outcome is divided into an inconclusive and a conclusive result. If the measurement outcome is conclusive, Bob can use the outcome to distinguish Alice's quantum state. If it is inconclusive, Bob cannot figure out the quantum state that Alice had prepared. The purpose of quantum state discrimination is to maximize the probability that Bob's conclusive result is correct. Many researchers have proposed a variety of discrimination strategies. In the minimum error discrimination strategy, Bob's measurement is designed to obtain only a conclusive result[1–5]. The purpose of this strategy is to minimize the probability that a conclusive result is erroneous. In the unambiguous discrimination strategy, Bob's measurement is designed to guarantee that his conclusive result is always correct[6–12]. The purpose of this strategy is to minimize the probability, that the outcome is inconclusive. In the maximal confidence strategy, Bob should maximize the confidence of a conclusive result[13]. Recently, other strategies, that interpolate between minimum error discrimination and unambiguous discrimination have been proposed. In the error margin strategy, Bob's measurement is designed not to make his error probability surpass an error margin[14–17]. In the fixed rate of the inconclusive result strategy, the probability that Bob obtains an inconclusive result is fixed to a specific value[18–23]. It is well known that quantum state discrimination provides a variety of quantum information protocols. Especially, unambiguous discrimination can be fruitfully applied to quantum key distribution (QKD)[24], quantum random number generator[25] and quantum state tomography[26].

Department of Applied Physics, Hanyang University, Ansan, Kyunggi-Do, 425-791, South Korea. e-mail: mslab.nk@gmail.com; yyhkwon@hanyang.ac.kr

In 2013, Bergou *et al.*[27] proposed *the sequential state discrimination strategy*. This strategy can consist of many receivers (called Bob 1, Bob 2 … Bob N), who are separated and are not allowed to perform classical communication with each other. In sequential state discrimination, a sender Alice sends one out of two quantum states, with a prior probability to Bob 1. It is assumed that all receivers are aware of the prior probabilities, before they perform sequential state discrimination. Bob 1 performs a measurement to discriminate Alice's quantum state. After the measurement, Bob 1 sends his post-measurement state to Bob 2. Then, Bob 2 performs his measurement to discriminate Bob 1's post-measurement state. This process is sequentially performed. The purpose of sequential state discrimination is to maximize the probability that all receivers successfully discriminate Alice's quantum state. According to Bergou *et al.*[27], the optimal (maximum) success probability is non-zero, in general. It implies that Bob $I+1$ can obtain information about Alice's quantum state, from Bob I's post-measurement state. This result not only enables us to know the property of a non-projective measurement but also allows its application to multiparty QKD strategy. Bergou *et al.*[27] and Pang *et al.*[28] separately investigated the sequential state discrimination of two pure states with equal prior probabilities. Solis-Prosser *et al.*[29] implemented the sequential state discrimination tratégy. In their work, two polarized single photon states with equal prior probabilities, were considered. Moreover, Zhang *et al.*[30] investigated the sequential state discrimination of two pure states with unequal prior probabilities. Hillery and Mimih[31] considered the sequential state discrimination of N symmetric pure state, with equal prior probabilities.

However, most studies of sequential state discrimination have been focused on special cases. In other words, the generalized structure of sequential state discrimination has not been investigated yet[32–34]. Therefore, in this report, we consider a generalization of sequential state discrimination. That is, in constructing sequential state discrimination, we do not limit the prior probabilities and the number of quantum states and receivers. Moreover, we consider the most general case of quantum states, in which every quantum state can be either pure[32] or mixed state[33]. Because unambiguous discrimination of general mixed states is not known yet[35–37], sequential state discrimination for general mixed states is beyond the scope of this paper. However, if mixed states are given in the form of Herzog's work[36], we can build generalized sequential state discrimination of two mixed states. Also, in terms of success probability, generalized sequential state discrimination provides better result in mixed states than in pure states.

First, we show that generalized sequential state discrimination can be expressed to a mathematical optimization problem. This optimization problem provides an optimal positive-operator-valued-measurement (POVM) condition, as well as an optimal success probability. Exploiting this structure, we explicitly investigate the generalized sequential state discrimination of two quantum states. Naturally, our investigation contains previous works[27,28]. Also, we apply it to multiparty QKD. We show that if the number of receivers is too many, generalized sequential state discrimination of two pure states can be performed, with very small optimal success probability. It means that generalized sequential state discrimination of two pure states can be suitable for multiparty QKD, only when the number of receivers is not too many. Meanwhile, generalized sequential state discrimination of two mixed states can be performed, with high optimal success probability. Especially, its optimal success probability exceeds those of quantum reproducing[27] and quantum broadcasting[38,39] strategy. It implies that generalized sequential state discrimination of two mixed states can be more suitable for multiparty QKD than other strategies.

In addition, we show that linear optics can be used to experimentally implement generalized sequential state discrimination. Here, our models can be implemented by modifying the Banaszek model[40] or the Huttner model[41]. We show that generalized sequential state discrimination of binary coherent states[34] can be implemented optimally. Moreover, we show that generalized sequential state discrimination of two mixed states can be implemented optimally. Further, we consider mixed states, which consists of coherent states. When an information carrier is a coherent state, which is robust in a noisy environment[42], our model can be suitable for implementing a realistic multiparty QKD.

Finally, we analyze the security of multiparty QKD based on optimal sequential state discrimination. It is known that B92 protocol provides unconditional security[43]. Therefore, one can guess that the QKD based on generalized sequential state discrimination guarantees security. To show this, we evaluate the secret key rate[44] of multiparty QKD based on generalized sequential state discrimination. Our result tells that the multiparty QKD guarantees nonzero secret key rate even in low channel efficiency. In addition, our multiparty QKD is composed of the method based on prepare and measure[24,45,46] and is more robust in noise than the QKD of multipartite entanglement.

Results

Scenario of Sequential State Discrimination. The concept of generalized sequential state discrimination can be understood as a game, consisting of a sender Alice and N receivers such as Bob 1, Bob 2,…, Bob N (see Fig. 1). In this scenario, every party acts as follows: Alice prepares a quantum state $\rho_i \in \{\rho_1, \ldots, \rho_n\}$, with a prior probability q_i and sends ρ_i to Bob 1. Bob 1 performs a POVM $\{M_0^{(1)}, M_1^{(1)}, \ldots, M_n^{(1)}\}$ on Alice's quantum state, for unambiguous discrimination. Here, $M_j^{(1)}$ is a POVM element, corresponding to a measurement outcome j. If Bob 1 obtains a conclusive outcome ($j \neq 0$), he thinks Alice's quantum state as ρ_j. If Bob 1 obtains an inconclusive result ($j = 0$), he cannot figure out which quantum state Alice had prepared. If Bob 1 obtains a conclusive result, he sends a post-measurement state to Bob 2. Because in generalized sequential state discrimination every receiver should perform unambiguous discrimination, the post-measurement state of Bob 1 is given as $\sigma_i^{(1)} \propto K_j^{(1)} \rho_i K_j^{(1)\dagger} \delta_{ij} (i, j \neq 0)$. Here, δ_{ij} is the Kronecker delta and $K_i^{(1)}$ is the Kraus operator, satisfying $M_i^{(1)} = K_i^{(1)\dagger} K_i^{(1)}$. Likewise, Bob 2 performs unambiguous discrimination on Bob 1's post-measurement state $\sigma_i^{(1)}$, using POVM $\{M_0^{(2)}, M_1^{(2)}, \ldots, M_n^{(2)}\}$. Then, Bob 2 sends his post-measurement state $\sigma_i^{(2)} \propto K_j^{(2)} \sigma_i^{(1)} K_j^{(2)\dagger} \delta_{ij}$ to Bob 3. This process is sequentially conducted from Bob 3 to Bob N. The average success probability of generalized sequential state discrimination is given as

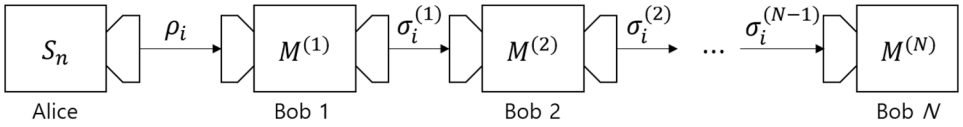


Figure 1. Schematic of the concept of sequential state discrimination. In this concept, Alice prepares $\rho_i \in S_n$, with a prior probability q_i. Bob 1 discriminates Alice's quantum state, using POVM $M^{(1)} = \{M_i^{(1)}\}_{i=0}^n$, without an error. Using POVM $M^{(2)} = \{M_i^{(2)}\}_{i=0}^n$, Bob 2 also discriminates $\sigma_i^{(1)}$ which is the post-measurement state of Bob 1, without an error. Then, this process is sequentially performed from Bob 3 to Bob N.

$$P_s^{(B_1,\ldots,B_N)} = \sum_{i=1}^{n} q_i \mathrm{Tr}[\rho_i M_i^{(1)}]\mathrm{Tr}[\rho_i^{(1)} M_i^{(2)}]\mathrm{Tr}[\rho_i^{(2)} M_i^{(3)}] \times \cdots \times \mathrm{Tr}[\rho_i^{(N-1)} M_i^{(N)}]. \quad (1)$$

(In Eq. (1), each Bob 1, Bob 2, …, Bob N is briefly expressed as B_1, B_2, …, B_N). The purpose of generalized sequential state discrimination is to maximize the average success probability, as expressed in Eq. (1). In the process, every receiver should obey the following rules:

Rule 1. Bob 1, Bob 2, …, Bob $N-1$ performs a nonoptimal unambiguous discrimination. However, Bob N performs an optimal unambiguous discrimination.

Rule 2. Classical communication is forbidden between every receiver.

If Bob $I \in \{1, 2, \ldots, N-1\}$ performs an optimal unambiguous discrimination, Bob $I+1$ cannot obtain any information from Bob I's post-measurement state. Moreover, if one of the receivers sends his measurement outcome through classical communication, an eavesdropper can steal the measurement outcome without being noticed by any receivers. Thus, it is reasonable that Rules 1 and 2 should be imposed on every receiver.

Construction of the Optimization Problem. In this section, we express generalized sequential state discrimination as an optimization problem. To construct the optimization problem, we should involve not only two rules but also POVM conditions for every receiver. First, we should consider a POVM that performs an unambiguous discrimination.

POVM for unambiguous discrimination. Let us find the condition for the POVM $\{M_0, M_1, \ldots, M_n\}$ that performs an unambiguous discrimination. This POVM should satisfy the following conditions (I) $M_i \geq 0 (\forall\, i \in \{1, \ldots, n\})$ (II) $M_i = M_i^\dagger (\forall\, i \in \{1, \ldots, n\})$ (III) $M_0 + M_1 + \cdots + M_n = I$ and (IV) $\mathrm{Tr}\rho_i M_j = \delta_{ij}\mathrm{Tr}\rho_i M_i (\forall\, i, j \in \{1, \ldots, n\})$. Here, the conditions of (I), (II), and (III) are positive-semidefinite, Hermitian and completeness condition, respectively. Especially, (IV) is the condition in which the POVM performs an unambiguous discrimination. However, understanding an unambiguous discrimination is confined only to a special set of quantum states $S_n = \{\rho_1, \rho_2, \ldots, \rho_n\}$. If the set of quantum states S_n satisfies the following theorem, there exists a POVM that performs an unambiguous discrimination on S_n.

Theorem 1. If[7] $\mathrm{supp}(\rho_i)$ satisfies $\mathrm{supp}(\rho_i) \nsubseteq \bigcup_{j\neq i} \mathrm{supp}(\rho_k)$ for all $\rho_i \in S_n$, there exists a POVM that performs an unambiguous discrimination on S_n.

If S_n satisfies Theorem 1, the support of M_i can be spanned by the support of ρ_i, orthogonal to $\bigcup_{j\neq i} \mathrm{supp}(\rho_k)$. For example, let us consider $S_2 = \{\rho_1, \rho_2\}$. Then, the support of $M_1(M_2)$ is spanned by the kernel of $\rho_2(\rho_1)$[7]. For $\tilde{S}_n = \{\psi_1, \psi_2, \ldots, \psi_n\}$, Theorem 1 is simply stated as follows.

Theorem 2. If[6] $\tilde{S}_n$ is a set of linearly independent pure states, there exists a POVM that performs an unambiguous discrimination on $\tilde{S}_n$.

Proof. Suppose $\tilde{S}_n$ is a set of linearly independent pure states. Then, Gram matrix $G = \{\langle\psi_i|\psi_j\rangle\}_{i,j=1}^n$ is positive definite[47]. Thus, there exists an inverse of G. Using G^{-1}, we can construct M_i as

$$M_i = \alpha_i |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|, \quad |\tilde{\psi}_i\rangle = \sum_{j=1}^{n} G_{ji}^{-1}|\psi_j\rangle. \quad (2)$$

Here, $\alpha_i \geq 0$. The inner product between $|\psi_j\rangle$ and $|\tilde{\psi}_i\rangle$ is simply calculated as

$$\langle\psi_j|\tilde{\psi}_i\rangle = \sum_{j=1}^{n} G_{ki}^{-1} G_{jk} = (GG^{-1})_{ji} = \delta_{ji}.$$

Therefore, the equality $\langle\psi_j|M_i|\psi_j\rangle = \delta_{ij}\langle\psi_i|M_i|\psi_i\rangle$ holds for all POVM elements $M_i \in \{M_1, \ldots, M_n\}$. We notice that $M_1, \ldots, M_n$, in Eq. (2), are Hermitian and positive-semidefinite. According to the completeness condition, $M_0 = I - M_1 - \cdots - M_n$ is also Hermitian. Now, we show that M_0 can be positive-semidefinite. If $\alpha_1, \ldots, \alpha_n$ are

efficiently small, M_0 tends to converge to I. In this case, M_0 is obviously positive-semidefinite, which completes the proof of Theorem. □

By Theorem 2, every POVM $\{M_0, M_1, \ldots, M_n\}$ has a one-to-one correspondance with an n-dimensional real vector $(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Moreover, the POVM conditions can be expressed, in terms of every component in this real vector. The positive-semidefiniteness condition of M_0 can be obtained through the following theorem.

Theorem 3. Let[32] us define a Hermitian matrix $\bar{M} = \{\langle\psi_i|M_0|\psi_j\rangle\}_{i,j=1}^n$ and all $m \times m (m < n)$ principal submatrices $\bar{M}_m$. M_0 is positive-semidefinite if and only if every $\bar{M}$ and $\forall\ \bar{M}_m$ is positive-semidefinite.

Proof. We exploit the fact that M_0 is positive-semidefinite if and only if $\langle\psi|M_0|\psi\rangle \geq 0$ for all $|\psi\rangle \in \mathscr{H}$[47]. Because $\bar{S}_n$ is a set of linearly independent pure states, every $|\psi\rangle \in \mathscr{H}$ can be expressed as $|\psi\rangle = v_1|\psi_1\rangle + \cdots + v_n|\psi_n\rangle$. We can easily obtain the following equality:

$$\langle\psi|M_0|\psi\rangle = v^\dagger \bar{M} v.$$

Here, $v = (v_1, v_2, \ldots, v_n) \in \mathbb{C}^n$. In other words, $\langle\psi|M_0|\psi\rangle \geq 0$ for all $|\psi\rangle \in \mathscr{H}$, if and only if $v^\dagger \bar{M} v \geq 0$ for all $v \in \mathbb{C}^n$. Every components in V needs not to be nonzero. That is, $v^\dagger \bar{M} v \geq 0$ if and only if $\forall\ \bar{M}, \bar{M}_m$ are positive-semidefinite. □

According to Rule 2, no receiver can perform any classical communication. In sequential state discrimination, the post-measurement state contains a measurement outcome. Hence, we should construct a Kraus operator, corresponding to POVM[48]. According to Eq. (2), every POVM, corresponding to conclusive result, is rank-1. Therefore, K_i is expressed as $K_i = U_i\sqrt{M_i}$, from singular value decomposition. Here, U_i is unitary operator and $\sqrt{M_i}$ is a square-root operator of M_i. Then, the Kraus operator, corresponding to conclusive result, is constructed as

$$K_i = U_i\sqrt{M_i} = U_i\sqrt{\alpha_i}|\tilde{\psi}_i\rangle\langle\tilde{\psi}_i| = \sqrt{\alpha_i}(U_i|\tilde{\psi}_i\rangle)\langle\tilde{\psi}_i| = \sqrt{\alpha_i}|\phi_i\rangle\langle\tilde{\psi}_i|.$$

Then, the post-measurement state, corresponding to conclusive result i, is expressed as $|\phi_i\rangle \propto K_i|\psi_i\rangle$[48]. Now, we construct the Kraus operator K_0, which satisfies $M_0 = K_0^\dagger K_0$. It is complicated to obtain K_0 from M_0. If we assume that every pure state in $\bar{S}_n$ spans $\mathscr{H}$, when $K_0|\psi_i\rangle$, for some i, is not involved in $\{K_j|\psi_j\rangle\}_{j=1}^n$, every post-meaurement state $\{K_0|\psi_i\rangle\}_{i=1}^n \cup \{K_i|\psi_i\rangle\}_{i=1}^n$ is linearly dependent. Therefore, post-measurement states cannot be discriminated unambiguously. This implies that every post-measurement state $K_0|\psi_i\rangle$ should be involved in $\{K_i|\psi_i\rangle\}_{i=1}^n$. We construct K_0 that maps $|\psi_i\rangle$ into $K_i|\psi_i\rangle$, and it is expressed as[32,33]

$$K_0 = \sqrt{\gamma_1}|\phi_1\rangle\langle\tilde{\psi}_1| + \sqrt{\gamma_2}|\phi_2\rangle\langle\tilde{\psi}_2| + \cdots + \sqrt{\gamma_n}|\phi_n\rangle\langle\tilde{\psi}_n|.$$

Here, $\gamma_i \geq 0$. From $\gamma_i = 1 - \alpha_i$, we can see that α_i is less than 1. We should find γ_i to satisfy $M_0 = K_0^\dagger K_0$. To solve this problem, we exploit the following theorem.

Theorem 4. Let[33] $\bar{S}_n$ be a set of linearly independent pure states. Then, $A = B$ if and only if $\langle\psi_i|A|\psi_j\rangle = \langle\psi_i|B|\psi_j\rangle (\ \forall\ i, j)$.

Substituting both A and B, in Theorem 4, into each M_0 and $K_0^\dagger K_0$, we obtain

$$\gamma_i = 1 - \alpha_i,\ \ \sqrt{\gamma_i\gamma_j}\langle\phi_i|\phi_j\rangle = \langle\psi_i|\psi_j\rangle. \tag{3}$$

Equation (3) includes an argument from Bergou *et al.*[27] Combining these two equalities, we derive an overlap between two post-measurement states as

$$\langle\phi_i|\phi_j\rangle = \frac{\langle\psi_i|\psi_j\rangle}{\sqrt{(1-\alpha_i)(1-\alpha_j)}}. \tag{4}$$

According to Eq. (4), the overlap $\langle\phi_i|\phi_j\rangle$ is larger than or equal to $\langle\psi_i|\psi_j\rangle$. Because $|\langle\phi_i|\phi_j\rangle| \leq 1$, we obtain

$$(1-\alpha_i)(1-\alpha_j) \geq |\langle\psi_i|\psi_j\rangle|^2,\ \ \forall\ i, j. \tag{5}$$

This equality corresponds to the POVM condition, which performs an unambiguous discrimination on a pure state ($\bar{S}_2$). If every receiver performs an optimal unambiguous discrimination, Eq. (5) becomes a strict equality. Then, the overlap between post-measurement states becomes one, according to Eq. (4). Hence, to obey Rule 1, the POVM of Bob 1, Bob 2,..., Bob $N-1$ should not satisfy the equality of Eq. (5). Furthermore, because every submatrix $\bar{M}_{ab}$ should be positive-semidefinite, Eq. (5) is also involved in the POVM condition, performing an unambiguous discrimination of n pure states.

Generalizing POVM for mixed state discrimination. In this section, we investigate the generalized sequential state discrimination of mixed quantum states. Unfortunately, an explicit form of POVM, that performs an unambiguous discrimination of arbitrary mixed states is unknown. That is because we do not know how to deal with Theorem 1. When mixed states can be expressed in the form given by Herzog's work[36], POVM can be constructed explicitly. Suppose that every mixed state has the same rank. Then, each mixed state on Hilbert space $\mathscr{H} = \mathscr{H}_1 \oplus \mathscr{H}_2 \oplus \cdots \oplus \mathscr{H}_m$ has the following form:

$$\rho_i = r_{i1}|r_{i1}\rangle\langle r_{i1}| \oplus r_{i2}|r_{i2}\rangle\langle r_{i2}| \oplus \cdots \oplus r_{im}|r_{im}\rangle\langle r_{im}|, \;\; r_{i1}, r_{i2}, \ldots, r_{im} > 0. \tag{6}$$

Here, $m = \mathrm{rank}(\rho_i)$. According to the trace condition of ρ_i, $\sum_{j=1}^{m} r_{ij} = 1$ holds for all i. If we consider that every mixed state has a form like that of Eq. (6), then Theorem 1 can be explicitly expressed as follows:

Theorem 5. Suppose[33] that all elements in S_n have the same form as that of Eq. (6). If $\{|r_{1j}\rangle, |r_{2j}\rangle, \ldots, |r_{nj}\rangle\}$ are linearly independent for every $j \in \{1, \ldots, m\}$, then there exists a POVM that performs an unambiguous discrimination on S_n.

Proof. Let us construct the POVM element M_i, corresponding to measurement outcome i as

$$M_i = M_{i1} \oplus M_{i2} \oplus \cdots \oplus M_{im}.$$

Here, $\{M_{0j}, M_{1j}, \ldots, M_{nj}\}$ is a sub-POVM, defined on sub-Hilbert space $\mathscr{H}_j$. Because every M_{ij} is positive-semidefinite, M_i is also positive-semidefinite. The completeness condition of POVM $\{M_0, M_1, \ldots, M_n\}$ is straightforwardly proved as

$$\begin{aligned}\sum_{i=0}^{n} M_i &= \sum_{i=0}^{n} M_{i1} \oplus M_{i2} \oplus \cdots \oplus M_{im} \\ &= \left(\sum_{i=0}^{n} M_{i1}\right) \oplus \left(\sum_{i=0}^{n} M_{i2}\right) \oplus \cdots \oplus \left(\sum_{i=0}^{n} M_{im}\right) \\ &= I_1 \oplus I_2 \oplus \cdots \oplus I_m \\ &= I.\end{aligned}$$

Here, I_j is an identity operator, defined on sub-Hilbert space $\mathscr{H}_j$. Sub-POVM $\{M_{0j}, M_{1j}, \ldots, M_{nj}\}$ only acts on $\{|r_{1j}\rangle, |r_{2j}\rangle, \ldots, |r_{nj}\rangle\}$. If $\{|r_{1j}\rangle, |r_{2j}\rangle, \ldots, |r_{nj}\rangle\}$ are linearly independent, every sub-POVM is obtained, using similar process as Theorems 2 and 3. Therefore, we obtain POVM that performs unambiguous discrimination, which completes the proof of Theorem. □

With the help of Theorem 5, we can apply a method that deals with the discrimination of pure states into a mixed-state case. If $i \neq 0$, the POVM element M_i can be expressed as

$$M_i = \alpha_{i1}|\tilde{r}_{i1}\rangle\langle\tilde{r}_{i1}| \oplus \alpha_{i2}|\tilde{r}_{i2}\rangle\langle\tilde{r}_{i2}| \oplus \cdots \oplus \alpha_{im}|\tilde{r}_{im}\rangle\langle\tilde{r}_{im}|. \tag{7}$$

According to the completeness condition, M_0 is given as

$$\begin{aligned}M_0 &= M_{01} \oplus M_{02} \oplus \cdots \oplus M_{0m} \\ &= \left(I_1 - \sum_{i=0}^{n} M_{01}\right) \oplus \left(I_2 - \sum_{i=0}^{n} M_{02}\right) \oplus \cdots \oplus \left(I_{m_0} - \sum_{i=0}^{n} M_{0m_0}\right) \\ &= \left(I_1 - \sum_{i=0}^{n} \alpha_{01}\tilde{r}_{01}\tilde{r}_{01}\right) \oplus \cdots \oplus \left(I_{m_0} - \sum_{i=0}^{n} \alpha_{0m}\tilde{r}_{0m}\tilde{r}_{0m}\right).\end{aligned} \tag{8}$$

Then, the Kraus operator K_i, corresponding to M_i of Eq. (8), is given as

$$K_i = \sqrt{\alpha_{i1}}|s_{i1}\rangle\langle\tilde{r}_{i1}| \oplus \sqrt{\alpha_{i2}}|s_{i2}\rangle\langle\tilde{r}_{i2}| \oplus \cdots \oplus \sqrt{\alpha_{im}}|s_{im}\rangle\langle\tilde{r}_{im}|.$$

Hence, the post-measurement state σ_i is expressed as

$$\begin{aligned}\sigma_i &= \frac{K_i\rho_i K_i^{\dagger}}{Tr[K_i\rho_i K_i^{\dagger}]} \\ &= \frac{r_{i1}\alpha_{i1}|s_{i1}\rangle\langle s_{i1}| \oplus r_{i2}\alpha_{i2}|s_{i2}\rangle\langle s_{i2}| \oplus \cdots \oplus r_{im}\alpha_{im}|s_{im}\rangle\langle s_{im}|}{r_{i1}\alpha_{i1} + r_{i2}\alpha_{i2} + \cdots + r_{im}\alpha_{im}}.\end{aligned}$$

We can obtain the Kraus operator K_0, corresponding to M_0, by exploiting Theorem 3. Because every eigenvector of σ_i should satisfy

$$\langle s_{ij}|s_{kj}\rangle = \frac{\langle r_{ij}|r_{kj}\rangle}{\sqrt{(1-\alpha_{ij})(1-\alpha_{kj})}}, \tag{9}$$

from Eq. (9) we can obtain

$$(1-\alpha_{ij})(1-\alpha_{kj}) \geq |r_{ij}|r_{kj}|^2. \tag{10}$$

Both Eqs. (9) and (10) imply the following meaning. if either α_{ij} or α_{kj} is nonzero, $|\langle s_{ij}|s_{kj}\rangle|$ is larger than $|\langle r_{ij}|r_{kj}\rangle|$. That is, the support of two post-measurement states is more overlapped than that of Alice's mixed states. If an optimal unambiguous discrimination is performed, Eq. (10) becomes a strict equality. Moreover, according

to Eq. (9), $|\langle s_{ij}|s_{kj}\rangle|$ becomes equal to 1. Therefore, for all i, $\mathrm{supp}(\sigma_i) = \cup_{j\neq i}\ \mathrm{supp}(\sigma_j)$ holds, which implies that $\{\sigma_1, \ldots, \sigma_n\}$ cannot be discriminated, without any error.

Now, let us consider the case where every ρ_i has a different rank. Without loss of generality, we can assume an inequality such as $\mathrm{rank}(\rho_1) > \mathrm{rank}(\rho_2) > \cdots > \mathrm{rank}(\rho_n)$. Then, a POVM element can be constructed as

$$M_i = M_{i1} \oplus M_{i2} \oplus \cdots \oplus M_{im_i},$$

where $m_i = \mathrm{rank}(\rho_i)$. Each POVM element can be constructed in the following manner: If $1 \leq j \leq m_1$, sub-POVM $\{M_{0j}, M_{1j}, \ldots, M_{nj}\}$ discriminates $\{|r_{1j}\rangle, |r_{2j}\rangle, \ldots, |r_{nj}\rangle\}$ without any error. If $m_1 < j \leq m_2$, sub-POVM $\{M_{0j}, M_{1j}, \ldots, M_{nj}\}$ discriminates $\{|r_{1j}\rangle, |r_{2j}\rangle, \ldots, |r_{n-1j}\rangle\}$. The remaining part of the POVM elements can also be constructed inductively.

Optimization problem for pure states case. Assume that $|\psi_i\rangle \in \bar{S}_n$ is prepared, with a prior probability q_i. Then, the POVM $\{M_0^{(I)}, M_1^{(I)}, \ldots, M_n^{(I)}\}$ of Bob $I \in \{1, \ldots, N\}$ corresponds to a vector $(\alpha_1^{(I)}, \ldots, \alpha_n^{(I)})$ in an n–dimensional real vector space. Using this vector, we can express Eq. (1) as

$$P_s^{(B_1,\ldots,B_N)} = \sum_{i=1}^{n} q_i \alpha_i^{(1)} \alpha_i^{(2)} \alpha_i^{(3)} \times \cdots \times \alpha_i^{(N)}, \tag{11}$$

where $\alpha_i^{(1)} = \langle\psi_i|M_i^{(1)}|\psi_i\rangle$, $\alpha_i^{(I)} = \langle\phi_i^{(I-1)}|M_i^{(I)}|\phi_i^{(I-1)}\rangle$. The constraints on POVM can be expressed in terms of $(\alpha_1^{(I)}, \ldots, \alpha_n^{(I)})$. Applying Rule 1 and Rule 2[32], we can construct POVM conditions as

$$\begin{aligned} (\alpha_1^{(I)}, \ldots, \alpha_n^{(I)}) &\in C_{\mathrm{int}}^{(I)},\ I \leq N-1 \\ (\alpha_1^{(N)}, \ldots, \alpha_n^{(N)}) &\in \partial C^{(N)}. \end{aligned} \tag{12}$$

Here, $C_{\mathrm{int}}^{(I)}$ and $\partial C^{(I)}$ are defined as

$$\begin{aligned} C^{(I)} &= \{(\alpha_1^{(I)}, \ldots, \alpha_n^{(I)}) \in \mathbb{R}^n | \bar{M} \geq 0 \wedge \bar{M}_m \geq 0\ \ \forall\, m < n\}, \\ C_{\mathrm{int}}^{(I)} &= \{(\alpha_1^{(I)}, \ldots, \alpha_n^{(I)}) \in \mathbb{R}^n | \bar{M} > 0 \wedge \bar{M}_m \geq 0\ \ \forall\, m < n\}, \\ \partial C^{(I)} &= \{(\alpha_1^{(I)}, \ldots, \alpha_n^{(I)}) \in \mathbb{R}^n | \bar{M} = 0 \wedge \bar{M}_m \geq 0\ \ \forall\, m < n\}. \end{aligned}$$

Then, Bob I's POVM condition is expressed as $C^{(I)} = C_{\mathrm{int}}^{(I)} \cup \partial C^{(I)}$. Combining Eq. (11) with Eq. (12), we can express generalized sequential state discrimination as following optimization problem[32]:

$$\begin{aligned} \text{maximize}\quad & P_s^{(B_1,\ldots,B_N)} = \sum_{i=1}^{n} q_i \alpha_i^{(1)} \alpha_i^{(2)} \alpha_i^{(3)} \times \cdots \times \alpha_i^{(N)} \\ \text{subject to}\quad & (\alpha_1^{(I)}, \ldots, \alpha_n^{(I)}) \in C_{\mathrm{int}}^{(I)},\ \forall\, I \leq N-1 \\ & (\alpha_1^{(N)}, \ldots, \alpha_n^{(N)}) \in \partial C^{(N)}. \end{aligned} \tag{13}$$

Now, let us investigate the geometric properties of each $C^{(I)}$. The set of POVM that performs an unambiguous discrimination is convex and $C^{(I)}$ is also convex:

Theorem 6. Every[32] $C^{(I)}$ is convex.

It is important to investigate the relation between $C^{(I)}$ and $C^{(I+1)}$, to analyze the generalized sequential state discrimination. In our previous work[32], we proposed the following conjecture:

Conjecture 1. If[32] there exists nonzero $\alpha_i^{(I)}$ in $(\alpha_1^{(I)}, \ldots, \alpha_n^{(I)})$, the size of set $C^{(I+1)}$ is smaller than that of $C^{(I)}$.

Considering the discrimination problem of two pure states, we can confirm that Conjecture 1 holds. Conjecture 1 has the following meaning. When the real vector $(\alpha_1^{(I)}, \ldots, \alpha_n^{(I)})$ has at least one nonzero component $\alpha_1^{(I)}$, Bob I can obtain partial information of Alice's quantum state, by performing a measurement on Bob $I-1$'s post-measurement state, with a nonzero probability. Conjecture 1 implies that options for POVM that Bob $I+1$ can choose are limited, as Bob I obtains the information. In the extreme case, if Bob I obtains the maximal information, then Bob $I+1$ cannot construct a POVM to unambiguously discriminate Bob I's post-measurement state, which means that Bob $I+1$ cannot obtain any information from Bob I's post-measurement state. Hence, we can propose the following conjecture:

Conjecture 2. If[32] $(\alpha_1^{(I)}, \ldots, \alpha_n^{(I)}) \in \partial C^{(I)}$, $(\alpha_1^{(I+1)}, \ldots, \alpha_n^{(I+1)}) = (0, \ldots, 0)$ is the only element of $C^{(I+1)}$.

If Alice prepares a pure state from $\bar{S}_2$, both Conjecture 1 and Conjecture 2 hold[32]. In the case of $N = 3$, we can numerically check that both conjectures 1 and 2 are correct.

Optimization problem for the mixed states case. Now, let us consider a mixed states case. When Alice prepares ρ_i, which is expressed as Eq. (6), Bob $I \in \{1, \ldots, N\}$'s POVM $\{M_0^{(I)}, M_1^{(I)}, \ldots, M_n^{(I)}\}$ corresponds to the real vector $(\alpha_{11}, \ldots, \alpha_{nm}) \in \mathbb{R}^{nm}$. This real vector is included in $\tilde{C}^{(I)} = \tilde{C}_{\mathrm{int}}^{(I)} \cup \partial\tilde{C}^{(I)}$, where $\tilde{C}_{\mathrm{int}}^{(I)}$ and $\partial\tilde{C}^{(I)}$ are respectively defined as

$$\tilde{C}_{\text{int}}^{(I)} = \tilde{C}_{\text{int},1}^{(I)} \bigcap \tilde{C}_{\text{int},2}^{(I)} \bigcap \cdots \bigcap \tilde{C}_{\text{int},m}^{(I)},$$
$$\partial\tilde{C}^{(I)} = \partial\tilde{C}_1^{(I)} \bigcap \partial\tilde{C}_2^{(I)} \bigcap \cdots \bigcap \partial\tilde{C}_m^{(I)}.$$

Here, $\tilde{C}_{\text{int},j}^{(I)}$ and $\partial\tilde{C}^{(I)}$ are respectively defined as

$$\tilde{C}_{\text{int},j}^{(I)} = \{(\alpha_{1j}, \ldots, \alpha_{nj}) \in \mathbb{R}^n | \bar{M}_j > 0 \wedge \bar{M}_{j,m} \geq 0 \ \ \forall\, m < n\},$$
$$\partial\tilde{C}_j^{(I)} = \{(\alpha_{1j}, \ldots, \alpha_{nj}) \in \mathbb{R}^n | \bar{M}_j = 0 \wedge \bar{M}_{j,m} \geq 0 \ \ \forall\, m < n\}.$$

$\bar{M}_j = \{\langle r_{ij}|M_{0j}|r_{kj}\rangle\}_{i,k=1}^n$ and $\bar{M}_{j,m}$ are $m \times m$ principal submatrices. Then, we can express generalized sequential state discrimination of mixed states, as following optimization problem[33]:

$$\begin{aligned} \text{maximize} \quad & P_s^{(B_1,\ldots,B_N)} = \sum_{i=1}^n q_i \left(r_{i1} \prod_{I=1}^N \alpha_{i1}^{(I)} + r_{i2} \prod_{I=1}^N \alpha_{i2}^{(I)} + \cdots r_{im} \prod_{I=1}^N \alpha_{im}^{(I)} \right) \\ \text{subject to} \quad & (\alpha_{1j}^{(I)}, \ldots, \alpha_{nj}^{(I)}) \in \tilde{C}_{\text{int},j}^{(I)}, \ \ \forall\, j, \ \ \forall\, I \leq N-1 \\ & (\alpha_{1j}^{(N)}, \ldots, \alpha_{nj}^{(N)}) \in \partial\tilde{C}_j^{(N)}. \ \ \forall\, j \end{aligned}$$

When $m = 1$, this optimization problem describes the generalized sequential state discrimination of pure states. Note that the j-th constraint only affects sub-POVM $\sum_{i=1}^n q_i \prod_{I=1}^N \alpha_{ij}^{(I)}$. From this property, this optimization problem can be partitioned into the following sub-optimization problems[33]:

$$\begin{aligned} \text{maximize} \quad & p_{s,j} = \sum_{i=1}^n q_i r_{ij} \left(\prod_{I=1}^N \alpha_{ij}^{(I)} \right) \\ \text{subject to} \quad & (\alpha_{1j}^{(I)}, \ldots, \alpha_{nj}^{(I)}) \in \tilde{C}_{\text{int},j}^{(I)}, \ \ \forall\, I \leq N-1 \\ & (\alpha_{1j}^{(N)}, \ldots, \alpha_{nj}^{(N)}) \in \partial\tilde{C}_j^{(N)}. \end{aligned}$$

Then, the optimal success probability is expressed as $\max P_s^{(B_1,\ldots,B_N)} = \max p_{s,1} + \max p_{s,2} + \cdots + \max p_{s,m}$.

Next, we consider the case that no mixed state has the same rank. More precisely, we assume that $\text{rank}(\rho_1) > \text{rank}(\rho_1) > \cdots > \text{rank}(\rho_n)$, without loss of generality. If $\text{rank}(\rho_l) < j \leq \text{rank}(\rho_{l+1})$, the j-th sub-optimization problem is given as

$$\begin{aligned} \text{maximize} \quad & p_{s,j} = \sum_{i=1}^{n-l} q_i r_{ij} \left(\prod_{I=1}^N \alpha_{ij}^{(I)} \right) \\ \text{subject to} \quad & (\alpha_{1j}^{(I)}, \ldots, \alpha_{nj}^{(I)}) \in \tilde{C}_{\text{int},j}^{(I)}, \ \ \forall\, I \leq N-1 \\ & (\alpha_{1j}^{(N)}, \ldots, \alpha_{nj}^{(N)}) \in \partial\tilde{C}_j^{(N)}. \end{aligned}$$

Because every sub-optimization problem in the case of mixed states is the same as that in the pure state case, if every mixed state is expressed as Eq. (6), we can apply the method for pure states to the generalized sequential state discrimination of mixed states. Unfortunately, Eq. (6) is not the case of the most general mixed state. However, if we use these mixed states as an information carrier, the optimal success probability of the generalized sequential state discrimination can exceed that of the quantum reproducing[27] and the quantum broadcasting strategy[39]. This implies that generalized sequential state discrimination is a more suitable strategy for application to multiparty QKD than the other two strategies. Furthermore, Eq. (6) can be implemented using linear optics. In the next sections, we explain these advantages in detail.

Generalized Sequential State Discrimination of Two Quantum States. In this section, we consider the optimization problem proposed in the previous section. We deal not only with the problem of two pure states but also with the problem of two mixed states in a multi-receiver case.

Generalized sequential state discrimination of two pure states. Here, we consider the generalized sequential state discrimination with an arbitrary N. First, let us consider the case of $N = 3$. The three receivers are denoted as Bob, Charlie, and David, and each POVM of Bob, Charlie, and David corresponds to the two dimensional real vectors (α_1, α_2), (β_1, β_2), and (γ_1, γ_2), respectively. According to Eq. (12), each real vector should satisfy

$$(\alpha_1, \alpha_2) \in C_{\text{int}}^{(\text{B})}, \ \ (\beta_1, \beta_2) \in C_{\text{int}}^{(\text{C})}, \ \ (\gamma_1, \gamma_2) \in \partial C^{(\text{D})}. \tag{14}$$

where $C_{\text{int}}^{(X)}$ and $\partial C^{(X)} (X \in \{B, C, D\})$ are respectively defined as[32]

$$
\begin{aligned}
C_{\text{int}}^{(\text{B})} &= \{(\alpha_1, \alpha_2) \in \mathbb{R}^2 | (1-\alpha_1)(1-\alpha_2) > |\langle\psi_1|\psi_2\rangle|^2\},\\
C_{\text{int}}^{(\text{C})} &= \{(\beta_1, \beta_2) \in \mathbb{R}^2 | (1-\beta_1)(1-\beta_2) > |\langle\phi_1^{(\text{B})}|\phi_2^{(\text{B})}\rangle|^2\},\\
C_{\text{int}}^{(\text{D})} &= \{(\gamma_1, \gamma_2) \in \mathbb{R}^2 | (1-\gamma_1)(1-\gamma_2) > |\langle\phi_1^{(\text{C})}|\phi_2^{(\text{C})}\rangle|^2\},\\
\partial C^{(\text{B})} &= \{(\alpha_1, \alpha_2) \in \mathbb{R}^2 | (1-\alpha_1)(1-\alpha_2) = |\langle\psi_1|\psi_2\rangle|^2\},\\
\partial C^{(\text{C})} &= \{(\beta_1, \beta_2) \in \mathbb{R}^2 | (1-\beta_1)(1-\beta_2) = |\langle\phi_1^{(\text{B})}|\phi_2^{(\text{B})}\rangle|^2\},\\
\partial C^{(\text{D})} &= \{(\gamma_1, \gamma_2) \in \mathbb{R}^2 | (1-\gamma_1)(1-\gamma_2) = |\langle\phi_1^{(\text{C})}|\phi_2^{(\text{C})}\rangle|^2\}.
\end{aligned}
$$

The set of POVM, labeled as X∈{B, C, D}, can be expressed as $C^{(\text{X})} = C_{\text{int}}^{(\text{X})} \cup \partial C^{(\text{X})}$. Therefore, Eq. (13) becomes[32]

$$
\begin{aligned}
\text{maximize} \quad & P_s^{(\text{B,C,D})} = q_1\alpha_1\beta_1\gamma_1 + q_2\alpha_2\beta_2\gamma_2\\
\text{subject to} \quad & (1-\alpha_1)(1-\alpha_2) > |\langle\psi_1|\psi_2\rangle|^2\\
& (1-\beta_1)(1-\beta_2) > |\langle\phi_1^{(\text{B})}|\phi_2^{(\text{B})}\rangle|^2\\
& (1-\gamma_1)(1-\gamma_2) = |\langle\phi_1^{(\text{C})}|\phi_2^{(\text{C})}\rangle|^2
\end{aligned}
\tag{15}
$$

To solve this problem, we need to consider the equality constraint of Eq. (15). David's optimal condition of generalized sequential state discrimination can be obtained by finding a tangential point (γ_1, γ_2) between a plane $P_s^{(\text{B,C,D})} = (q_1\alpha_1\beta_1)\gamma_1 + (q_2\alpha_2\beta_2)\gamma_2$ and a surface $(1-\gamma_1)(1-\gamma_2) = |\langle\phi_1^{(\text{C})}|\phi_2^{(\text{C})}\rangle|^2$. When this tangential point is substituted into Eq. (15), Eq. (15) becomes the following optimization problem:

$$
\begin{aligned}
\text{maximize} \quad & P_s^{(\text{B,C,D})} = q_1\alpha_1\beta_1 + q_2\alpha_2\beta_2 - 2|\langle\psi_1|\psi_2\rangle|\sqrt{\frac{q_1q_2\alpha_1\alpha_2\beta_1\beta_2}{(1-\alpha_1)(1-\alpha_2)(1-\beta_1)(1-\beta_2)}}\\
\text{subject to} \quad & (1-\alpha_1)(1-\alpha_2) > |\langle\psi_1|\psi_2\rangle|^2\\
& \beta_2 \le \frac{\beta_1(1-\beta_1)}{\beta_1(1-\beta_1) + \mathcal{X}(\alpha_1, \alpha_2)}, \ \mathcal{X}(\alpha_1, \alpha_2) = \frac{q_2\alpha_2}{q_1\alpha_1}\frac{|\langle\psi_1|\psi_2\rangle|^2}{(1-\alpha_1)(1-\alpha_2)},\\
& \beta_1 \le \frac{\beta_2(1-\beta_2)}{\beta_2(1-\beta_2) + \mathcal{Y}(\alpha_1, \alpha_2)}, \ \mathcal{Y}(\alpha_1, \alpha_2) = \frac{q_1\alpha_1}{q_2\alpha_2}\frac{|\langle\psi_1|\psi_2\rangle|^2}{(1-\alpha_1)(1-\alpha_2)}.
\end{aligned}
\tag{16}
$$

The detailed derivation of Eq. (16) can be found in the Methods section. Because this optimization problem is difficult to solve analytically, one may apply a numerical method to solve it. Therefore, for the numerical method, a penalty function may be used to solve this constrained optimization problem[49].

To search for the optimal condition of $(\alpha_1, \alpha_2, \beta_1, \beta_2)$, we need to find the condition where the derivative $\partial P_s^{(\text{B,C,D})}/\partial\beta_i$ becomes zero. The condition that (β_1, β_2) satisfies the zero derivative is given as

$$
\beta_2 = \frac{\beta_1(1-\beta_1)^3}{\beta_1(1-\beta_1)^3 + \mathcal{X}(\alpha_1, \alpha_2)}, \ \beta_1 = \frac{\beta_2(1-\beta_2)^3}{\beta_2(1-\beta_2)^3 + \mathcal{Y}(\alpha_1, \alpha_2)}.
\tag{17}
$$

In general, it is difficult to find (β_1, β_2) that satisfies Eq. (17). When $q_1 = q_2$ and $\alpha_1 = \alpha_2 = \alpha$, (β_1, β_2) is analytically expressed as

$$
\beta_1 = \beta_2 = 1 - \sqrt{\frac{|\langle\psi_1|\psi_2\rangle|}{1-\alpha}} = \beta.
\tag{18}
$$

Because $\alpha_1 = \alpha_2$ and $\beta_1 = \beta_2$, $\gamma_1 = \gamma_2$ also holds (see the Methods section). This condition is equal to that obtained by Bergou *et al.*[27] In this case, the objective function of Eq. (16) is expressed as

$$
\begin{aligned}
P_s^{(\text{B,C,D})} &= \alpha\beta - |\langle\psi_1|\psi_2\rangle|\frac{\alpha\beta}{(1-\alpha)(1-\beta)}\\
&= \alpha\left\{1 - \sqrt{\frac{|\langle\psi_1|\psi_2\rangle|}{1-\alpha}}\right\}^2.
\end{aligned}
\tag{19}
$$

We can easily check that Eq. (19) is maximized when $\alpha = 1 - s^{1/3}$ holds. In that case, an optimal success probability can be analytically described as $P_s^{(\text{B,C,D}),\text{opt}} = (1-s^{1/3})^3$. This success probability is equal to the result of Bergou *et al.*[27] However, this success probability is not optimal in general. That is because the equality condition $(\partial/\partial\beta_1, \partial/\partial\beta_2)P_s^{(\text{B,C,D})} = 0$ does not guarantee optimum. Furthermore, we cannot confirm that the optimal condition satisfies the additional constraints $\alpha_1 = \alpha_2$ and $\beta_1 = \beta_2$. Therefore, we should check whether the maximum of Eq. (19) is really equal to that of Eq. (16). We plot the maxima of both Eqs. (16) and (19) in Fig. 2. In the Fig. 2, the solid black

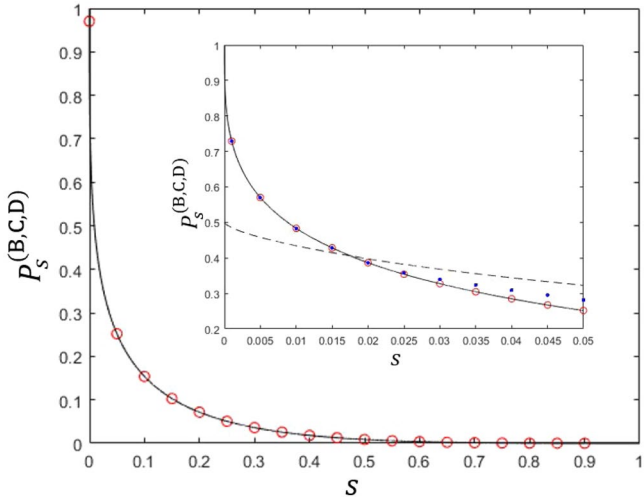


Figure 2. The success probability of generalized sequential state discrimination when Bob, Charlie, and David participate as receivers. Here, $s = |\langle\psi_1|\psi_2\rangle|$ denotes the overlap between two quantum states, and we use the identical prior probability ($q_1 = q_2$). The small graph shows the optimal success probability in the region of $0 < s < 0.05$. The solid black line shows the optimal success probability when three receivers discriminate every two pure state of Alice's[27]. The black dashed line as Eq. (21) shows the optimal success probability when three receivers discriminate only one of two pure states of Alice's (Eq. (21) is a generalization of the result of Pang *et al.*[28]). The red circles and the blue dots display the optimal success probability from Eq. (16). More specifically, the red circles (the blue dots) shows the optimal success probability when the constraint conditions of $\alpha_1 = \alpha_2$ and $\beta_1 = \beta_2$ are (are not) added to Eq. (16). If $s \leq 0.017559$, the red circles and the blue dots coincide with the solid black line, which shows that our result agrees with that of Bergou *et al.*[27]. Further, the blue dots are larger than the solid black line, but are smaller than the black dashed line. Therefore, if $s > 0.017559$, the optimal condition of generalized sequential state discrimination does not include the constraint conditions of $\alpha_1 = \alpha_2$ and $\beta_1 = \beta_2$.

line shows the maximum of Eq. (19). The red circles (blue dots) shows the maximum of Eq. (16) with (without) the additional constraint $\alpha_1 = \alpha_2$ and $\beta_1 = \beta_2$. If the overlap $|\langle\psi_1|\psi_2\rangle|$ becomes smaller, the maxima of both Eqs. (16) and (19) become to coincide with. When the overlap is small, the optimal strategy of every receiver is to discriminate two pure states of Alice. Because the prior probabilities of two pure states are identical, the optimal measurement of every receiver does not show any bias to a specific pure state. Therefore, the condition of $\alpha_1 = \alpha_2$, $\beta_1 = \beta_2$, $\gamma_1 = \gamma_2$ should be included in the optimality conditions. If the overlap $|\langle\psi_1|\psi_2\rangle|$ becomes larger, the maximum of Eq. (16) becomes larger than that of Eq. (19). In this case, $\alpha_1 = \alpha_2$, $\beta_1 = \beta_2$, and $\gamma_1 = \gamma_2$ are not optimal conditions anymore for the generalized sequential state discrimination. Especially, we observe that at least one of γ_1 and γ_2 becomes zero. This means that it is an optimal strategy when Bob, Charlie, and David discriminate one of Alice's two pure states.

If Bob, Charlie, and David only discriminate one of Alice's pure state, the generalized sequential state discrimination can be expressed as the following optimization problem:

$$\text{maximize } P_s^{(B,C,D)} = q_i\alpha_i\beta_i\left\{1 - \frac{|\langle\phi_1^{(B)}|\phi_2^{(B)}\rangle|^2}{1-\beta_i}\right\}. \tag{20}$$

From the equality $\partial P_s^{(B,C,D)}/\partial\beta_i = 0$, we obtain $\beta_i = 1 - |\langle\psi_1|\psi_2\rangle|/\sqrt{(1-\alpha_1)(1-\alpha_2)}$. Substituting it into Eq. (20), we derive

$$\begin{aligned} P_s^{(B,C,D)} &= q_i\alpha_i\left\{1 - \frac{|\langle\psi_1|\psi_2\rangle|}{\sqrt{(1-\alpha_1)(1-\alpha_2)}}\right\}^2 \\ &\leq q_i\alpha_i\left\{1 - \frac{|\langle\psi_1|\psi_2\rangle|}{\sqrt{1-\alpha_i}}\right\}^2 \\ &\leq q_i(1-s^{2/3})^3. \end{aligned} \tag{21}$$

The first inequality of Eq. (21) becomes equality at $\alpha_j = 0 (j \neq i)$. The second inequality becomes equality when $\alpha_i = 1 - |\langle\psi_1|\psi_2\rangle|^{2/3}$ holds. Therefore, the optimal success probability is given as $P_s^{(B,C,D),opt} = \max\{q_1, q_2\}(1 - |\langle\psi_1|\psi_2\rangle|^{2/3})^3$, as shown in Fig. 2. In case of $q_1 = q_2$, when $|\langle\psi_1|\psi_2\rangle| < (2^{1/3} - 1)^3 \simeq 0.0175599$ is satisfied, it is optimal for the three receivers to discriminate two of Alice's pure states. However, if $|\langle\psi_1|\psi_2\rangle| \geq (2^{1/3} - 1)^3 \simeq 0.0175599$ is fulfilled, discriminating only one of Alice's pure state is optimal.

Next, we consider the case of $N = 4$. In this case, let us denote the four receivers as Bob, Charlie, David, and Eliot. Each POVM of the four receivers corresponds to the two dimensional real vectors (α_1, α_2), (β_1, β_2), (γ_1, γ_2), and (δ_1, δ_2). According to Eq. (12), each real vector should satisfy

$$(\alpha_1, \alpha_2) \in C_{\rm int}^{(\rm B)},\ (\beta_1, \beta_2) \in C_{\rm int}^{(\rm C)},\ (\gamma_1, \gamma_2) \in C_{\rm int}^{(\rm D)},\ (\delta_1, \delta_2) \in \partial C^{(\rm E)}. \tag{22}$$

Here, $C_{\rm int}^{(\rm E)}$ and $\partial C^{(\rm E)}$ are respectively defined as

$$\begin{aligned} C_{\rm int}^{(\rm E)} &= \{(\delta_1, \delta_2) \in \mathbb{R}^2 | (1-\delta_1)(1-\delta_2) > |\langle \phi_1^{(\rm D)} | \phi_2^{(\rm D)} \rangle|^2\}, \\ \partial C^{(\rm E)} &= \{(\delta_1, \delta_2) \in \mathbb{R}^2 | (1-\delta_1)(1-\delta_2) = |\langle \phi_1^{(\rm D)} | \phi_2^{(\rm D)} \rangle|^2\}. \end{aligned}$$

Moreover, the POVM condition for Eliot is expressed as $C^{(\rm E)} = C_{\rm int}^{(\rm E)} \cup \partial C^{(\rm E)}$. Hence, we can obtain the following optimization problem:

$$\begin{aligned} \text{maximize} \quad & P_s^{(\rm B,C,D)} = q_1\alpha_1\beta_1\gamma_1\delta_1 + q_2\alpha_2\beta_2\gamma_2\delta_2 \\ \text{subject to} \quad & (1-\alpha_1)(1-\alpha_2) > |\langle \psi_1 | \psi_2 \rangle|^2, \\ & (1-\beta_1)(1-\beta_2) > |\langle \phi_1^{(\rm B)} | \phi_2^{(\rm B)} \rangle|^2, \\ & (1-\gamma_1)(1-\gamma_2) > |\langle \phi_1^{(\rm C)} | \phi_2^{(\rm C)} \rangle|^2, \\ & (1-\delta_1)(1-\delta_2) = |\langle \phi_1^{(\rm D)} | \phi_2^{(\rm D)} \rangle|^2. \end{aligned} \tag{23}$$

Now, let us consider the equality constraint of Eq. (23). The optimal condition of the generalized sequential state discrimination for Eliot is given as a tangential point (δ_1, δ_2) between a plane $P_s^{(\rm B,C,D,E)} = (q_1\alpha_1\beta_1\gamma_1)\delta_1 + (q_2\alpha_2\beta_2\gamma_2)\delta_2$ and a surface $(1-\delta_1)(1-\delta_2) = |\langle \phi_1^{(\rm D)} | \phi_2^{(\rm D)} \rangle|^2$. If this tangential point is substituted into the objective function of Eq. (23), the following optimization problem can be obtained:

$$\begin{aligned} \text{maximize} \quad & P_s^{(\rm B,C,D,E)} = q_1\alpha_1\beta_1\gamma_1 + q_2\alpha_2\beta_2\gamma_2 - 2|\langle \psi_1 | \psi_2 \rangle| \sqrt{\frac{q_1q_2\alpha_1\alpha_2\beta_1\beta_2\gamma_1\gamma_2}{(1-\alpha_1)(1-\alpha_2)(1-\beta_1)(1-\beta_2)(1-\gamma_1)(1-\gamma_2)}} \\ \text{subject to} \quad & (1-\alpha_1)(1-\alpha_2) > |\langle \psi_1 | \psi_2 \rangle|^2 \\ & (1-\alpha_1)(1-\alpha_2)(1-\beta_1)(1-\beta_2) > |\langle \psi_1 | \psi_2 \rangle|^2 \\ & \gamma_2 \le \frac{\gamma_1(1-\gamma_1)}{\gamma_1(1-\gamma_1) + \mathcal{X}(\alpha_1, \alpha_2, \beta_1, \beta_2)\gamma_1}, \ \mathcal{X}(\alpha_1, \alpha_2, \beta_1, \beta_2) = \frac{q_2\alpha_2\beta_2}{q_1\alpha_1\beta_1} \frac{|\langle \psi_1 | \psi_2 \rangle|^2}{(1-\alpha_1)(1-\alpha_2)(1-\beta_1)(1-\beta_2)} \\ & \gamma_1 \le \frac{\gamma_2(1-\gamma_2)}{\gamma_2(1-\gamma_2) + \mathcal{Y}(\alpha_1, \alpha_2, \beta_1, \beta_2)\gamma_2}, \ \mathcal{Y}(\alpha_1, \alpha_2, \beta_1, \beta_2) = \frac{q_1\alpha_1\beta_1}{q_2\alpha_2\beta_2} \frac{|\langle \psi_1 | \psi_2 \rangle|^2}{(1-\alpha_1)(1-\alpha_2)(1-\beta_1)(1-\beta_2)} \end{aligned} \tag{24}$$

The detailed derivation of Eq. (24) is provided in the Methods section. When the constraints $\alpha_1 = \alpha_2$, $\beta_1 = \beta_2$, $\gamma_1 = \gamma_2$, and $\delta_1 = \delta_2$ are added, this optimization problem is difficult to solve analytically. Thus we solve this problem numerically. We show the maximum of Eq. (24) in Fig. 3. When the constraints $\alpha_1 = \alpha_2$, $\beta_1 = \beta_2$, $\gamma_1 = \gamma_2$, and $\delta_1 = \delta_2$ are added to Eq. (24), the optimal success probability becomes equal to the result by Bergou *et al.*[27] If the overlap is small, this equality constraint is included in the optimal condition of sequential state discrimination. Because the prior probabilities of two pure states are identical, the optimal measurement of every receiver does not show any bias to a specific pure state. If we do not add these constraints, the optimal success probability becomes larger than that provided by Bergou *et al.*[27]. In this case, we observe that at least one of δ_1 and δ_2 becomes zero. This implies that it is optimal only when four receivers discriminate only one out of two pure states of Alice.

If Bob, Charlie, David, and Eliot only discriminate one out of two pure states, the generalized sequential state discrimination is described as the following optimization problem:

$$\text{maximize } P_s^{(\rm B,C,D,E)} = q_i\alpha_i\beta_i \left\{ 1 - \frac{|\langle \phi_1^{(\rm B)} | \phi_2^{(\rm B)} \rangle|}{\sqrt{(1-\beta_1)(1-\beta_2)}} \right\}^2. \tag{25}$$

The success probability satisfies the following inequalities:

$$\begin{aligned} P_s^{(\rm B,C,D,E)} &\le q_i\alpha_i\beta_i \left\{ 1 - \frac{|\langle \phi_1^{(\rm B)} | \phi_2^{(\rm B)} \rangle|}{\sqrt{1-\beta_i}} \right\}^2 \\ &\le q_i\alpha_i(1 - |\langle \phi_1^{(\rm B)} | \phi_2^{(\rm B)} \rangle|^{2/3})^3 \\ &= q_i\alpha_i \left\{ 1 - \left(\frac{|\langle \psi_1 | \psi_2 \rangle|}{\sqrt{(1-\alpha_1)(1-\alpha_2)}} \right)^{2/3} \right\}^3 \\ &\le q_i\alpha_i \left\{ 1 - \left(\frac{|\langle \psi_1 | \psi_2 \rangle|}{\sqrt{1-\alpha_i}} \right)^{2/3} \right\}^3 \\ &\le q_i(1 - \sqrt{|\langle \psi_1 | \psi_2 \rangle|})^4 \end{aligned} \tag{26}$$

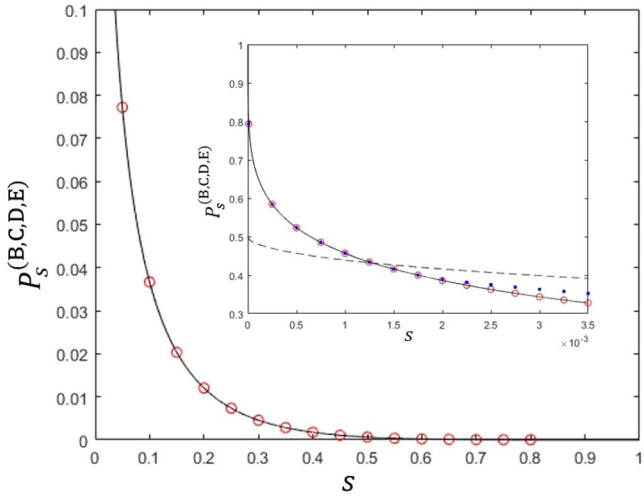


Figure 3. The success probability of generalized sequential state discrimination when Bob, Charlie, David, and Eliot participate as receivers. Here, $s = |\langle\psi_1|\psi_2\rangle|$ denotes the overlap between two quantum states, and we use the identical prior probability ($q_1 = q_2$). The small graph shows the optimal success probability in the region of $0 < s < 0.0035$. The solid black line shows the optimal success probability when four receivers discriminate every two pure state of Alice's[27]. The black dashed line as Eq. (26) shows the optimal success probability when four receivers discriminate only one of two pure states of Alice's (Eq. (26) is a generalization of the result of Pang *et al.*[28]). The red circles and the blue dots display the optimal success probability from Eq. (24). More specifically, the red circles (the blue dots) shows the optimal success probability when the constraint conditions of $\alpha_1 = \alpha_2$, $\beta_1 = \beta_2$, and $\gamma_1 = \gamma_2$ are (are not) added to Eq. (16). If $s \leq 0.001282$, the red circles and the blue dots coincide with the solid black line, which shows that our result agrees with that of Bergou *et al.*[27]. Further, the blue dots are larger than the solid black line, but are smaller than the black dashed line. Therefore, if $s > 0.001282$, the optimal condition of generalized sequential state discrimination does not include the constraint conditions of $\alpha_1 = \alpha_2, \beta_1 = \beta_2$, and $\gamma_1 = \gamma_2$.

In Eq. (26), the first inequality becomes equality at $\beta_j = 0 (j \neq i)$. Likewise, the third inequality becomes equality at $\alpha_j = 0 (j \neq i)$. The second and fourth inequality become zero when the partial derivatives $\partial P_s^{(B,C,D,E)}/\partial\alpha_i$ and $\partial P_s^{(B,C,D,E)}/\partial\beta_i$ become zero. Therefore, the maximum of Eq. (25) becomes $P_s^{(B,C,D,E),opt} = \max\{q_1, q_2\}(1 - \sqrt{|\langle\psi_1|\psi_2\rangle|})$. When $q_1 = q_2$, if $|\langle\psi_1|\psi_2\rangle| < (2^{1/4} - 1)^4 \simeq 0.00128159$, it is optimal for the four receivers to discriminate every two pure state of Alice. If $|\langle\psi_1|\psi_2\rangle| \geq (2^{1/4} - 1)^4 \simeq 0.00128159$, it is optimal for the four receivers to discriminate only one out of two pure states.

From the previous results, we can consider the generalized sequential state discrimination for arbitrary N, in an inductive manner. We can construct an optimization problem of the generalized sequential state discrimination for any N as follows:

$$
\begin{aligned}
\text{maximize} \quad & P_s^{(B_1,\ldots,B_N)} = q_1 \prod_{I=1}^{N-1} \alpha_1^{(I)} + q_2 \prod_{I=1}^{N-1} \alpha_2^{(I)} - 2|\langle\psi_1|\psi_2\rangle| \\
& \sqrt{q_1 q_2} \prod_{I=1}^{N-1} \sqrt{\frac{\alpha_1^{(I)}\alpha_2^{(I)}}{(1-\alpha_1^{(I)})(1-\alpha_2^{(I)})}} \\
\text{subject to} \quad & \prod_{I=1}^{J} (1-\alpha_1^{(I)})(1-\alpha_2^{(I)}) > |\langle\psi_1|\psi_2\rangle|^2 \quad \forall J \in \{1, \ldots, N-2\} \\
& \alpha_2^{(N-1)} \leq \frac{\alpha_1^{(N-1)}(1-\alpha_1^{(N-1)})}{\alpha_1^{(N-1)}(1-\alpha_1^{(N-1)}) + \mathcal{X}(\vec{\alpha}, \vec{\beta})}, \quad \mathcal{X}(\vec{\alpha}, \vec{\beta}) \\
& \qquad = \frac{q_2}{q_1}\left(\prod_{I=1}^{N-1} \frac{\alpha_2^{(I)}}{\alpha_1^{(I)}}\right) \frac{|\langle\psi_1|\psi_2\rangle|^2}{\prod_{I'=1}^{N-1}(1-\alpha_1^{(I')})(1-\alpha_2^{(I')})} \\
& \alpha_1^{(N-1)} \leq \frac{\alpha_2^{(N-1)}(1-\alpha_2^{(N-1)})}{\alpha_2^{(N-1)}(1-\alpha_2^{(N-1)}) + \mathcal{Y}(\vec{\alpha}, \vec{\beta})}. \quad \mathcal{Y}(\vec{\alpha}, \vec{\beta}) \\
& \qquad = \frac{q_1}{q_2}\left(\prod_{I=1}^{N-1} \frac{\alpha_1^{(I)}}{\alpha_2^{(I)}}\right) \frac{|\langle\psi_1|\psi_2\rangle|^2}{\prod_{I'=1}^{N-1}(1-\alpha_1^{(I')})(1-\alpha_2^{(I')})}
\end{aligned}
\tag{27}
$$

where $\overrightarrow{\alpha} = (\alpha_1^{(1)}, \alpha_2^{(1)}, \cdots, \alpha_1^{(N)}, \alpha_2^{(N)})$ and $\overrightarrow{\beta} = (\beta_1^{(1)}, \beta_2^{(1)}, \cdots, \beta_1^{(N)}, \beta_2^{(N)})$. If prior probabilities are all equal, the optimal success probability is obtained as

$$\begin{aligned} P_s^{(B_1,\ldots,B_N),\mathrm{opt}} &= (1 - |\langle\psi_1|\psi_2\rangle|^{1/N})^N, \ |\langle\psi_1|\psi_2\rangle| < S(N) \\ P_s^{(B_1,\ldots,B_N),\mathrm{opt}} &= \frac{1}{2}(1 - |\langle\psi_1|\psi_2\rangle|^{2/N})^N. \ |\langle\psi_1|\psi_2\rangle| \geq S(N) \end{aligned} \tag{28}$$

where $S(N) = (2^{1/N} - 1)^N$. Equation (28) satisfies the result of Bergou[27] and Pang[28]. If $|\langle\psi_1|\psi_2\rangle| < S(N)$, the optimal condition contains $\alpha_1^{(I)} = \alpha_2^{(I)}(\ \forall\ I)$. This property was argued by Bergou *et al.*[27] When $N \in \{2, 3, \ldots, 7\}$, the value of $S(N)$ is numerically given as

$$\begin{aligned} S(2) &= 0.171572875253810 \\ S(3) &= 0.017559993780021 \\ S(4) &= 0.001281592197970 \\ S(5) &= 7.269939897187259 \times 10^{-5} \\ S(6) &= 3.372943879071272 \times 10^{-6} \\ S(7) &= 1.323880715612381 \times 10^{-7} \end{aligned}$$

When N becomes larger, $S(N)$ rapidly converges to zero. This implies that when the overlap between two pure states is not small enough, discriminating two pure states when many receivers participate is not a good strategy. Therefore, sequential state discrimination can be applicable for multiparty QKD in the case of a suitable number of receivers. That is because, in multiparty QKD, all receivers are required to discriminate every quantum state[24,27].

Generalized sequential state discrimination of two mixed states. Here, let us consider the generalized sequential state discrimination of two mixed states. For convenience, we will consider rank-2 mixed states such as

$$\begin{aligned} \rho_1 &= r_1|r_1\rangle\langle r_1| \oplus \bar{r}_1|\bar{r}_1\rangle\langle\bar{r}_1|, \\ \rho_2 &= r_2|r_2\rangle\langle r_2| \oplus \bar{r}_2|\bar{r}_2\rangle\langle\bar{r}_2|. \end{aligned} \tag{29}$$

Equation (29) has the same form as that of Eq. (6). Like in Eq. (6), every POVM corresponds to a real vector $(\alpha_1^{(I)}, \alpha_2^{(I)}, \bar{\alpha}_1^{(I)}, \bar{\alpha}_2^{(I)})$. We can describe the generalized sequential state discrimination of two mixed states as the following optimization problem[33]:

$$\begin{aligned} \text{maximize} \quad & P_s^{(B_1,\ldots,B_N)} = q_1\left(r_1\prod_{I=1}^{N}\alpha_1^{(I)} + \bar{r}_1\prod_{I=1}^{N}\bar{\alpha}_1^{(I)}\right) + q_2\left(r_2\prod_{I=1}^{N}\alpha_2^{(I)} + \bar{r}_2\prod_{I=1}^{N}\bar{\alpha}_2^{(I)}\right) \\ \text{subject to} \quad & (1-\alpha_1^{(1)})(1-\alpha_2^{(1)}) > |\langle r_1|r_2\rangle|^2, \ (1-\bar{\alpha}_1^{(1)})(1-\bar{\alpha}_2^{(1)}) > |\langle\bar{r}_1|\bar{r}_2\rangle|^2 \\ & (1-\alpha_1^{(I+1)})(1-\alpha_2^{(I+1)}) \\ & \quad > |\langle s_1^{(I)}|s_2^{(I)}\rangle|^2, \ (1-\bar{\alpha}_1^{(I+1)})(1-\bar{\alpha}_2^{(I+1)}) \\ & \quad > |\langle\bar{s}_1^{(I)}|\bar{s}_2^{(I)}\rangle|^2, \ \forall\ I \in \{1, N-2\}(1-\alpha_1^{(N)})(1-\alpha_2^{(N)}) \\ & = |\langle s_1^{(N-1)}|s_2^{(N-1)}\rangle|^2, \ (1-\bar{\alpha}_1^{(N)})(1-\bar{\alpha}_2^{(N)}) = |\langle\bar{s}_1^{(N-1)}|\bar{s}_2^{(N-1)}\rangle|^2 \end{aligned} \tag{30}$$

Then, Eq. (30) can be divided into the following two optimization problems:

$$\begin{aligned} \text{maximize} \quad & p_s = q_1 r_1\prod_{I=1}^{N}\alpha_1^{(I)} + q_2 r_2\prod_{I=1}^{N}\alpha_2^{(I)} \\ \text{subject to} \quad & (1-\alpha_1^{(1)})(1-\alpha_2^{(1)}) > |\langle r_1|r_2\rangle|^2 \\ & (1-\alpha_1^{(I+1)})(1-\alpha_2^{(I+1)}) > |\langle s_1^{(I)}|s_2^{(I)}\rangle|^2, \ \forall I \in \{1, \ldots, N-2\} \\ & (1-\alpha_1^{(N)})(1-\alpha_2^{(N)}) = |\langle s_1^{(N-1)}|s_2^{(N-1)}\rangle|^2. \end{aligned}$$

$$\begin{aligned} \text{maximize} \quad & \bar{p}_s = q_1\bar{r}_1\prod_{I=1}^{N}\bar{\alpha}_1^{(I)} + q_2\bar{r}_2\prod_{I=1}^{N}\bar{\alpha}_2^{(I)} \\ \text{subject to} \quad & (1-\bar{\alpha}_1^{(1)})(1-\bar{\alpha}_2^{(1)}) > |\langle\bar{r}_1|\bar{r}_2\rangle|^2 \\ & (1-\bar{\alpha}_1^{(I+1)})(1-\bar{\alpha}_2^{(I+1)}) > |\langle\bar{s}_1^{(I)}|\bar{s}_2^{(I)}\rangle|^2, \ \forall I \in \{1, \ldots, N-2\} \\ & (1-\bar{\alpha}_1^{(N)})(1-\bar{\alpha}_2^{(N)}) = |\langle\bar{s}_1^{(N-1)}|\bar{s}_2^{(N-1)}\rangle|^2. \end{aligned}$$

That is, the maximum of Eq. (30) becomes $\max P_s^{(B_1,\ldots,B_N),\mathrm{opt}} = \max p_s + \max\bar{p}_s$. Although we consider rank-2 mixed states as Eq. (29), we can generalize this argument to any mixed states, with an arbitrary rank. If $q_1 = q_2$, $r_1 = r_2 = r$, and $\bar{r}_1 = \bar{r}_2 = \bar{r}$ are assumed, then the optimal success probability can be found as[33]

$$
\begin{aligned}
\max P_s^{(B_1,\cdots,B_N)} &= r(1-|\langle r_1|r_2\rangle|^{1/N})^N && |\langle r_1|r_2\rangle| < S(N) \wedge |\langle \bar{r}_1|\bar{r}_2\rangle| < S(N)\\
&\quad + \bar{r}(1-|\langle \bar{r}_1|\bar{r}_2\rangle|^{1/N})^N,\\
\max P_s^{(B_1,\ldots,B_N)} &= r(1-|\langle r_1|r_2\rangle|^{1/N})^N && |\langle r_1|r_2\rangle| < S(N) \wedge |\langle \bar{r}_1|\bar{r}_2\rangle| \geq S(N)\\
&\quad + \bar{r}\frac{1}{2}(1-|\langle \bar{r}_1|\bar{r}_2\rangle|^{2/N})^N,\\
\max P_s^{(B_1,\ldots,B_N)} &= r\frac{1}{2}(1-|\langle r_1|r_2\rangle|^{2/N})^N && |\langle r_1|r_2\rangle| \geq \bar{S}(N) \wedge |\langle \bar{r}_1|\bar{r}_2\rangle| < S(N)\\
&\quad + \bar{r}(1-|\langle \bar{r}_1|\bar{r}_2\rangle|^{1/N})^N,\\
\max P_s^{(B_1,\ldots,B_N)} &= r\frac{1}{2}(1-|\langle r_1|r_2\rangle|^{2/N})^N && |\langle r_1|r_2\rangle| \geq S(N) \wedge |\langle \bar{r}_1|\bar{r}_2\rangle| \geq S(N)\\
&\quad + \bar{r}\frac{1}{2}(1-|\langle \bar{r}_1|\bar{r}_2\rangle|^{2/N})^N.
\end{aligned}
$$

For either $q_1 \neq q_2$ or $r_1 \neq r_2 (\bar{r}_1 = \bar{r}_2)$, when $|\langle r_1|r_2\rangle| < S(N) (|\langle \bar{r}_1|\bar{r}_2\rangle| < S(N))$, $\max p_s (\max \bar{p}_s)$ is difficult to obtain analytically. Therefore, one may evaluate $\max p_s (\max \bar{p}_s)$ numerically. However, when $|\langle r_1|r_2\rangle| \geq \bar{S}(N) (|\langle \bar{r}_1|\bar{r}_2\rangle| \geq S(N))$, one can obtain $\max p_s = \max\{q_1 r_1, q_2 r_2\}(1-|\langle r_1|r_2\rangle|^{2/N})^N (\max \bar{p}_s = \max\{q_1 \bar{r}_1, q_2 \bar{r}_2\}(1-|\langle \bar{r}_1|\bar{r}_2\rangle|^{2/N})^N)$.

If $|\langle r_1|r_2\rangle| \geq S(N)$ and $|\langle \bar{r}_1|\bar{r}_2\rangle| \geq S(N)$, it is optimal that every receiver discriminates Alice's two pure state. However, If $|\langle r_1|r_2\rangle| < S(N)$ or $|\langle \bar{r}_1|\bar{r}_2\rangle| < S(N)$, discriminating only one out of Alice's two pure states is optimal.

Comparison with other discrimination strategies. There are other strategies for multi-party QKD, besides sequential state discrimination. The first one is the quantum reproducing strategy[27]. This strategy is performed as in the following procedure (see Fig. 4): Bob 1 optimally discriminates Alice's quantum states, without any error. If Bob 1 obtains a conclusive result, he can reproduce the same quantum state, which corresponds to his conclusive result. Then, Bob 1 sends the quantum state to Bob 2. This procedure is recursively performed from Bob 2 to Bob N. If Bob I obtains an inconclusive result, he tells every receiver, through classical communication, that he failed to discriminate the quantum state of Alice. The success probability of the quantum reproducing strategy is expressed as

$$
\begin{aligned}
P_{s,rep}^{(B_1,\ldots,B_N)} &= q_1 \mathrm{Pr}_{B_1}[1|\rho_1]\mathrm{Pr}_{B_2}[1|\rho_1] \times \cdots \times \mathrm{Pr}_{B_N}[1|\rho_1]\\
&\quad + q_2 \mathrm{Pr}_{B_1}[2|\rho_2]\mathrm{Pr}_{B_2}[2|\rho_2] \times \cdots \times \mathrm{Pr}_{B_N}[2|\rho_2].
\end{aligned}
$$

Here, let us consider the case of S_2. Then, $\mathrm{Pr}_{B_I}[i|\rho_i] = \mathrm{Tr}[\rho_i M_i^{(I)}]$ is the probability that Bob I obtains the measurement outcome i. If we assume an equal prior probability, when mixed states have the same eigenvalues, the optimal success probability of the quantum reproducing strategy is derived as (see Method)[21]

$$
P_{rep.}^{(B_1,\ldots,B_N),\mathrm{opt}} = (1 - rs - \bar{r}\bar{s})^N.
$$

Here, $r_1 = r_2 = r$ and $\bar{r}_1 = \bar{r}_2 = \bar{r}$. s and $\bar{s}$ are defined as $s = |\langle r_1|r_2\rangle|$ and $\bar{s} = |\langle \bar{r}_1|\bar{r}_2\rangle|$, respectively.

The second case is the quantum broadcasting strategy[27,32]. This strategy is performed as in the following process (see Fig. 5): Bob 1 puts Alice's unknown quantum states into a quantum broadcasting machine, which transforms ρ_i into an $N-$partite state $\sigma_i^{(B_1,\ldots,B_N)}$, with a probability of less than 1[39]. Here, these states satisfy $\mathrm{Tr}_{B_1,\ldots,B_{I-1},B_{I+1},\ldots,B_N}[\sigma_i^{(B_1,\ldots,B_N)}] = \rho_i (\forall I)$. If Bob 1 succeeds in quantum broadcasting, Then, Bob 1, Bob 2,$\cdots$, and Bob N can share $\sigma_i^{(B_1,\ldots,B_N)}$. Then, every receiver discriminates his partial state ρ_i, without any error. If Bob 1 fails, however, he tells everyone, through classical communication, that quantum broadcasting has failed. The optimal success probability of quantum broadcasting is expressed as

$$
\begin{aligned}
P_{s,broad}^{(B_1,\ldots,B_N)} &= q_1 \mathrm{Pr}_{broad}[\rho_1]\mathrm{Pr}_{B_1}[1|\rho_1]\mathrm{Pr}_{B_2}[1|\rho_1] \times \cdots \times \mathrm{Pr}_{B_N}[1|\rho_1]\\
&\quad + q_2 \mathrm{Pr}_{broad}[\rho_2]\mathrm{Pr}_{B_1}[2|\rho_2]\mathrm{Pr}_{B_2}[2|\rho_2] \times \cdots \times \mathrm{Pr}_{B_N}[2|\rho_2]
\end{aligned}
$$

Here, $\mathrm{Pr}_{broad}[\rho_i]$ is the maximal success probability to succeed in broadcasting when ρ_i is given. The optimal success probability of the quantum broadcasting strategy is larger than that of the quantum reproducing strategy. In Fig. 5, quantum broadcasting strategies for three receivers (Bob, Charlie, and David) and four receivers (Bob, Charlie, David, and Eliot) are described. In these cases, the optimal success probabilities of the quantum broadcast strategy are given by

$$
\begin{aligned}
P_{s,broad}^{(\mathrm{B,C,D}),\mathrm{opt}} &= \min\left\{\frac{1}{1+s}, \frac{1}{1+\bar{s}}\right\}^2 (1 - rs - \bar{r}\bar{s})^3,\\
P_{s,broad}^{(\mathrm{B,C,D,E}),\mathrm{opt}} &= \min\left\{\frac{1}{1+s}, \frac{1}{1+\bar{s}}\right\}^3 (1 - rs - \bar{r}\bar{s})^4.
\end{aligned}
$$

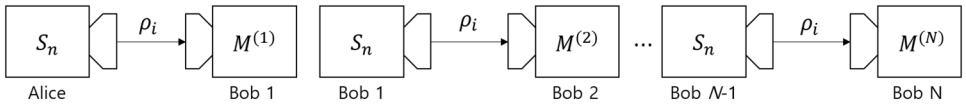


Figure 4. Schematic of the quantum reproducing strategy for Bob 1, Bob 2, ⋯, and Bob $N-1$.

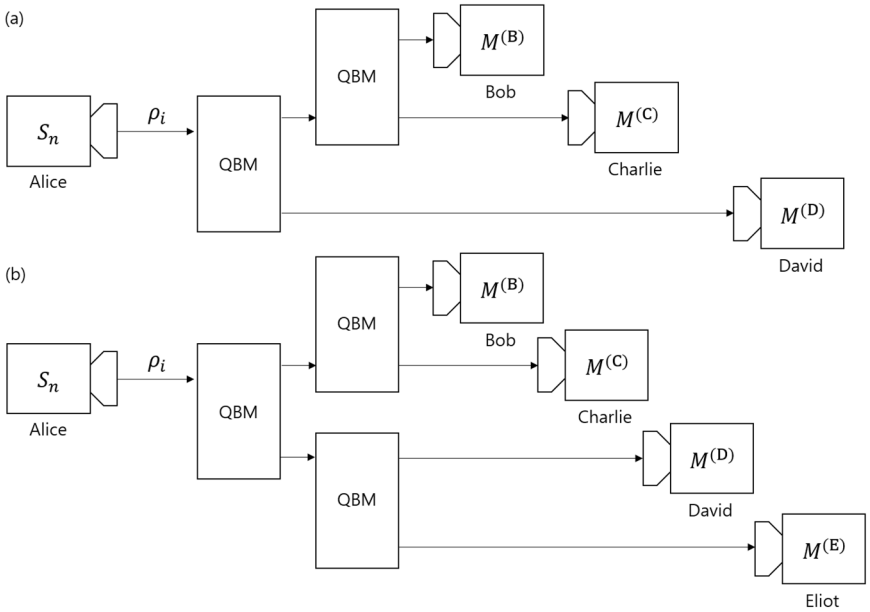


Figure 5. Schematic of the quantum broadcasting strategy. Here, QBM denotes a quantum broadcasting machine[39]. (**a**) consists of Bob, Charlie, and David. (**b**) consists of Bob, Charlie, David, and Eliot.

Here, $\min\left\{\frac{1}{1+s}, \frac{1}{1+\bar{s}}\right\}$ is the optimal probability that once quantum broadcasting succeeds[39]. Because $\Pr_{broad}[\rho_1] = \Pr_{broad}[\rho_2]$, the optimal success probability of quantum broadcasting can be derived, similar to that of quantum reproducing. If Alice prepares one out of two pure states, the optimal success probability of the generalized sequential state discrimination is less than that of quantum reproducing or quantum broadcasting[27]. However, if Alice prepares one out of two mixed states, the optimal success probability of the generalized sequential state discrimination can be larger than that of both the quantum reproducing and the quantum broadcasting strategy. Namely, the generalized sequential state discrimination of mixed states has more potential for application to multiparty QKD than those of the quantum reproducing and quantum broadcasting strategies. It should be noted that sequential state discrimination can be a good candidate for application to multiparty QKD when mixed states are used, in contrast to the result of the pure states obtained by Bergou *et al.*[27].

Example 1. Suppose that Alice prepares one out of two mixed states $\rho_i \in \{\rho_1, \rho_2\}$, with equal prior probabilities. Here, two mixed states are expressed as Eq. (29), where $r = 0.6$, $\bar{r} = 1 - r = 0.4, s = 0.7$, and $\bar{s} = 0.001$. In the case of $N = 3$(Bob,Charlie, and David), the optimal success probability for each strategy is numerically obtained as

$$\begin{aligned}\max P_{seq}^{(\mathrm{B,C,D})} &= 0.294443356418367,\\ \max P_{rep}^{(\mathrm{B,C,D})} &= 0.194708598336000,\\ \max P_{broad}^{(\mathrm{B,C,D})} &= 0.067373217417301.\end{aligned}$$

Here, P_{seq}, P_{rep}, and P_{rep} denote the success probability of generalized sequential state discrimination, quantum reproducing, and quantum broadcasting, respectively. In the case of $N = 4$(Bob, Charlie, David, and Eliot), optimal success probability for each strategy is numerically obtained as

$$\begin{aligned}\max P_{seq}^{(\mathrm{B,C,D,E})} &= 0.182986042905254,\\ \max P_{rep}^{(\mathrm{B,C,D,E})} &= 0.112853103595546,\\ \max P_{broad}^{(\mathrm{B,C,D,E})} &= 0.022970304008863.\end{aligned}$$

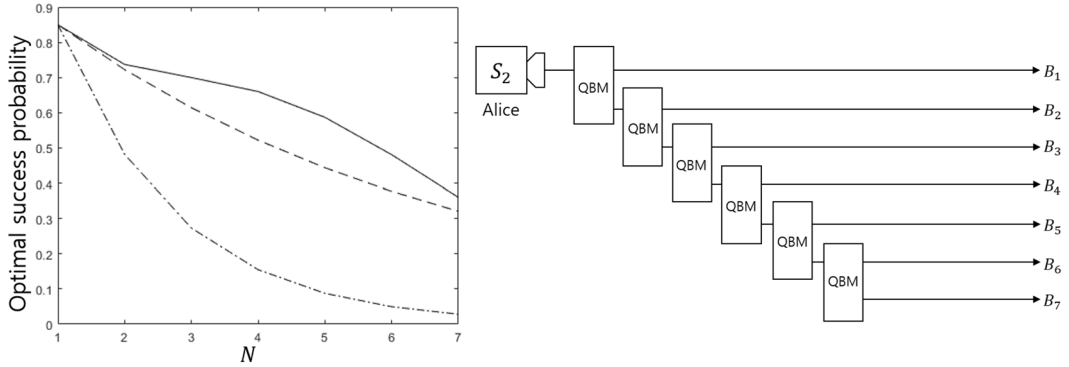


Figure 6. Plot of the optimal success probability of generalized sequential state discrimination (solid black line), quantum reproducing strategy (black dashed line) and quantum broadcasting strategy (dash-dot black line). We also describe a specific way to perform quantum broadcasting strategy.

Therefore, it can be seen that, when two mixed states such as Eq. (29), with $r = 0.6$, $\bar{r} = 0.7$, $s = 0.7$, and $\bar{s} = 0.001$, are used, the optimal success probability of generalized sequential state discrimination performs better than quantum reproducing and quantum broadcasting.

Example 2. Suppose Alice prepares one out of two mixed states $\rho_i \in \{\rho_1, \rho_2\}$, with equal prior probabilities. Here, two mixed states are expressed as Eq. (29), where $r = 0.3$, $\bar{r} = 1 - r = 0.7$, $s = 0.5$, and $\bar{s} = 5 \times 10^{-8}$. We plotted the optimal success probability of generalized sequential state discrimination and quantum reproducing strategy in Fig. 6. As can be seen in the figure, the optimal success probability of generalized sequential state discrimination exceeds those of the quantum reproducing and quantum broadcasting strategies. Here, we describe a specific way to perform the quantum broadcasting strategy, as shown in Fig. 6, when seven receivers participate. When the given quantum states are non-orthogonal, because the success probability of quantum broadcasting cannot achieve to one, generalized sequential state discrimination also outperforms quantum broadcasting strategy. In the extreme case, if $N = 1$, the optimal success probability in Fig. 6 becomes equal to the optimal unambiguous discrimination[21].

In conclusion, the generalized sequential state discrimination of two mixed states can outperform the other two strategies. It can be implemented using linear optics. In the next section, we will describe its implementation in detail.

Optical implementation. Here, we explain the method to implement the generalized sequential state discrimination of two coherent states, using linear optics.

Implementation of the POVM for unambiguous discrimination. Suppose that Alice prepares $|\psi_i\rangle \in \bar{S}_n$, with a prior probability q_i. When an ancilla state $|\mathscr{B}\rangle$ is prepared in Bob, his measurement that performs an unambiguous discrimination can be constructed as

$$U_{\mathrm{AB}}^{(\mathrm{B})}|\psi_i\rangle_A \otimes |\mathscr{B}\rangle_B = \sqrt{\alpha_i}|\phi_i\rangle_A \otimes |\mathscr{B}_i\rangle_B + \sqrt{\bar{\alpha}_i}|\phi_0\rangle_A \otimes |\mathscr{B}_0\rangle_B. \tag{31}$$

Here, $\{|\mathscr{B}_0\rangle, |\mathscr{B}_1\rangle, \ldots, |\mathscr{B}_n\rangle\}$ is an orthonormal basis. Moreover, $\alpha_i(\bar{\alpha}_i)$ is a conditional probability, that Bob obtains conclusive result i(inconclusive result), when Alice prepares ψ_i. It is well known that Eq. (31) is equivalent to Eq. (2), in unambiguous discrimination.Moreover, Eq. (31) shows a way to implement an unambiguous discrimination in real-world settings.

If $\bar{S}_2$ consists of two polarized single photon states $|\psi_i\rangle = a_i|H\rangle + b_i|V\rangle (i = 1, 2)$, a global unitary operator $U_{AB}^{(\mathrm{B})}$ can be implemented using linear optics. Solis-Prosser *et al.*[29] used this method to perform a sequential state discrimination of two polarized single-photon states, with equal prior probability. In their model, an ancilla state in Eq. (31) corresponds to a single-photon path. If their model is applied to generalized sequential state discrimination, Bob I should prepare 3^I paths. Therefore, if the number of receivers is large, generalized sequential state discrimination should require an exponentially large number of single photon paths.

However, the sequential state discrimination of coherent states does not require many paths[34]. One can perform the sequential state discrimination by using the modified Banaszek or the Huttner model. In the next subsection. we will explain the modified Banaszek model)[40,41]. Both models can perform an unambiguous discrimination of two nonorthogonal coherent states, with general prior probabilities. Furthermore, both models can achieve an IDP limit[8–11]. By simply adding beamsplitters in the Banaszek or the Huttner model, one can perform a generalized measurement, that produces post-measurement states[34].

Implementation of the sequential state discrimination of two pure states. In this subsection, we propose a method to implement the generalized sequential state discrimination of two coherent states. In our previous work[34], the sequential state discrimination of two coherent states was discussed in the case of two receivers.

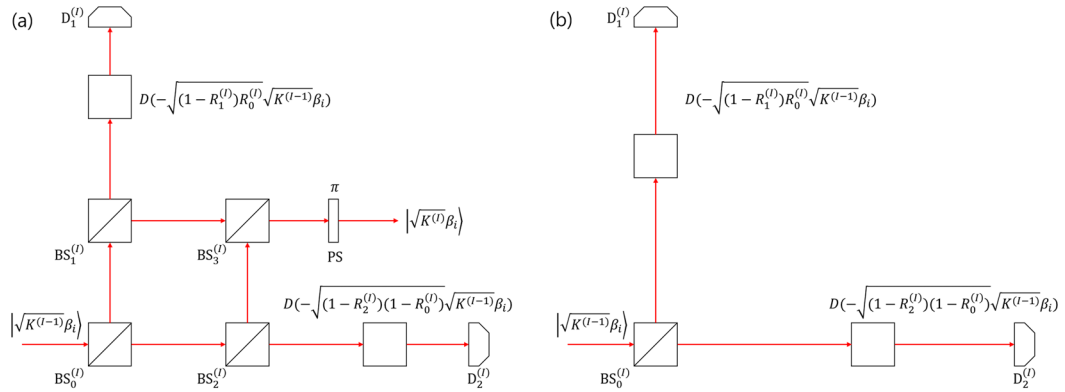


Figure 7. Schematic of the generalized sequential state discrimination based on the Banaszek model[40]. (**a**) Shows the measurement for Bob $I < N$. (**b**) Shows the measurement for Bob N. $\mathrm{BS}_i^{(I)}$ means the beam splitters of Bob I's measurement. $\mathrm{D}_i^{(I)}$ is Bob I's i-th on-off detector, PS is π–phase shifter and D is beam splitter, which is mathematically expressed as a displacement operator[42].

Here, we deal with sequential state discrimination involving N receivers. Based on the Banaszek model, Bob $I \in \{1, \ldots, N\}$'s measurement can be designed as shown in Fig. 7. According to the figure, Alice prepares one out of two coherent states $|\beta_i\rangle (i = 1, 2)$, where $|\beta_i\rangle = e^{-|\beta_i|^2} \sum_{n=0}^{\infty} \frac{\beta_i^n}{\sqrt{n!}} |n\rangle$. Bob I's measurement consists of beam combiners and two on-off detectors. If two on-off detectors $\mathrm{D}_1^{(I)}$ and $\mathrm{D}_2^{(I)}$ give outcomes of [off,on]([on,off]), Bob I distinguishes Alice's coherent state as $|\beta_1\rangle (|\beta_2\rangle)$. If two outcomes are [off,off], Bob I cannot distinguish Alice's coherent state. Here, [off,off] corresponds to an inconclusive result.

If $I < N$, beam splitters $\mathrm{BS}_1^{(I)}$, $\mathrm{BS}_2^{(I)}$, and $\mathrm{BS}_3^{(I)}$ are used to produce the post-measurement state. If $R_i^{(I)}$ denotes the reflectivity of $\mathrm{BS}_i^{(I)}$, $R_3^{(I)}$ can be given as[34]

$$R_3^{(I)} = \frac{R_2^{(I)}(1 - R_0^{(I)})}{R_1^{(I)} R_0^{(I)} + R_2^{(I)}(1 - R_0^{(I)})}.$$

Bob I's post-measurement state can be expressed as $\left|\sqrt{\prod_{J=1}^{I} f(R_0^{(J)}, R_1^{(J)}, R_2^{(J)})}\,\beta_i\right\rangle$, where f is a real function: $f(x, y, z) = xy + (1 - x)z$. According to Rule 1, Bob N should perform an optimal unambiguous discrimination on Bob $N - 1$'s post-measurement state. Therefore, Bob N's measurement is same as in the Banaszek model (see Fig. 7). In our optical model, the success probability of the generalized sequential state discrimination is obtained as

$$\begin{aligned} P_s^{(B_1,\ldots,B_N)} &= q_1 \left\{1 - e^{-\bar{R}_2^{(1)} R_0^{(1)} |\beta_1 - \beta_2|^2}\right\} \left\{1 - e^{-R_2^{(2)} R_0^{(2)} K^{(1)} |\beta_1 - \beta_2|^2}\right\} \\ &\times \left\{1 - e^{-R_2^{(3)} R_0^{(3)} K^{(2)} |\beta_1 - \beta_2|^2}\right\} \times \cdots \times \left\{1 - e^{-R_2^{(N-1)} R_0^{(N-1)} K^{(N-1)} |\beta_1 - \beta_2|^2}\right\} \\ &\times \left\{1 - e^{-R^{(N)} K^{(N)} |\beta_1 - \beta_2|^2}\right\} \\ &+ q_2 \left\{1 - e^{-\bar{R}_1^{(1)} R_0^{(1)} |\beta_1 - \beta_2|^2}\right\} \left\{1 - e^{-\bar{R}_1^{(2)} R_0^{(2)} K^{(1)} |\beta_1 - \beta_2|^2}\right\} \\ &\times \left\{1 - e^{-\bar{R}_1^{(3)} R_0^{(3)} K^{(2)} |\beta_1 - \beta_2|^2}\right\} \times \cdots \times \left\{1 - e^{-\bar{R}_1^{(N-1)} R_0^{(N-1)} K^{(N-1)} |\beta_1 - \beta_2|^2}\right\} \\ &\times \left\{1 - e^{-R^{(N)} K^{(N)} |\beta_1 - \beta_2|^2}\right\}. \end{aligned} \tag{32}$$

Here, $\bar{R} = 1 - R$ and $K^{(I)} = \prod_{J=1}^{I} f(R_0^{(I)}, R_1^{(I)}, R_2^{(I)})$. The optimal success probability of Eq. (32) is shown in Figs. 8 and 9. In Fig. 8, we assume that the prior probabilities are equal. In Fig. 9, we assume that $q_1 = 0.4$ and $q_2 = 0.6$. The red circles (blue dots) shows the optimal success probability, with (without) the additional constraints $R_0^{(I)} = 1 (\forall I \in \{1, \ldots, N - 1\})$ and $R^{(N)} = 1$. In Fig. 8, when $|\beta_1 - \beta_2|^2 < B(N)$, the maximum of Eq. (32) is equal to $P_s^{(B_1,\ldots,B_N),\mathrm{opt}} = (1 - |\langle\beta_1|\beta_2\rangle|^{1/N})^N$. When $|\beta_1 - \beta_2|^2 \geq B(N)$, the maximum of Eq. (32) is equal to $P_s^{(B_1,\ldots,B_N),\mathrm{opt}} = \frac{1}{2}(1 - |\langle\beta_1|\beta_2\rangle|^{2/N})^N$, where $B(N) = -2N \ln(2^{1/N} - 1)$. We can numerically calculate $B(N)$ as

$$\begin{aligned} B(2) &= 3.525494348078171 \\ B(3) &= 8.084264089976305 \\ B(4) &= 13.319304138790477 \\ B(5) &= 19.058354881391878 \\ B(6) &= 25.199449280612455 \\ B(7) &= 31.675056582901121 \end{aligned}$$

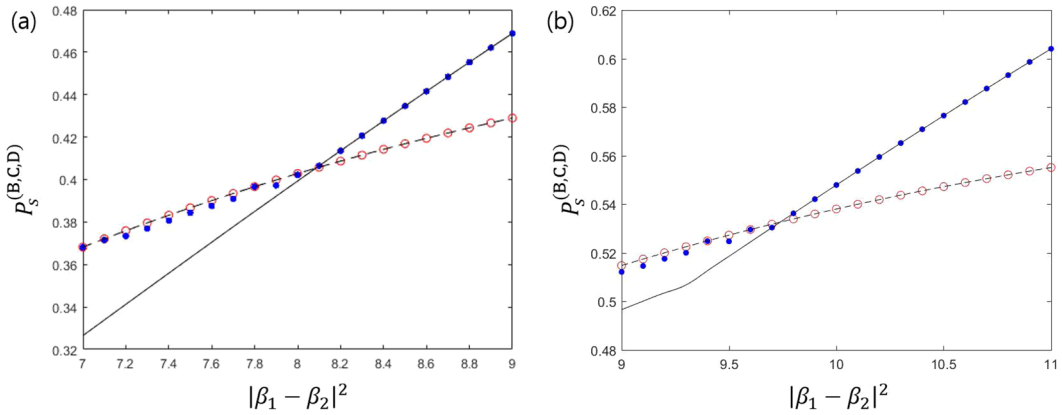


Figure 8. Plots of the success probability of the sequential state discrimination of coherent states, when there are three receivers. The solid black line (dashed black line) shows the optimal success probability when the three receivers discriminate two pure states of Alice (one out of two pure states of Alice). The red circles (blue dots) shows the maximum of Eq. (32), with (without) $R_0^{(I)} = 1$. In (**a**), we use $q_1 = q_2 = 0.5$, and in (**b**) we use $q_1 = 0.4$, $q_2 = 0.6$.

In Fig. 9, when $|\beta_1 - \beta_2|^2$ is small, the maximum of Eq. (32) is equal to that of the optimization problem in Eq. (27). If $|\beta_1 - \beta_2|^2$ is large, the maximum of Eq. (32) is equal to $P_s^{(B_1,\ldots,B_N),\mathrm{opt}} = 0.6(1 - |\langle\beta_1|\beta_2\rangle|^{2/N})^N$. Therefore, we conclude that our model can optimally perform a generalized sequential state discrimination of two coherent states. Because the Huttner model provides the same measurement probability distribution as that of the Banaszek model[34], generalized sequential state discrimination can be performed optimally, using the modified Huttner model. Unlike the Banaszek model, the Huttner model uses a horizontally polarized coherent state $|\beta_i\rangle$, mixed with a vertically polarized coherent state $|\gamma\rangle$, as an information carrier. Therefore, if an eavesdropper attempts to steal information encoded in coherent light, the eavesdropper will inevitably change at least one of two polarized coherent states. Hence, eavesdropping ruins the unambiguous discrimination and produces an error on the receiver's measurement. Therefore, all receivers can notice the fact that an eavesdropper exists by checking whether an error occurs.

We compare the optimal success probabilities of Figs. 8 and 9. One can see that in Fig. 10, the solid red line which denotes the optimal success probability of sequential state discrimination for three receivers is larger than the solid black line which denotes the optimal success probability of sequential state discrimination for four receivers. The reason for the difference between two success probabilities is due to the strategy of David. In the case of $N = 3$, David becomes the last receiver and chooses optimal unambiguous discrimination. However, in the case of $N = 4$, David is not the last receiver and should choose nonoptimal unambiguous discrimination.

Implementing the sequential state discrimination of two mixed states. In this subsection, we propose a way to implement the generalized sequential state discrimination of two mixed states. In our model, the mixed states are produced as in the following process (See Fig. 11): First, Alice prepares one out of two coherent states $|\beta_i\rangle$, $|\bar{\beta}_i\rangle$, with prior probabilities $|r_i\rangle$, $|\bar{r}_i\rangle$. Second, Alice polarizes the coherent state $|\beta_i\rangle(|\bar{\beta}_i\rangle)$ in the horizontal (vertical) direction. After performing two steps, Alice obtains a mixed state as[50]

$$\rho_i = r_i|\beta_i \otimes H\rangle\langle\beta_i \otimes H| + \bar{r}_i|\bar{\beta}_i \otimes V\rangle\langle\bar{\beta}_i \otimes V|, \tag{33}$$

where $|\beta_i \otimes H\rangle = |\beta_i\rangle \otimes |H\rangle$ and $|\bar{\beta}_i \otimes V\rangle = |\bar{\beta}_i\rangle \otimes |V\rangle$. Because $|\beta_i \otimes H\rangle$ and $|\bar{\beta}_i \otimes V\rangle$ are orthogonal to each other, Eq. (33) is equal to Eq. (6). If Alice wants to build rank-m mixed states, she would perform the following process: First, Alice prepares a coherent state $|\beta_{ij}\rangle \in \{|\beta_{i1}\rangle, \ldots, |\beta_{im}\rangle\}$ with a prior probability r_{ij}. Second, she passes β_{ij} to the j-th photon path (D_j). Then, she obtains the following mixed states:

$$\rho_i = r_{i1}|\beta_{i1} \otimes D_1\rangle\langle\beta_{i1} \otimes D_1| + \cdots + r_{im}|\beta_{im} \otimes D_m\rangle\langle\beta_{im} \otimes D_m|, \tag{34}$$

where $|\beta_{ij} \otimes D_j\rangle = |\beta_{ij}\rangle \otimes |D_j\rangle$. Moreover, $|D_j\rangle$ denotes the j-th path state.

$|\beta_i \otimes H\rangle$ and $|\bar{\beta}_i \otimes V\rangle$ can be perfectly discriminated by using a polarized beam splitter. We can use the Banaszek model to discriminate the nonorthogonal coherent states and in Fig. 10, we propose an optical model to discriminate the mixed states, expressed as Eq. (33). The Huttner model can also be used to perform the measurement for the generalized sequential state discrimination of two mixed states, in a similar way to that in Fig. 10.

Security analysis of multiparty QKD based on sequential state discrimination - Part I: Eve's single trial for eavesdropping

In this section, we analyze the security of multiparty QKD, which optimal sequential state discrimination provides. Even though our analysis is confined to the case of four receivers (Bob, Charlie, David, Eliot), it can be consistently extended to the case of arbitrary number of receivers (See Fig. 12). In information theory, the

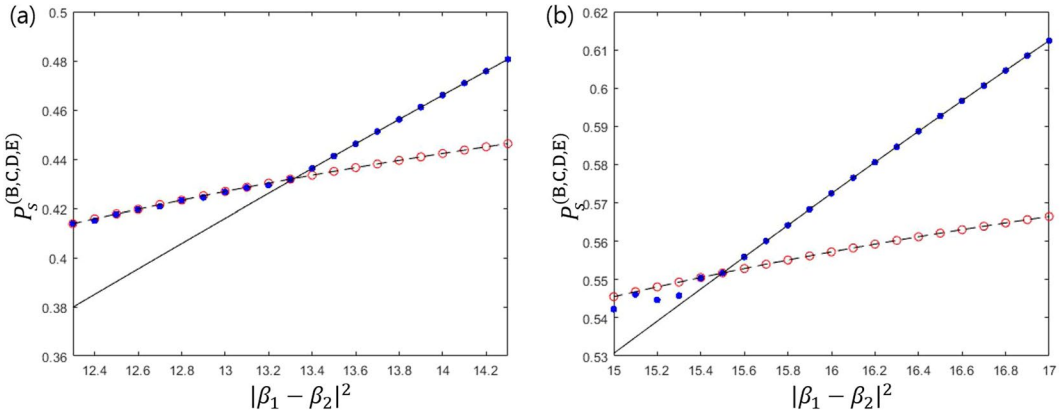


Figure 9. Plots of the success probability of the sequential state discrimination of the coherent states, when four receivers exist. The solid black line (dashed black line) shows the optimal success probability when three receivers discriminate two pure states of Alice (one out of two pure states of Alice). In (**a**), we use $q_1 = q_2 = 0.5$ and in (**b**), we use $q_1 = 0.4$, $q_2 = 0.6$.

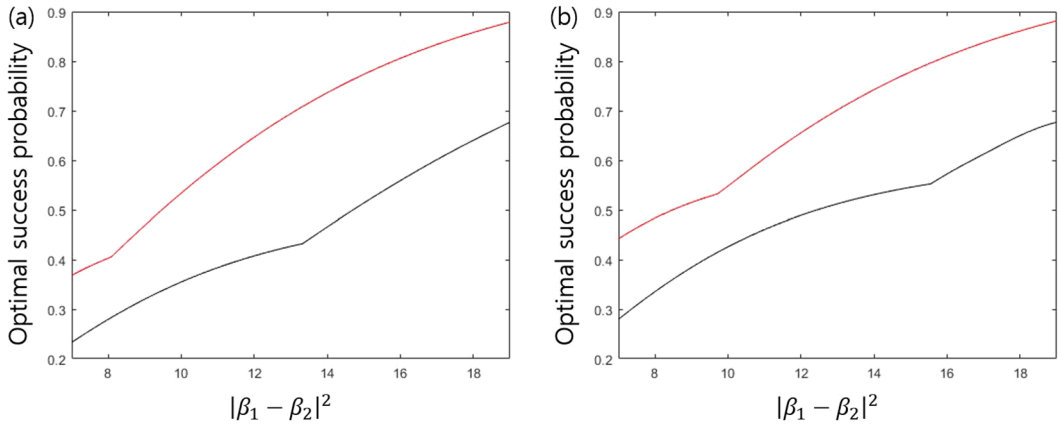


Figure 10. The optimal success probabilities when receivers are three and four. In (**a**), the prior probabilities of two coherent states are identical. In (**b**), the prior probabilities of two coherent states are $q_1 = 0.4$ and $q_1 = 0.6$. Here, the solid red (black) line denotes the case of $N = 3(N = 4)$. This result shows that the optimal success probability of $N = 3$ is larger than that of $N = 4$. It can be understood as follows: For instance, when receivers are three and four, the third receiver called David should use a strategy depending on the existence of an extra receiver. In the case of $N = 3$, David is the last receiver and should choose optimal unambiguous discrimination. However, in the case of $N = 4$, David is not the last receiver and should use nonoptimal unambiguous discrimination. Therefore, the optimal success probability of $N = 3$ is larger than that of $N = 4$.

classical bit of Alice can be expressed by $i \in \{0, 1\}$ and we use $\{|0\rangle, |1\rangle, |?\rangle\}$ as a computational basis. Here, $|?\rangle$ is a computational basis that corresponds to the "failure" of Eve.

In QKD, Alice should minimize the prior information of the classical bit. Otherwise, Eve can obtain the prior information of the classical bit without being caught by the sender and the receiver. Alice prepares quantum states $|\psi_0\rangle$ and $|\psi_1\rangle$ corresponding to classical bit 0 and 1, with identical prior probability. In the view of Alice and Bob, it is the situation where Alice and Bob share the entangled state $|0\rangle \otimes |\psi_0\rangle + |1\rangle \otimes |\psi_1\rangle$[43]. Suppose that Eve tries to eavesdrop between Alice and Bob (Later, we will consider the case where the strategy of Eve is a collective attack[43]). When we denote the eavesdropping of Eve as a quantum channel $\Lambda_B^{(A\to B)}$, the bipartite quantum state between Alice and Bob can be expressed by

$$\sigma_{AB} = (\mathrm{id}_A \otimes \Lambda_B^{(A\to B)})(|\Psi\rangle\langle\Psi|_{AB}),$$

where $|\Psi\rangle_{AB} = (1/\sqrt{2})(|0\rangle_A \otimes |\psi_0\rangle_B + |1\rangle_A \otimes |\psi_1\rangle_B)$ and id_A is an identity channel. One can assume that Alice and Bob do not have any information about Eve. Then, $\Lambda_B^{(A\to B)}$ can be seen as

$$\Lambda_B^{(A\to B)}(\sigma) = \eta_{AB}\sigma + (1 - \eta_{AB})\frac{I_B}{2},$$

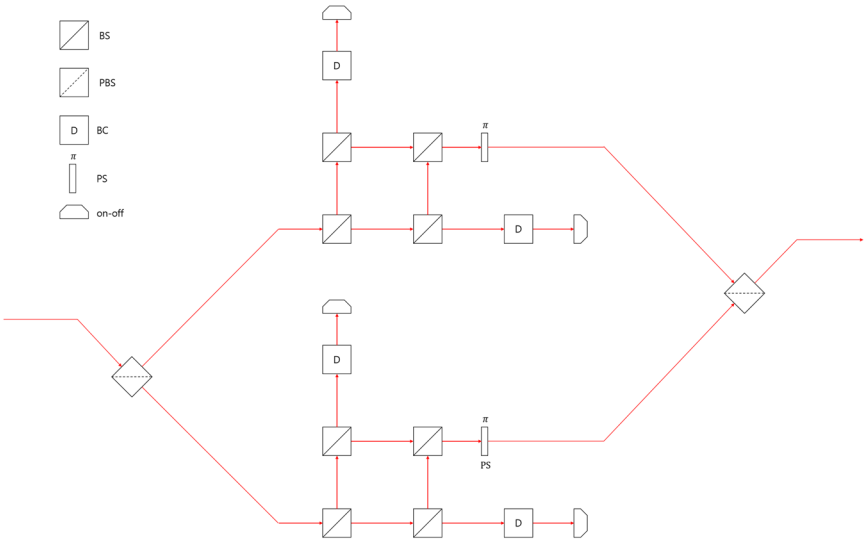


Figure 11. Schematic of the optical model for performing the generalized sequential state discrimination of two mixed states. Here, BS is a beam splitter, PBS is a polarized beam splitter, D is a beam combiner, PS is a phase shifter, and on-off is an on-off detector.

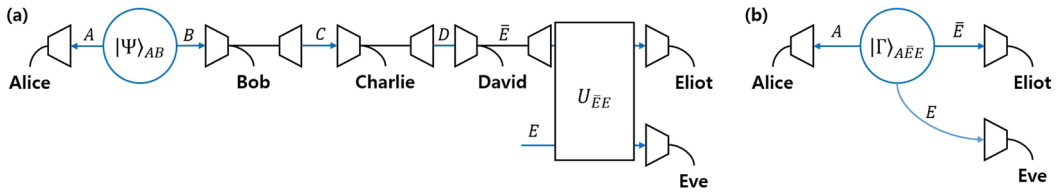


Figure 12. The case where Eve eavesdrops between David and Eliot. In (**a**), Eve eavesdrops between David and Eliot. Here, Eve interacts her system E with system $\bar{E}$. The interaction is described by the global unitary operator $U_{\bar{E}E}$. After the interaction, Eve measures system E. The description of (**a**) is equivalent to the case of (**b**), where Alice, Eve, and Eliot share $|\Gamma\rangle_{A\bar{E}E}$.

where $\eta_{AB} \in [0, 1]$ is the efficiency of the quantum channel. As the efficiency is more close to 1, Alice and Bob can be less affected by Eve. Then, the bipartite state σ_{AB} can be given as

$$\sigma_{AB} = \eta_{AB}|\Psi\rangle\langle\Psi|_{AB} + (1 - \eta_{AB})|+\rangle\langle+|_A \otimes \frac{I_B}{2}. \tag{35}$$

The purification of the bipartite state σ_{AB} can be found as

$$|\Gamma\rangle_{ABE} = \sqrt{\eta_{AB}}|\Psi\rangle_{AB} \otimes |?\rangle_E + \sqrt{1 - \eta_{AB}}|+\rangle_A \otimes |\phi_+\rangle_{BE}, \tag{36}$$

where $|\phi_+\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle)$. Equation (36) can be understood as follows. If Eve fails to eavesdrop with a probability η_{AB}, Alice and Bob succeed in sharing $|\Psi\rangle$. Then, Alice and Bob can share a secret key. Meanwhile, the quantum state of Eve is given by $|?\rangle$. If Eve succeeds to eavesdrop with a probability of $1 - \eta_{AB}$, Eve shares a maximally entangled state with Bob.

The joint probability of the case where Alice prepares $|\psi_i\rangle$, Bob obtains j as a result of measurement, and Eve gets bit k can be given as follows:

$$P_{ABE}(i, j, k) = \mathrm{Tr}_{ABE}\{|\Gamma\rangle\langle\Gamma|_{ABE}(|i\rangle\langle i|_A \otimes M_j \otimes |k\rangle\langle k|_E)\}, \ \ i, j \in \{0, 1\}. \tag{37}$$

When the prior probability is identical, the optimal measurement of Bob corresponds to the case of $\alpha_0 = \alpha_1 = 1 - s^{1/N}$. Therefore, one can obtain the following probabilities (The detailed derivation can be found in Method):

$$\begin{aligned} P_A(i) &= \frac{1}{2}, \\ P_{AB}(i,j) &= \eta_{AB}\frac{1}{2}(1-s^{1/4})\delta_{ij} + (1-\eta_{AB})\frac{1-s^{1/4}}{4(1-s^2)}, \\ P_E(k) &= \frac{1-\eta_{AB}}{2}, \\ P_{BE}(j,k) &= \frac{(1-\eta_{AB})(1-s^{1/4})}{4\{1+(-1)^k s\}}. \end{aligned} \tag{38}$$

In Eq. (38), $i, j, k \in \{0, 1\}$ is considered. Because an inconclusive result of Bob and failure of Eve cannot provide any information, Bob (Eve) can discard the inconclusive result (failure). The post-processing transforms four probabilities of Eq. (38) as follows:

$$\begin{aligned} \tilde{P}_A(i) &= \frac{P_A(i)}{P_A(0)+P_A(1)}, \tilde{P}_E(i) = \frac{P_E(i)}{P_E(0)+P_E(1)}, \\ \tilde{P}_{AB}(i,j) &= \frac{P_{AB}(i,j)}{P_{AB}(0,0)+P_{AB}(0,1)+P_{AB}(1,0)+P_{AB}(1,1)}, \tilde{P}_{BE}(j,k) \\ &= \frac{P_{BE}(j,k)}{P_{BE}(0,0)+P_{BE}(0,1)+P_{BE}(1,0)+P_{BE}(1,1)}, \end{aligned}$$

for $i, j, k \in \{0, 1\}$. It should be noted that the four probabilities obtained from post-processing are dependent only on the probability of the conclusive result. From these four probabilities, one can evaluate the secret key rate between Alice and Bob in the following way[44]:

$$K_{AB:E} = \max\{0, I(A:B) - I(B:E)\}.$$

Here, $I(X:Y)(H(X,Y))$ is Shannon's mutual information (joint Shannon entropy) between X and Y. And because of $\tilde{P}_A(i) = \tilde{P}_E(i) = 1/2(\forall\, i \in \{0,1\})$, the relation of $I(A:B) - I(B:E) = H(B,E) - H(A,B)$ holds. Therefore, the secret key rate is rewritten as

$$K_{AB:E} = \max\{0, H(B,E) - H(A,B)\}.$$

Now, let us consider the case where Eve eavesdrops between Bob and Charlie. In this case, the quantum state between Alice and Bob is the entangled state $|0\rangle \otimes |\phi_0^{(B)}\rangle + |1\rangle \otimes |\phi_1^{(B)}\rangle$(The detailed derivation is found in Method). Here, $|\phi_i^{(B)}\rangle$ is the post-measurement quantum state corresponding to $i \in \{0, 1\}$ which is the result of measurement of Bob. Because Eve eavesdrops between Bob and Charlie, when we denote the eavesdropping of Eve as a quantum channel $\Lambda_B^{(B\to C)}$, the bipartite state between Bob and Charlie can be given as

$$\sigma_{AC} = (\mathrm{id}_A \otimes \Lambda_C^{(B\to C)})(|\Phi^{(B)}\rangle\langle\Phi^{(B)}|_{AC}),$$

where $|\Phi^{(B)}\rangle_{AC} = (1/\sqrt{2})(|0\rangle_A \otimes |\phi_0^{(B)}\rangle_C + |1\rangle_A \otimes |\phi_1^{(B)}\rangle_C)$. Likewise Eq. (37), we can obtain the marginal probabilities of Alice, Charlie, and Eve:

$$\begin{aligned} P_A(i) &= \frac{1}{2}, \\ P_{AC}(i,j) &= \eta_{BC}\frac{1}{2}(1-s^{1/4})\delta_{ij} + (1-\eta_{BC})\frac{1-s^{1/4}}{4(1-s^{3/2})}, \\ P_E(k) &= \frac{1-\eta_{BC}}{2}, \\ P_{CE}(j,k) &= \frac{(1-\eta_{BC})(1-s^{1/4})}{4\{1+(-1)^k s^{3/4}\}}. \end{aligned} \tag{39}$$

Here, η_{BC} is a channel efficiency between Bob and Charlie. In the case where Eve eavesdrops between Charlie and David, the marginal probabilities of Alice, David, and Eve are given as

$$\begin{aligned} P_A(i) &= \frac{1}{2}, \\ P_{AD}(i,j) &= \eta_{CD}\frac{1}{2}(1-s^{1/4})\delta_{ij} + (1-\eta_{CD})\frac{1-s^{1/4}}{4(1-s)}, \\ P_E(k) &= \frac{1-\eta_{CD}}{2}, \\ P_{DE}(j,k) &= \frac{(1-\eta_{CD})(1-s^{1/4})}{4\{1+(-1)^k s^{1/2}\}}, \end{aligned} \tag{40}$$

where η_{BC} is a channel efficiency between Charlie and David. And in the case where Eve eavesdrops between David and Eliot, the marginal probabilities of Alice, Eliot, and Eve are obtained as (Here, the index $\bar{E}$ denotes Eliot)

$$\begin{aligned} P_A(i) &= \frac{1}{2}, \\ P_{A\bar{E}}(i,j) &= \eta_{D\bar{E}}\frac{1}{2}(1-s^{1/4})\delta_{ij} + (1-\eta_{D\bar{E}})\frac{1-s^{1/4}}{4(1-s^{1/2})}, \\ P_{\bar{E}}(k) &= \frac{1-\eta_{D\bar{E}}}{2}, \\ P_{\bar{E}E}(j,k) &= \frac{(1-\eta_{D\bar{E}})(1-s^{1/4})}{4\{1+(-1)^k s^{1/4}\}}. \end{aligned} \tag{41}$$

The secret key rate can be evaluated by

$$K_{AX:E} = \max\{0,\, I(A\colon X) - I(X\colon E)\} = \max\{0,\, H(X,E) - H(A,X)\},\ \ X \in \{B, C, D, \bar{E}\}.$$

Figure 13 shows $K_{AX:E}$. Here, η is the efficiency of channel where Eve involves. In Fig. 13, we consider the case of $s = 0.00128$. Also, solid line, dashed line, dash-dot line, and dotted line denote the cases of $X = B,\ C,\ D$ and $\bar{E}$ respectively.

One can see that in Fig. 13, the secret key rate is the lowest in the case of $X = \bar{E}$(dotted line).This implies that the best performance of Eve can be obtained between David and Eliot. However, it should be emphasized that the effect depending on the position of eavesdropping is not big.

Security analysis of multiparty QKD based on sequential state discrimination - Part II: Eve's multi-trial for eavesdropping

Here, we consider the case where Eve uses quantum memories. By using quantum memories of Eve, she can perform eavesdropping between sender and receivers. Suppose that Alice, Bob, and Charlie are involved in sequential state discrimination as a sender and two receivers. In this case, for eavesdropping, Eve uses two quantum memories: one quantum memory is used between Alice and Bob, and another quantum memory is used between Bob and Charlie (It should be noted that even though we consider the sequential state discrimination comprised of a sender and two receivers, our argument can be extended to the sequential state discrimination comprised of a sender and multi-receivers).

Now, if Eve use a quantum memory E_B for evesdropping between Alice and Bob (see Fig. 14), system of A, B, and E_B can be described as

$$|\Gamma\rangle_{ABE_B} = \sqrt{\eta_{AB}}|\Psi\rangle_{AB} \otimes |?\,\rangle_{E_B} + \sqrt{1-\eta_{AB}}|+\rangle_A \otimes |\phi_+\rangle_{BE_B}.$$

When Bob discards an inconclusive result, $|\Gamma\rangle_{ABE_B}$ becomes the following mixed state:

$$\sigma_{ACE_B} = \mathcal{N}(\eta_{AB})\{|\mathcal{E}_0\rangle\langle\mathcal{E}_0|_{AE_B} \otimes |\phi_0^{(B)}\rangle\langle\phi_0^{(B)}|_C + |\mathcal{E}_1\rangle\langle\mathcal{E}_1|_{AE_B} \otimes |\phi_1^{(B)}\rangle\langle\phi_1^{(B)}|_C\}.$$

Here, $K_i^{(B)}$: $\mathscr{H}_B \to \mathscr{H}_C$ is the Kraus operator of Bob which corresponds to the measurement result $i \in \{0,\ 1,\ ?\ \}$. And we have $\mathcal{N}(\eta_{AB}) = [\langle\mathcal{E}_0|\mathcal{E}_0\rangle + \langle\mathcal{E}_1|\mathcal{E}_1\rangle]^{-1}$. The non- normalized vector $|\mathcal{E}_0\rangle,\ |\mathcal{E}_1\rangle$ is defined as follows:

$$\begin{aligned} |\mathcal{E}_0\rangle_{AE_B} &= \sqrt{\frac{\eta_{AB}(1-\sqrt{s})}{2}}|0\rangle_A \otimes |?\,\rangle_{E_B} + \sqrt{\frac{(1-\eta_{AB})(1-\sqrt{s})}{2}}|+\rangle_A \otimes |\alpha_0\rangle_{E_B}, \\ |\mathcal{E}_1\rangle_{AE_B} &= \sqrt{\frac{\eta_{AB}(1-\sqrt{s})}{2}}|1\rangle_A \otimes |?\,\rangle_{E_B} + \sqrt{\frac{(1-\eta_{AB})(1-\sqrt{s})}{2}}|+\rangle_A \otimes |\alpha_1\rangle_{E_B}. \end{aligned}$$

Here, Bob's POVM consists of $\alpha_i|\alpha_i\rangle\langle\alpha_i|$. When Eve uses a quantum memory E_C for eavesdropping between Bob and Charlie, the eavesdropping of Eve can be expressed as a quantum channel $\Lambda_C^{(B\to C)}$. That is, the eavesdropping of Eve transforms σ_{ACE_B} as follows:

$$\begin{aligned} \mathrm{id}_{AE_B} \otimes \Lambda_C^{(B\to C)}(\sigma_{ACE_B}) &= \mathcal{N}(\eta_{AB})\Bigg[\eta_{BC}\sum_{x=0}^{1}|\mathcal{E}_x\rangle\langle\mathcal{E}_x|_{AE_B} \otimes |\phi_x^{(B)}\rangle\langle\phi_p^{(B)}|_C \\ &\quad + (1-\eta_{BC})\sum_{x=0}^{1}|\mathcal{E}_x\rangle\langle\mathcal{E}_x|_{AE_B} \otimes \frac{I_C}{2}\Bigg]. \end{aligned}$$

The purification of $\mathrm{id}_{AE_B} \otimes \Lambda_C^{(B\to C)}(\sigma_{ACE_B})$ is given as

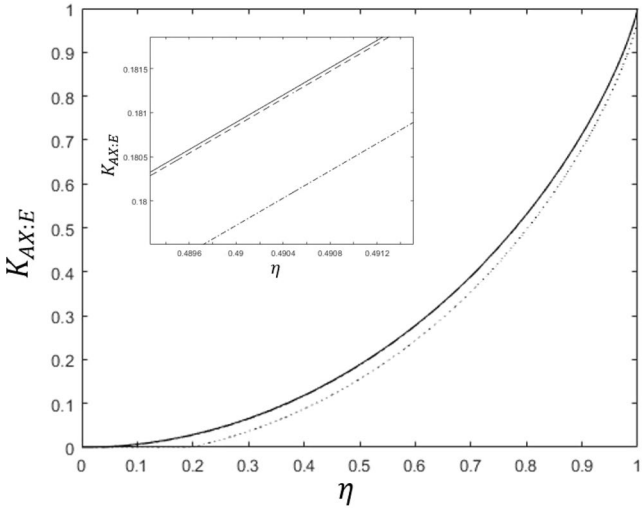


Figure 13. The secret key rate $K_{AX:E}$. Here, solid line, dashed line, dashed-dot line and dotted line correspond to the case of $X = B$, C, D and $\bar{E}$, respectively. η is the efficiency of the quantum channel, where eavesdropper Eve exists. According to this, the nonzero secret key rate is guaranteed in almost every region of η.

$$\begin{aligned}
|\Gamma\rangle_{ACE_BE_C} &= \sqrt{\eta_{BC}\mathcal{N}(\eta_{AB})}\{|\mathcal{E}_0\rangle_{AE_B}\otimes|\phi_0^{(B)}\rangle_C\otimes|?_0\rangle_{E_C} \\
&\quad + |\mathcal{E}_1\rangle_{AE_B}\otimes|\phi_1^{(B)}\rangle_C\otimes|?_1\rangle_{E_C}\} \\
&= \sqrt{\frac{(1-\eta_{BC})\mathcal{N}(\eta_{AB})}{2}}\big(|\mathcal{E}_0\rangle_{AE_B}\otimes|0\rangle_C\otimes|00\rangle_{E_C} \\
&\quad + |\mathcal{E}_1\rangle_{AE_B}\otimes|0\rangle_C\otimes|01\rangle_{E_C} \\
&\quad + |\mathcal{E}_0\rangle_{AE_B}\otimes|1\rangle_C\otimes|10\rangle_{E_C} + |\mathcal{E}_1\rangle_{AE_B}\otimes|1\rangle_C\otimes|11\rangle_{E_C}\big).
\end{aligned}$$

Here, $|?_0\rangle$ and $|?_1\rangle$ are computational basis corresponding to Eve's failure. It should be noted that $|?_0\rangle$ and $|?_1\rangle$ are orthogonal to each other. The computational basis is orthogonal to $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$.

Unlike system E_B, system E_C is composed of two subsystems. It is because when Eve eavesdrops between Bob and Charlie, Eve also can eavesdrop between Alice and Bob. When E_{C1} and E_{C2} are the subsystems of E_C, $|\Gamma\rangle_{ACE_BE_C}$ can be described in the following way:

$$\begin{aligned}
|\Gamma\rangle_{ACE_BE_C} &= \sqrt{\eta_{BC}\mathcal{N}(\eta_{AB})}\Big\{|\mathcal{E}_0\rangle_{AE_B}\otimes|\phi_0^{(B)}\rangle_C\otimes|?_0\rangle_{E_C} \\
&\quad + |\mathcal{E}_1\rangle_{AE_B}\otimes|\phi_1^{(B)}\rangle_C\otimes|?_1\rangle_{E_C}\Big\} \\
&\quad + \sqrt{(1-\eta_{BC})\mathcal{N}(\eta_{AB})}\Big\{|\mathcal{E}_0\rangle_{AE_B}\otimes|0\rangle_{E_{C2}} \\
&\quad + |\mathcal{E}_1\rangle_{AE_B}\otimes|1\rangle_{E_{C2}}\Big\}\otimes|\phi_+\rangle_{CE_{C1}}.
\end{aligned}$$

Here, $|\phi_+\rangle$ is a maximally entangled state $|\phi_+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$. In other word, subsystem E_{C1} is used for eavesdropping of Alice's quantum state and subsystem E_{C2} is used for eavesdropping of Bob's post-measurement state.

When Bob and Charlie perform optimal sequential state discrimination, the prior probability is $P_A(i) = 1/2(\ \forall\ i \in \{0, 1\})$ (The detailed calculation can be found in Method). And, the marginal probability between Alice and Charlie is given as follows:

$$\begin{aligned}
P_{AC}(i,j) &= \eta_{BC}\mathcal{N}(\eta_{AB})(1-\sqrt{s})\delta_{j0}\mathcal{X}_0(i) + \eta_{BC}\mathcal{N}(\eta_{AB})(1-\sqrt{s})\delta_{j1}\mathcal{X}_1(i) \\
&\quad + \frac{(1-\eta_{BC})\mathcal{N}(\eta_{AB})}{2(1+\sqrt{s})}\{\mathcal{X}_0(i) + \mathcal{X}_1(i)\}.
\end{aligned}$$

Here, $\mathcal{X}_a(i)$ is defined in the following way:

$$\mathcal{X}_a(i) = \frac{1}{2}\eta_{AB}(1-\sqrt{s})\delta_{ia} + \frac{(1-\eta_{AB})(1-\sqrt{s})}{4(1-s^2)}.$$

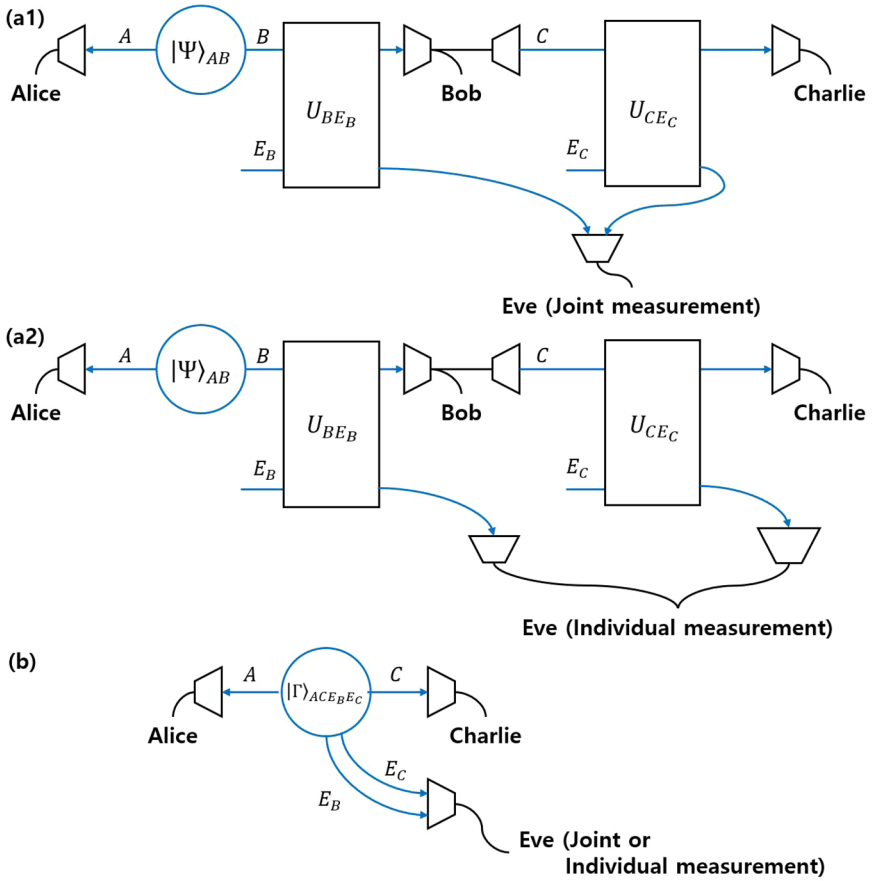


Figure 14. The case where Eve eavesdrops between Alice and Bob and between Bob and Charlie. In (**a1**), Eve eavesdrops between Alice and Bob and between Bob and Charlie. First, Eve prepares two systems of E_B and E_C. Then, Eve interacts system E_B with system B (The interaction is expressed by the global unitary operator U_{BE_B}). Second, Eve interacts system E_C with system C (This interaction is described by the global unitary operator U_{CE_C}). Atfer these interactions, Eve measures system E_B and E_C globally (We denote this measurement as joint measurement). Here, the structure of joint measurement is determined by a unitary transformation $V = \{V_{pq}\}_{p,q=1}^{18}$. If the unitary transformation V is fixed as the identity, (**a1**) and (**a2**) are equivalent. In (**a2**), Eve measures system E_B and system E_C locally (We denote this measurement as an individual measurement). The description of (**a1**) and (**a2**) is equivalent to the case of (**b**), where Alice, Charlie, and Eve share $|\Gamma\rangle_{ACE_BE_C}$.

The result of measurement of Eve can be expressed as a single label $p \in \{?, 0, 1\}_{E_B} \times \{?_0, ?_1, 00, 01, 10, 11\}_{E_C}$ (The notation of the label can be found in Fig. 15). It should be noted that $|?_0\rangle$ and $|?_1\rangle$ cannot be expressed by a linear combination of $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$.

The marginal probability of Charlie and Eve is given by

$$\begin{aligned} P_E(p) &= \langle\Gamma|\Big(I_{AC} \otimes |\pi_p\rangle_{E_BE_C}\langle\pi_p|_{E_BE_C}\Big)|\Gamma\rangle \\ &= \langle\Gamma|_{ACE_BE_C}\Big(I_{AC} \otimes |\pi_p\rangle_{E_BE_C}\Big)\Big(I_{AC} \otimes \langle\pi_p|_{E_BE_C}\Big)|\Gamma\rangle_{ACE_BE_C}, \\ P_{CE}(k,p) &= \langle\Gamma|\Big(I_A \otimes \beta_k|\beta_k\rangle\langle\beta_k|_C \otimes |\pi_p\rangle_{E_BE_C}\langle\pi_p|_{E_BE_C}\Big)|\Gamma\rangle \\ &= \beta_k\langle\Gamma|_{ACE_BE_C}\Big(I_A \otimes |\beta_k\rangle_C \otimes |\pi_p\rangle_{E_BE_C}\Big) \\ &\quad \times \Big(I_A \otimes \langle\beta_k|_C \otimes \langle\pi_p|_{E_BE_C}\Big)|\Gamma\rangle_{ACE_BE_C}. \end{aligned}$$

$P_E(p)$ and $P_{CE}(p)$ can be found in Method and labeled vector $|\pi_p\rangle_{E_BE_C}$ can be expressed as

$$|\pi_p\rangle_{E_BE_C} = \sum_{q=1}^{18} V_{pq}|q\rangle_{E_BE_C},$$

where every $V_{pq} \in \mathbb{C}$ satisfies $\sum_{r=1}^{18} V_{pr}V_{qr}^* = \sum_{k=r}^{18} V_{rp}^* V_{rq} = \delta_{pq}$. The set of these labeled vectors $\{|\pi_p\rangle\}_{p=1}^{18}$ forms the joint projective measurement $\{|\pi_p\rangle\langle\pi_p|\}_{p=1}^{18}$ of Eve.

label of E_B	label of E_C	p	basis representation
?	$?_0$	1	$\|p=1\rangle_{E_BE_C} = \|?\rangle_{E_B} \otimes \|?_0\rangle_{E_C}$
?	$?_1$	2	$\|p=2\rangle_{E_BE_C} = \|?\rangle_{E_B} \otimes \|?_1\rangle_{E_C}$
?	00	3	$\|p=3\rangle_{E_BE_C} = \|?\rangle_{E_B} \otimes \|00\rangle_{E_C}$
?	01	4	$\|p=4\rangle_{E_BE_C} = \|?\rangle_{E_B} \otimes \|01\rangle_{E_C}$
?	10	5	$\|p=5\rangle_{E_BE_C} = \|?\rangle_{E_B} \otimes \|10\rangle_{E_C}$
?	11	6	$\|p=6\rangle_{E_BE_C} = \|?\rangle_{E_B} \otimes \|11\rangle_{E_C}$
0	$?_0$	7	$\|p=7\rangle_{E_BE_C} = \|0\rangle_{E_B} \otimes \|?_0\rangle_{E_C}$
0	$?_1$	8	$\|p=8\rangle_{E_BE_C} = \|0\rangle_{E_B} \otimes \|?_1\rangle_{E_C}$
0	00	9	$\|p=9\rangle_{E_BE_C} = \|0\rangle_{E_B} \otimes \|00\rangle_{E_C}$
0	01	10	$\|p=10\rangle_{E_BE_C} = \|0\rangle_{E_B} \otimes \|01\rangle_{E_C}$
0	10	11	$\|p=11\rangle_{E_BE_C} = \|0\rangle_{E_B} \otimes \|10\rangle_{E_C}$
0	11	12	$\|p=12\rangle_{E_BE_C} = \|0\rangle_{E_B} \otimes \|11\rangle_{E_C}$
1	$?_0$	13	$\|p=13\rangle_{E_BE_C} = \|1\rangle_{E_B} \otimes \|?_0\rangle_{E_C}$
1	$?_1$	14	$\|p=14\rangle_{E_BE_C} = \|1\rangle_{E_B} \otimes \|?_1\rangle_{E_C}$
1	00	15	$\|p=15\rangle_{E_BE_C} = \|1\rangle_{E_B} \otimes \|00\rangle_{E_C}$
1	01	16	$\|p=16\rangle_{E_BE_C} = \|1\rangle_{E_B} \otimes \|01\rangle_{E_C}$
1	10	17	$\|p=17\rangle_{E_BE_C} = \|1\rangle_{E_B} \otimes \|10\rangle_{E_C}$
1	11	18	$\|p=18\rangle_{E_BE_C} = \|1\rangle_{E_B} \otimes \|11\rangle_{E_C}$

Figure 15. The label of p in terms of basis of E_B and E_C. As an example, $p = 1$ corresponds to the case where the basis of E_B is "?" and the basis of E_C is "$?_0$", which is denoted as $|p=1\rangle_{E_BE_C} = |?\rangle_{E_B} \otimes |?_0\rangle_{E_C}$. And $p = 2$ corresponds to the case where the basis of E_B is "?" and the basis of E_C is "$?_1$", which is denoted as $|p=2\rangle_{E_BE_C} = |?\rangle_{E_B} \otimes |?_1\rangle_{E_C}$.

When Alice, Charlie, and Eve discard inconclusive result, marginal probability becomes

$$\begin{aligned}\tilde{P}_{AC}(i,j) &= \frac{P_{AC}(i,j)}{\sum_{i,j=0}^{1} P_{AC}(i,j)},\\ \tilde{P}_{E}(p) &= \frac{P_{E}(p)}{\sum_{p\notin 1,2,3,4,5,6,7,8,13,14\} P_{E}(p)},\\ \tilde{P}_{CE}(k,p) &= \frac{P_{CE}(k,p)}{\sum_{k=0}^{1}\sum_{p\notin\{1,2,3,4,5,6,7,8,13,14\}} P_{CE}(k,p)}.\end{aligned}$$

The secret key rate between Alice and Charlie, which is given by

$$K_{AC:E_BE_C} = \max\{0, I(A{:}\ C) - I(C{:}\ E)\} = \max\{0, H(A) - H(C,A) + H(C,E) - H(E)\},$$

is displayed in Fig. 16. For convenience, it is assumed that each channel efficiency is equal to each other $\eta_{AB} = \eta_{BC} = \bar{\eta}$. In Fig. 16, the solid black line corresponds to the case where Eve measures her subsystem, by the eighteen basis (This is the case where unitary transformation $\{V_{pq}\}_{p,q=1}^{18}$ is an identity). And, green points correspond to the cases of random unitary transformation. Because Alice and Bob cannot know Eve's system, treating unitary transformation as a random one can be justified.

Experiment 1: The nonzero secret key rate in the case of $s = 0.05$

Individual measurement. When Eve measures her subsystem using eighteen basis $\{|p\rangle\}_{p=1}^{18}$, if $\bar{\eta}$ is greater than $\bar{\eta}_{crit} = 0.65295$, Alice and Charlie can obtain nonzero secret key rate (The method of simulation can be found in Method).

Arbitrary joint measurement. When Eve selects a measurement out of 100000 measurements, the ratio to obtaining nonzero secret key rate increases as $\bar{\eta}$ increases. When $\bar{\eta} = 0.75$, the ratio to obtaining nonzero secret key rate becomes 36.323%. When $\bar{\eta} = 0.95$, the ratio to obtaining nonzero secret key rate becomes 99.978%. Specially, when $\bar{\eta} = 0.975$, nonzero secret key rate can be obtained regardless of a measurement.

Experiment 2: The nonzero secret key rate in the case of $s = 0.10$

Individual measurement. When Eve measures her subsystem using eighteen basis $\{|p\rangle\}_{p=1}^{18}$, if $\bar{\eta}$ is greater than $\bar{\eta}_{crit} = 0.65364$, Alice and Charlie can obtain nonzero secret key rate (The method of simulation can be found in Method).

Arbitrary joint measurement. When Eve selects a measurement out of 100000 measurements, the ratio to obtaining nonzero secret key rate increases as $\bar{\eta}$ increases. When $\bar{\eta} = 0.75$, the ratio to obtaining nonzero secret key rate becomes 36.193%. When $\bar{\eta} = 0.95$, the ratio to obtaining nonzero secret key rate becomes 99.854%. Specially, when $\bar{\eta} = 0.98$, nonzero secret key rate can be obtained regardless of a measurement.

Experiment 3: The nonzero secret key rate in the case of $s = 0.15$

Individual measurement. When Eve measures her subsystem using eighteen basis $\{|p\rangle\}_{p=1}^{18}$, if $\bar{\eta}$ is greater than $\bar{\eta}_{crit} = 0.65480$, Alice and Charlie can obtain nonzero secret key rate (The method of simulation can be found in Method).

Arbitrary joint measurement. When Eve selects a measurement out of 100000 measurements, the ratio to obtaining nonzero secret key rate increases as $\bar{\eta}$ increases. When $\bar{\eta} = 0.75$, the ratio to obtaining nonzero secret key rate becomes 36.253%. When $\bar{\eta} = 0.95$, the ratio to obtaining nonzero secret key rate becomes 99.830%. Specially, when $\bar{\eta} = 0.983$, nonzero secret key rate can be obtained regardless of a measurement.

Discussion

In this report, we presented a generalization of sequential state discrimination. In our work, we did not limit the prior probabilities and the number of quantum states and receivers. We could express the generalized sequential state discrimination as a mathematical optimization problem. Because this optimization cannot be solved analytically, a numerical method was applied to the construction of the optimal POVM. Our optimization problems include all the results of the previous work[27] as special cases. Moreover, we applied the generalized sequential state discrimination to multiparty QKD. If Alice prepares one out of two pure states, the generalized sequential state discrimination can be used to perform multiparty QKD when there are a few receivers. It should be noted that if Alice prepares one out of two mixed states, the optimal success probability of generalized sequential state discrimination can exceed that of the quantum reproducing and quantum broadcasting strategies. Therefore, the generalized sequential state discrimination of mixed states has more potential for application to multiparty QKD than the other strategies. Finally, we analyze the security of multiparty QKD provided by optimal sequential state discrimination. Our analysis shows that the multiparty QKD guarantees nonzero secret key rate even in low channel efficiency.

Even if we considered discriminating two quantum states, we could extend our argument for generalized sequential state discrimination to more than two quantum states. However, an unambiguous discrimination of more than three quantum states has not been known yet. Therefore, one needs to find a way to discriminate more than three quantum states, without any error.

If pure states $\{|\psi_1\rangle, \ldots, |\psi_n\rangle\}$ are linearly dependent, unambiguous discrimination cannot be performed. However, in the case of finite copies of coherent states $\{|\psi_1\rangle^{\otimes C}, \ldots, |\psi_n\rangle^{\otimes C}\}$, they are not always linearly dependent. Therefore, when finite copies of pure state are available, the receiver can perform unambiguous discrimination on $\{|\psi_1\rangle^{\otimes C}, \ldots, |\psi_n\rangle^{\otimes C}\}$[51,52]. Although supports of mixed states $\{\rho_1, \ldots, \rho_n\}$ are completely overlapped to each other, supports of $\{\rho_1^{\otimes C}, \ldots, \rho_n^{\otimes C}\}$ may not be completely overlapped and unambiguous discrimination of $\{\rho_1^{\otimes C}, \ldots, \rho_n^{\otimes C}\}$ can be performed. Using this idea, one may devise sequential state discrimination of general mixed states.

Methods

Derivation of the optimization problem. In this section, we derive the optimization problem of generalized sequential state discrimination. First, a tangential point (γ_1, γ_2) between a plane $P_s^{(\mathrm{B,C,D})}$ and a surface $(1-\gamma_1)(1-\gamma_2) = |\langle\phi_1^{(\mathrm{C})}|\phi_2^{(\mathrm{C})}\rangle|^2$ satisfies the following equality:

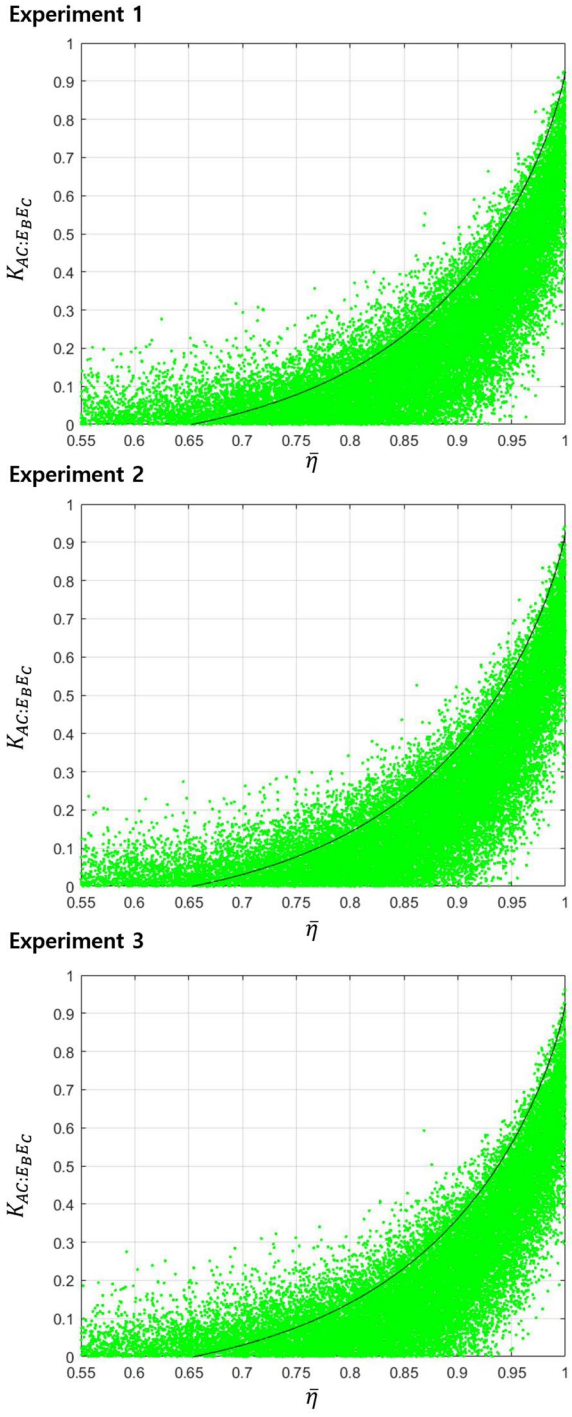
$$\frac{\partial P_s^{(\mathrm{B,C,D})}/\partial\gamma_1}{\partial P_s^{(\mathrm{B,C,D})}/\partial\gamma_2} = \frac{\partial\{(1-\gamma_1)(1-\gamma_2) - |\langle\phi_1^{(\mathrm{C})}|\phi_2^{(\mathrm{C})}\rangle|^2\}/\partial\gamma_1}{\partial\{(1-\gamma_1)(1-\gamma_2) - |\langle\phi_1^{(\mathrm{C})}|\phi_2^{(\mathrm{C})}\rangle|^2\}/\partial\gamma_2}.$$

Combining both above equality and $(1-\gamma_1)(1-\gamma_2) = |\langle\phi_1^{(\mathrm{C})}|\phi_2^{(\mathrm{C})}\rangle|^2$, we obtain (γ_1, γ_2) as

$$\gamma_1 = 1 - |\langle\phi_1^{(\mathrm{C})}|\phi_2^{(\mathrm{C})}\rangle|\sqrt{\frac{q_2\alpha_2\beta_2}{q_1\alpha_1\beta_1}} = 1 - \frac{|\langle\phi_1^{(\mathrm{B})}|\phi_2^{(\mathrm{B})}\rangle|}{\sqrt{(1-\beta_1)(1-\beta_2)}}\sqrt{\frac{q_2\alpha_2\beta_2}{q_1\alpha_1\beta_1}},$$

$$\gamma_2 = 1 - |\langle\phi_1^{(\mathrm{C})}|\phi_2^{(\mathrm{C})}\rangle|\sqrt{\frac{q_1\alpha_1\beta_1}{q_2\alpha_2\beta_2}} = 1 - \frac{|\langle\phi_1^{(\mathrm{B})}|\phi_2^{(\mathrm{B})}\rangle|}{\sqrt{(1-\beta_1)(1-\beta_2)}}\sqrt{\frac{q_1\alpha_1\beta_1}{q_2\alpha_2\beta_2}}.$$

Under the condition $0 \le \gamma_i \le 1 - |\langle\psi_1|\psi_2\rangle|^2$, we can show that (β_1, β_2) should satisfy the inequality constraints in Eq. (16). Because a detailed derivation is too lengthy, we omit the derivation. If we substitute (γ_1, γ_2) into the optimization problem, we can obtain Eq. (16).



$s = 0.05$

$\bar{\eta}$	number of cases that key rate is nonzero	number of cases that key rate is zero
0.75	36323	63677
0.80	57940	42060
0.85	81136	18864
0.90	95974	4026
0.95	99878	122
0.975	100000	0

$s = 0.10$

$\bar{\eta}$	number of cases that key rate is nonzero	number of cases that key rate is zero
0.75	36193	63807
0.80	57776	42224
0.85	80997	19003
0.90	95916	4084
0.95	99854	146
0.98	100000	0

$s = 0.15$

$\bar{\eta}$	number of cases that key rate is nonzero	number of cases that key rate is zero
0.75	36253	63747
0.80	57386	42614
0.85	80801	19199
0.90	95971	4029
0.95	99830	170
0.983	100000	0

Figure 16. The secret key rate between Alice and Charlie when Eve eavesdrops between Alice and Bob and between Bob and Charlie. The solid black line denotes the case where the unitary transformation of Eve is the identity. The green dots display the secret key rate when the unitary transformation of Eve is arbitrary. The table shows the ratio of nonzero secret key rate out of 100000 random cases.

If (γ_1, γ_2) satisfies $\gamma_1 < 0, \gamma_2 > 1 - |\langle\psi_1|\psi_2\rangle|^2$ or $\gamma_1 > 1 - |\langle\psi_1|\psi_2\rangle|^2, \gamma_2 < 0$, then $(\gamma_1, \gamma_2) = (1 - |\langle\psi_1|\psi_2\rangle|^2, 0)$ or $(\gamma_1, \gamma_2) = (0, 1 - |\langle\psi_1|\psi_2\rangle|^2)$ becomes an optimal condition. Substituting it into $P_s^{(\mathrm{B,C,D})}$, we obtain Eq. (20). Although we deals only with the $N = 3$ case, we can use this method for any N.

Optimal success probability of the quantum reproducing strategy. We derive the optimal success probability of the quantum reproducing strategy. To make it simple, we consider the $N = 2$ case. Then, the success probability is expressed as

$$\begin{aligned} P_{rep}^{(\mathrm{B,C})} &= \frac{1}{2}\mathrm{Pr}_{\mathrm{B}}[1|\rho_1]\mathrm{Pr}_{\mathrm{C}}[1|\rho_1] + \frac{1}{2}\mathrm{Pr}_{\mathrm{B}}[2|\rho_2]\mathrm{Pr}_{\mathrm{C}}[2|\rho_2] \\ &= \left\{\frac{1}{2}\mathrm{Pr}_{\mathrm{B}}[1|\rho_1] + \frac{1}{2}\mathrm{Pr}_{\mathrm{B}}[2|\rho_2]\right\} \\ &\quad \times \left\{\frac{\frac{1}{2}\mathrm{Pr}_{\mathrm{B}}[1|\rho_1]}{\frac{1}{2}\mathrm{Pr}_{\mathrm{B}}[1|\rho_1] + \frac{1}{2}\mathrm{Pr}_{\mathrm{B}}[2|\rho_2]}\mathrm{Pr}_{\mathrm{C}}[1|\rho_1]\right. \\ &\quad \left. + \frac{\frac{1}{2}\mathrm{Pr}_{\mathrm{B}}[2|\rho_2]}{\frac{1}{2}\mathrm{Pr}_{\mathrm{B}}[1|\rho_1] + \frac{1}{2}\mathrm{Pr}_{\mathrm{B}}[2|\rho_2]}\mathrm{Pr}_{\mathrm{C}}[2|\rho_2]\right\}. \end{aligned}$$

$\frac{1}{2}\mathrm{Pr}_{\mathrm{B}}[1|\rho_1] + \frac{1}{2}\mathrm{Pr}_{\mathrm{B}}[2|\rho_2]$ only depends on Bob's POVM. When Bob's POVM corresponds to the real vector (α_1, α_2)[21], we obtain optimal success probability from the following optimization problem:

$$\begin{aligned} \text{maximize} \quad & \frac{1}{2}(r\alpha_1 + \bar{r}\bar{\alpha}_1) + \frac{1}{2}(r\alpha_2 + \bar{r}\bar{\alpha}_2) \\ \text{subject to} \quad & (1-\alpha_1)(1-\alpha_2) \geq s^2, \\ & (1-\bar{\alpha}_1)(1-\bar{\alpha}_2) \geq \bar{s}^2. \end{aligned}$$

This optimization problem is partitioned into the following two sub-optimization problem:

$$\begin{aligned} \text{maximize} \quad & \alpha_1 + \alpha_2 \\ \text{subject to} \quad & (1-\alpha_1)(1-\alpha_2) \geq s^2 \\ \text{maximize} \quad & \bar{\alpha}_1 + \bar{\alpha}_2 \\ \text{subject to} \quad & (1-\bar{\alpha}_1)(1-\bar{\alpha}_2) \geq \bar{s}^2 \end{aligned}$$

The optimal solution of the two problems is given as $\alpha_1 = \alpha_2 = 1 - s$ and $\bar{\alpha}_1 = \bar{\alpha}_2 = 1 - \bar{s}$. Hence, we obtain the optimal success probability as $\max\left\{\frac{1}{2}\mathrm{Pr}_{\mathrm{B}}[1|\rho_1] + \frac{1}{2}\mathrm{Pr}_{\mathrm{B}}[2|\rho_2]\right\} = r(1-s) + \bar{r}(1-\bar{s})$. Because $\alpha_1 = \alpha_2$ and $\bar{\alpha}_1 = \bar{\alpha}_2$, $\mathrm{Pr}_{\mathrm{B}}[1|\rho_1] = \mathrm{Pr}_{\mathrm{B}}[2|\rho_2]$ also holds. Therefore, we obtain $\frac{\frac{1}{2}\mathrm{Pr}_{\mathrm{B}}[i \mid \rho_i]}{\frac{1}{2}\mathrm{Pr}_{\mathrm{B}}[1|\rho_1] + \frac{1}{2}\mathrm{Pr}_{\mathrm{B}}[2|\rho_2]} = \frac{1}{2}(\forall\, i)$. This means that Charlie's success probability is also expressed as $\frac{1}{2}\mathrm{Pr}_{\mathrm{C}}[1|\rho_1] + \frac{1}{2}\mathrm{Pr}_{\mathrm{C}}[2|\rho_2]$. In conclusion, the optimal success probability of the quantum reproducing strategy is given as $(r(1-s) + \bar{r}(1-\bar{s}))^2$. Although we consider only the $N = 2$ case, this calculation can be applied to any N.

Derivation of secret key rate in multiparty QKD - Part I: Eve's single trial of eavesdropping. Here, we explain the method to obtain the secret key rate of generalized sequential discrimination. Even though the identical prior probability is used in Result, we consider general prior probabilities given by q_0 and q_1. Then, the entangled state between Alice and Bob is expressed by

$$|\Psi\rangle_{AB} = \sqrt{q_0}|0\rangle_A \otimes |\psi_0\rangle_B + \sqrt{q_1}|1\rangle_A \otimes |\psi_1\rangle_B.$$

The quantum channel $\Lambda_B^{(A\to B)}$ transforms the entangled state $|\Psi\rangle$ as follows:

$$\begin{aligned} \sigma_{AB} &= (\mathrm{id}_A \otimes \Lambda_B^{(A\to B)})(|\Psi\rangle\langle\Psi|_{AB}) \\ &= q_0|0\rangle\langle 0|_A \otimes \left(\eta_{AB}|\psi_0\rangle\langle\psi_0|_B + (1-\eta_{AB})\frac{I_B}{2}\right) \\ &\quad + \sqrt{q_0 q_1}|0\rangle\langle 1|_A \otimes \left(\eta_{AB}|\psi_0\rangle\langle\psi_1|_B + (1-\eta_{AB})\frac{I_B}{2}\right) \\ &\quad + \sqrt{q_0 q_1}|1\rangle\langle 0|_A \otimes \left(\eta_{AB}|\psi_1\rangle\langle\psi_0|_B + (1-\eta_{AB})\frac{I_B}{2}\right) \\ &\quad + q_1|1\rangle\langle 1|_A \otimes \left(\eta_{AB}|\psi_1\rangle\langle\psi_1|_B + (1-\eta_{AB})\frac{I_B}{2}\right) \\ &= \eta_{AB}|\Psi\rangle\langle\Psi|_{AB} + (1-\eta_{AB})|e_+^{(A\to B)}\rangle\langle e_+^{(A\to B)}|_A \otimes \frac{I_B}{2}. \end{aligned}$$

Here, $|e_+^{(A\to B)}\rangle = \sqrt{q_0}|0\rangle + \sqrt{q_1}|1\rangle$. When $q_0 = q_1$, one can have $|e_+^{(A\to B)}\rangle = |+\rangle$. The purification σ_{AB} becomes

$$|\Gamma\rangle_{ABE} = \sqrt{\eta_{AB}}|\Psi\rangle_{AB} \otimes |?\rangle_E + \sqrt{1-\eta_{AB}}|e_+^{(A\to B)}\rangle_A \otimes |\phi_+\rangle_{BE}.$$

Because $|?\rangle$ and $|\phi_+\rangle$ are orthogonal to each other, the relation of $\mathrm{Tr}_E|\Gamma\rangle\langle\Gamma|_{ABE} = \sigma_{AB}$ is obvious. Therefore, two marginal probabilities $P_A(i)$ and $P_E(k)$ are evaluated as follows:

$$
\begin{aligned}
P_A(i) &= \mathrm{Tr}_{ABE}[|\Gamma\rangle\langle\Gamma|_{ABE}|i\rangle\langle i|_A \otimes I_{BE}] \\
&= \mathrm{Tr}_A[\mathrm{Tr}_{BE}(|\Gamma\rangle\langle\Gamma|_{ABE})|i\rangle\langle i|_A] \\
&= \mathrm{Tr}_A[\mathrm{Tr}_B\{\eta_{AB}|\Psi\rangle\langle\Psi|_{AB} \\
&\quad + (1-\eta_{AB})|e_+^{(A\to B)}\rangle\langle e_+^{(A\to B)}| \otimes \frac{I_B}{2}\}|i\rangle\langle i|_A] \\
&= \eta_{AB}q_i + (1-\eta_{AB})|\langle i|e_+^{(A\to B)}\rangle|^2 = q_i, \\
P_E(k) &= \mathrm{Tr}_{ABE}[|\Gamma\rangle\langle\Gamma|_{ABE} I_{AB} \otimes |k\rangle\langle k|_E] \\
&= \mathrm{Tr}_E[\mathrm{Tr}_{AB}\{|\Gamma\rangle\langle\Gamma|_{ABE}\}|k\rangle\langle k|_E] \\
&= (1-\eta_{AB})\left\langle k\left|\frac{I_E}{2}\right|k\right\rangle \\
&= (1-\eta_{AB})\frac{1}{2}\langle k|k\rangle = \frac{1-\eta_{AB}}{2}.
\end{aligned}
$$

To evaluate the marginal probabilities $P_{AB}(i, j)$ and $P_{BE}(j, k)$, we should use POVM element M_i of Bob. Using the condition of overlap $s = \langle\psi_0|\psi_1\rangle$ in two pure states of Alice, we can construct an explicit form of the two pure states as follows:

$$
|\psi_0\rangle = \sqrt{\frac{1+s}{2}}|0\rangle + \sqrt{\frac{1-s}{2}}|1\rangle,\ |\psi_1\rangle = \sqrt{\frac{1+s}{2}}|0\rangle - \sqrt{\frac{1-s}{2}}|1\rangle.
$$

The POVM element of Bob can be given as $\alpha_i|\alpha_i\rangle\langle\alpha_i|$[12], where $|\alpha_0\rangle$ and $|\alpha_1\rangle$ are expressed as follows:

$$
|\alpha_0\rangle = \frac{1}{\sqrt{2(1+s)}}|0\rangle + \frac{1}{\sqrt{2(1-s)}}|1\rangle,\ |\alpha_1\rangle = \frac{1}{\sqrt{2(1+s)}}|0\rangle - \frac{1}{\sqrt{2(1-s)}}|1\rangle. \tag{42}
$$

The state $|\alpha_i\rangle$ satisfies the following relations: (i) $\langle\alpha_i|\alpha_i\rangle = 1/(1-s^2)$, (ii) $|\langle k|\alpha_j\rangle| = 1/\sqrt{2\{1+(-1)^k s\}}$. Using these relations, the marginal probabilities $P_{AB}(i, j)$ and $P_{BE}(j, k)$ can be evaluated as

$$
\begin{aligned}
P_{AB}(i,j) &= \mathrm{Tr}_{ABE}\Big[|\Gamma\rangle\langle\Gamma|_{ABE}|i\rangle\langle i|_A \otimes M_j \otimes I_E\Big] \\
&= \mathrm{Tr}_{AB}\Big[\mathrm{Tr}_E\{|\Gamma\rangle\langle\Gamma|_{ABE}\}\}|i\rangle\langle i|_A \otimes M_j\Big] \\
&= \mathrm{Tr}_{AB}\left[\left\{\eta_{AB}|\Psi\rangle\langle\Psi|_{AB} + (1-\eta_{AB})|e_+^{(A\to B)}\rangle\langle e_+^{(A\to B)}| \otimes \frac{I_B}{2}\right\}|i\rangle\langle i|_A \otimes M_j\right] \\
&= \eta_{AB}\langle\Psi|(|i\rangle\langle i|_A \otimes M_j)|\Psi\rangle + (1-\eta_{AB})|\langle i|e_+^{(A\to B)}\rangle|^2\frac{1}{2}\mathrm{Tr}_B M_j \\
&= \eta_{AB}\langle\Psi|(|i\rangle\langle i|_A \otimes M_j)|\Psi\rangle + (1-\eta_{AB})|\langle i|e_+^{(A\to B)}\rangle|^2\frac{\alpha_j}{2}\langle\alpha_j|\alpha_j\rangle \\
&= \eta_{AB}q_i\alpha_i\delta_{ij} + (1-\eta_{AB})q_i\frac{\alpha_j}{2(1-s^2)}, \\
P_{BE}(j,k) &= \mathrm{Tr}_{ABE}[|\Gamma\rangle\langle\Gamma|_{ABE} I_A \otimes M_j \otimes |k\rangle\langle k|_E] \\
&= \mathrm{Tr}_{BE}[\mathrm{Tr}_A\{|\Gamma\rangle\langle\Gamma|_{ABE}\}M_j \otimes |k\rangle\langle k|_E] \\
&= \frac{1}{2}(1-\eta_{AB})\langle k|M_j|k\rangle \\
&= \frac{1-\eta_{AB}}{2}\alpha_j|\langle k|\alpha_j\rangle|^2 \\
&= \frac{(1-\eta_{AB})\alpha_j}{4\{1+(-1)^k s\}}.
\end{aligned}
$$

We can see that when $q_0 = q_1$, four marginal probabilities are given by Eq. (38).
When Bob eliminates an inconclusive result, the measurement of Bob provides the following ensemble:

$$
\begin{aligned}
&\frac{I_A \otimes K_0|\Psi\rangle\langle\Psi|_{AB}I_A \otimes K_0^\dagger + I_A \otimes K_1|\Psi\rangle\langle\Psi|_{AB}I_A \otimes K_1^\dagger}{\mathrm{Tr}\{I_A \otimes K_0|\Psi\rangle\langle\Psi|_{AB}I_A \otimes K_0^\dagger + I_A \otimes K_1|\Psi\rangle\langle\Psi|_{AB}I_A \otimes K_1^\dagger\}} \\
&= \frac{q_0\alpha_0}{q_0\alpha_0 + q_1\alpha_1}|0\rangle\langle 0|_A \otimes |\phi_0^{(B)}\rangle\langle\phi_0^{(B)}|_C \\
&\quad + \frac{q_1\alpha_1}{q_0\alpha_0 + q_1\alpha_1}|1\rangle\langle 1|_A \otimes |\phi_1^{(B)}\rangle\langle\phi_1^{(B)}|_C.
\end{aligned}
$$

Here, $K_i = \sqrt{\alpha_i}|\phi_i^{(B)}\rangle_C\langle\alpha_i|_B$ is a linear map of $\mathscr{H}_B \to \mathscr{H}_C$. The quantum state between Alice and Charlie becomes the following entangled state

$$\begin{aligned}|\Phi^{(B)}\rangle_{AB} &= \sqrt{\frac{q_0\alpha_0}{q_0\alpha_0+q_1\alpha_1}}|0\rangle_A \otimes |\phi_0^{(B)}\rangle_C + \sqrt{\frac{q_1\alpha_1}{q_0\alpha_0+q_1\alpha_1}}|1\rangle_A \otimes |\phi_1^{(B)}\rangle_C \\ &= \sqrt{Q_0^{(B)}}|0\rangle_A \otimes |\phi_0^{(B)}\rangle_C + \sqrt{Q_1^{(B)}}|1\rangle_A \otimes |\phi_1^{(B)}\rangle_C.\end{aligned}$$

When $q_0 = q_1$, the optimal condition is given by $\alpha_0 = \alpha_1 = 1 - s^{1/N}$. Therefore, we can find $Q_0^{(B)} = Q_1^{(B)}$.

Two post-measurement states $|\phi_0^{(B)}\rangle$ and $|\phi_1^{(B)}\rangle$ satisfies the overlap condition $s' = \langle\phi_0^{(B)}|\phi_1^{(B)}\rangle = s/\sqrt{(1-\alpha_0)(1-\alpha_1)}$ and the explicit forms of $|\phi_0^{(B)}\rangle$ and $|\phi_1^{(B)}\rangle$ become

$$|\phi_0^{(B)}\rangle = \sqrt{\frac{1+s'}{2}}|0\rangle + \sqrt{\frac{1-s'}{2}}|1\rangle,\ |\phi_1^{(B)}\rangle = \sqrt{\frac{1+s'}{2}}|0\rangle - \sqrt{\frac{1-s'}{2}}|1\rangle.$$

The POVM element of Charlie is given by $\beta_i|\beta_i\rangle\langle\beta_i|$, where $|\beta_0\rangle$ and $|\beta_1\rangle$ are expressed by

$$|\beta_0\rangle = \frac{1}{\sqrt{2(1+s')}}|0\rangle + \frac{1}{\sqrt{2(1-s')}}|1\rangle,\ |\beta_1\rangle = \frac{1}{\sqrt{2(1+s')}}|0\rangle - \frac{1}{\sqrt{2(1-s')}}|1\rangle. \tag{43}$$

We can see the relation of $\langle\phi_i^{(B)}|\alpha_j\rangle = \delta_{ij}$ from Eq. (43). Substituting Eq. (43) into the marginal probabilities, we can obtain P_{AC} and P_{CE}. Especially, when $q_0 = q_1$, from $\alpha_0 = \alpha_1 = 1 - s^{1/N}$, one can obtain $s' = s^{(N-1)/N}$. Using the similar method, for arbitrary X, we can find P_{AX} and P_{XE}.

Derivation of secret key rate in multiparty QKD - Part II: Eve's multi-trial of eavesdropping. Here, we show how to evaluate the secret key rate of the case where Eve performs eavesdropping between Alice and Bob and between Bob and Charlie. Here, prior probabilities q_0 and q_1 are considered to be arbitrary values. Suppose that Eve performs eavesdropping between Alice and Bob, using a quantum memory E_B. Then, Alice, Bob, and Eve share the following quantum state:

$$|\Gamma\rangle_{ABE_B} = \sqrt{\eta_{AB}}|\Psi\rangle_{AB} \otimes |?\,\rangle_{E_B} + \sqrt{1-\eta_{AB}}|e_+^{(A\to B)}\rangle_A \otimes |\phi_+\rangle_{BE_B}.$$

Let us assume that the Kraus operator of Bob is given as $\{K_0^{(B)}, K_1^{(B)}, K_?^{(B)}\}$. Then, Kraus operator $K_0^{(B)}$, $K_1^{(B)}$ transforms $|\Gamma\rangle_{ABE_B}$ as follows:

$$\begin{aligned}I_A \otimes K_0^{(B)} \otimes I_{E_B}|\Gamma\rangle_{ABE_B} &= \left\{\sqrt{\eta_{AB}q_0\alpha_0}|0\rangle_A \otimes |?\,\rangle_{E_B}\right. \\ &\quad \left. + \sqrt{\frac{(1-\eta_{AB})\alpha_0}{2}}|e_+^{(A\to B)}\rangle_A \otimes |\alpha_0\rangle_{E_B}\right\} \otimes |\phi_0^{(B)}\rangle_C \\ &= |\mathcal{E}_0\rangle_{AE_B} \otimes |\phi_0^{(B)}\rangle_C, \\ I_A \otimes K_1^{(B)} \otimes I_{E_B}|\Gamma\rangle_{ABE_B} &= \left\{\sqrt{\eta_{AB}q_1\alpha_1}|1\rangle_A \otimes |?\,\rangle_{E_B}\right. \\ &\quad \left. + \sqrt{\frac{(1-\eta_{AB})\alpha_1}{2}}|e_+^{(A\to B)}\rangle_A \otimes |\alpha_1\rangle_{E_B}\right\} \otimes |\phi_1^{(B)}\rangle_C \\ &= |\mathcal{E}_1\rangle_{AE_B} \otimes |\phi_1^{(B)}\rangle_C.\end{aligned}$$

When $\eta_{AB} = 1$, we have $|\mathcal{E}_i\rangle = \sqrt{q_i\alpha_i}|i\rangle_A \otimes |?\,\rangle_{E_B}$. Therefore, the argument of this case is identical to the security analysis of Part I.

After Bob performs a post-processing, $|\Gamma\rangle_{ABE_B}$ becomes the following tripartite state:

$$\begin{aligned}\sigma_{ACE_B} &= \frac{I_A \otimes K_0^{(B)} \otimes I_{E_B}|\Gamma\rangle\langle\Gamma|I_A \otimes K_0^{(B)\dagger} \otimes I_{E_B} + I_A \otimes K_1^{(B)} \otimes I_{E_B}|\Gamma\rangle\langle\Gamma|I_A \otimes K_1^{(B)\dagger} \otimes I_{E_B}}{(\langle\Gamma|I_A \otimes K_0^{(B)\dagger} \otimes I_{E_B})(I_A \otimes K_0^{(B)} \otimes I_{E_B}|\Gamma\rangle) + (\langle\Gamma|I_A \otimes K_1^{(B)\dagger} \otimes I_{E_B})(I_A \otimes K_1^{(B)} \otimes I_{E_B}|\Gamma\rangle)} \\ &= \mathcal{N}(\eta_{AB})\{|\mathcal{E}_0\rangle\langle\mathcal{E}_0|_{AE_B} \otimes |\phi_0^{(B)}\rangle\langle\phi_0^{(B)}|_C + |\mathcal{E}_1\rangle\langle\mathcal{E}_1|_{AE_B} \otimes |\phi_1^{(B)}\rangle\langle\phi_1^{(B)}|_C\}.\end{aligned}$$

When Eve performs eavesdropping between Bob and Charlie, σ_{ACE_B} becomes

$$\mathrm{id}_{AE_B} \otimes \Lambda_C^{(B\to C)}(\sigma_{ACE_B}) = \eta_{BC}\sigma_{ACE_B} + (1-\eta_{BC})\tau_{ACE_B}.$$

Here, τ_{ACE_B} is expressed by

$$\tau_{ACE_B} = \mathcal{N}(\eta_{AB})\{|\mathcal{E}_0\rangle\langle\mathcal{E}_0|_{AE_B} + |\mathcal{E}_1\rangle\langle\mathcal{E}_1|_{AE_B}\} \otimes \frac{I_C}{2}.$$

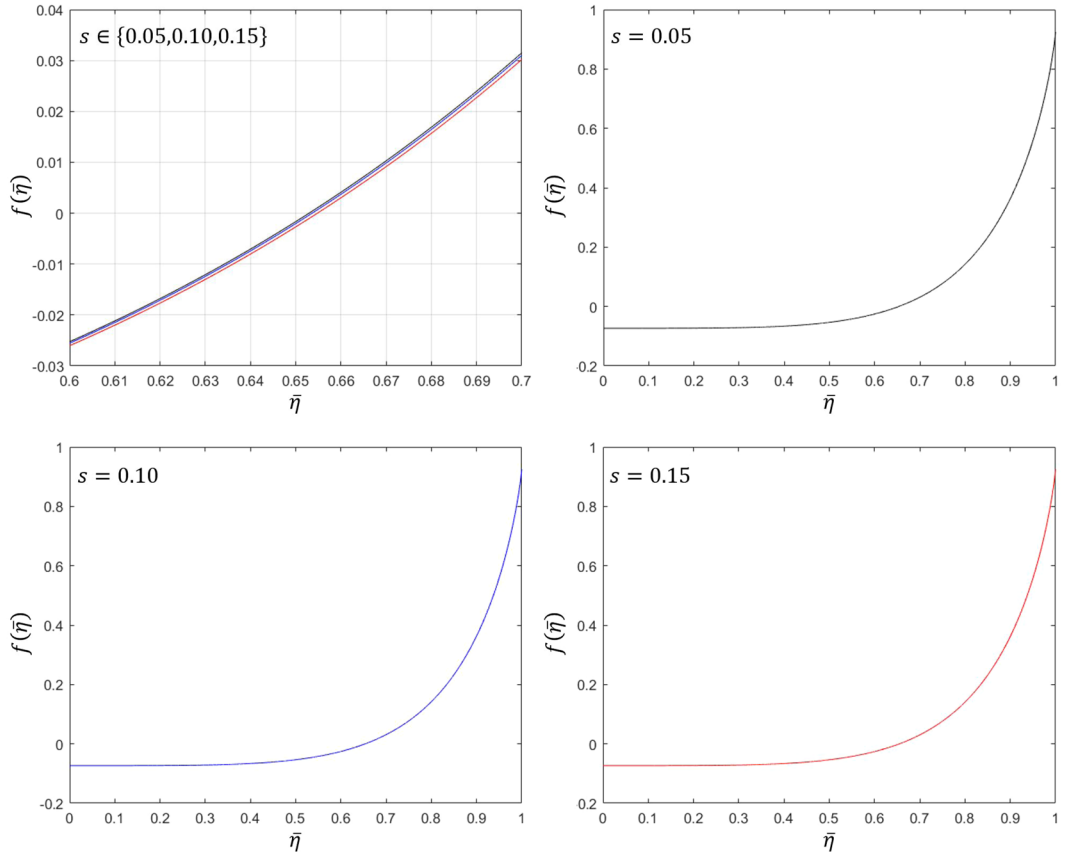


Figure 17. The graph of $f(\bar{\eta})$. In these graphs, the solid black line, the solid blue line, and the solid red line denote the cases of $s = 0.05,\ 0.10$, and 0.15, respectively. These graphs show that $f(\bar{\eta})$ is a monotonically increasing function of $\bar{\eta}$. Because $\bar{\eta}$ is a noise strength of channel, these graphs tell that noise of channel can make a bad influence on the secret key rate.

Let us denote the purifications of $\eta_{BC}\sigma_{ACE_B}$ and $(1-\eta_{BC})\tau_{ACE_B}$ as $|\eta_{BC}\sigma_{ACE_B}\rangle_{ACE_BE_C}$ and $|(1-\eta_{BC})\tau_{ACE_B}\rangle_{ACE_BE_C}$, respectively. Here, E_C is the quantum system of Eve which operates between Bob and Charlie. If $|\eta_{BC}\sigma_{ACE_B}\rangle_{ACE_BE_C}$ and $|(1-\eta_{BC})\tau_{ACE_B}\rangle_{ACE_BE_C}$ are orthogonal to each other, the following equality holds:

$$\begin{aligned}&\mathrm{Tr}_{E_C}(|\eta_{BC}\sigma_{ACE_B}\rangle + |(1-\eta_{BC})\tau_{ACE_B}\rangle)(\langle\eta_{BC}\sigma_{ACE_B}| + \langle(1-\eta_{BC})\tau_{ACE_B}|)_{ACE_BE_C}\\ &= \eta_{BC}\sigma_{ACE_B} + (1-\eta_{BC})\tau_{ACE_B}.\end{aligned}$$

Using $\{|?_0\rangle, |?_1\rangle, |00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ which consists of orthogonal basis of E_C, we can construct purification of $\mathrm{id}_{AE_B} \otimes \Lambda_C^{(B\to C)}(\sigma_{ACE_B})$. First, $|\eta_{BC}\sigma_{ABE_B}\rangle$ can be constructed by the basis $|?_0\rangle, |?_1\rangle$. Second, $|(1-\eta_{AB})\tau_{ACE_B}\rangle$ can be constructed by $|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Then, $|\eta_{BC}\sigma_{ACE_B}\rangle$ and $|(1-\eta_{BC})\tau_{ACE_B}\rangle$ are orthogonal to each other. In conclusion, the purification of $\mathrm{id}_{AE_B} \otimes \Lambda_C^{(B\to C)}(\sigma_{ACE_B})$ can be given as follows:

$$\begin{aligned}|\Gamma\rangle_{ACE_BE_C} &= |\eta_{BC}\sigma_{ACE_B}\rangle + |(1-\eta_{BC})\tau_{ACE_B}\rangle\\ &= \sqrt{\mathcal{N}(\eta_{AB})}\Big[\sqrt{\eta_{BC}}\Big\{|\mathcal{E}_0\rangle_{AE_B}\otimes|\phi_0^{(B)}\rangle_C\otimes|?_0\rangle_{E_C}\\ &\quad + |\mathcal{E}_1\rangle_{AE_B}\otimes|\phi_1^{(B)}\rangle_C\otimes|?_1\rangle_{E_C}\Big\}\\ &\quad + \sqrt{1-\eta_{BC}}|e_+^{(A\to B\to C)}\rangle_{AE_BE_{C2}}\otimes|\phi_+\rangle_{CE_{C1}}\Big].\end{aligned}$$

Here, $|\phi_+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, $|e_+^{(A\to B\to C)}\rangle = |0\rangle\otimes|\mathcal{E}_0\rangle + |1\rangle\otimes|\mathcal{E}_1\rangle$.

To evaluate the secret key rate between Alice and Charlie, one must obtain the marginal probabilities P_A, P_C, P_{CA}, P_{CE}. First, $P_A(i)$ can be evaluated as follows:

$$
\begin{aligned}
P_A(i) &= \mathrm{Tr}[|i\rangle\langle i|_A \otimes I_{CE_BE_C}|\Gamma\rangle\langle\Gamma|_{ACE_BE_C}] \\
&= \mathcal{N}(\eta_{AB})\underbrace{\left[\eta_{AB}\alpha_0 + \frac{(1-\eta_{AB})(\alpha_0+\alpha_1)}{2(1-s^2)}\right]}_{\mathcal{N}_0(\eta_{AB})} q_0\delta_{i0} \\
&\quad + \mathcal{N}(\eta_{AB})\underbrace{\left[\eta_{AB}\alpha_1 + \frac{(1-\eta_{AB})(\alpha_0+\alpha_1)}{2(1-s^2)}\right]}_{\mathcal{N}_1(\eta_{AB})} q_1\delta_{i1}.
\end{aligned}
$$

Because of $\mathcal{N}(\eta_{AB}) = [\mathcal{N}_0(\eta_{AB}) + \mathcal{N}_1(\eta_{AB})]^{-1}$, $P_A(i)$ is expressed as

$$
P_A(i) = \frac{\mathcal{N}_0(\eta_{AB})}{\mathcal{N}_0(\eta_{AB}) + \mathcal{N}_1(\eta_{AB})}\delta_{i0} + \frac{\mathcal{N}_1(\eta_{AB})}{\mathcal{N}_0(\eta_{AB}) + \mathcal{N}_1(\eta_{AB})}\delta_{i1}.
$$

That is, $P_A(i)$ is a prior probability after Eve's eavesdropping and Bob's measurement. Specially, when $\eta_{AB} = 1$, $P_A(i)$ is given as follows:

$$
\begin{aligned}
P_A(i) &= \frac{q_0\alpha_0}{q_0\alpha_0 + q_1\alpha_1}\delta_{i0} + \frac{q_1\alpha_1}{q_0\alpha_0 + q_1\alpha_1}\delta_{i1} \\
&= \frac{q_0\langle\psi_0|M_0^{(B)}|\psi_0\rangle}{q_0\langle\psi_0|M_0^{(B)}|\psi_0\rangle + q_1\langle\psi_1|M_1^{(B)}|\psi_1\rangle}\delta_{i0} \\
&\quad + \frac{q_1\langle\psi_1|M_1^{(B)}|\psi_1\rangle}{q_0\langle\psi_0|M_0^{(B)}|\psi_0\rangle + q_1\langle\psi_1|M_1^{(B)}|\psi_1\rangle}\delta_{i1}.
\end{aligned}
$$

Second, $P_E = P_{E_BE_C}(l, (m, n))$ is evaluated as follows:

$$
\begin{aligned}
P_{E_BE_C}(l, (m, n)) &= \mathrm{Tr}[I_A \otimes |l\rangle\langle l|_{E_B} \otimes |mn\rangle\langle mn|_{E_C}|\Gamma\rangle\langle\Gamma|] \\
&= \mathrm{Tr}_{E_BE_C}[|l\rangle\langle l|_{E_B} \otimes |mn\rangle\langle mn|_{E_C}\mathrm{Tr}_{AC}|\Gamma\rangle\langle\Gamma|].
\end{aligned}
$$

Here, $\mathrm{Tr}_{AC}|\Gamma\rangle\langle\Gamma|_{ACE_BE_C}$ is given by

$$
\begin{aligned}
\mathrm{Tr}_{AC}|\Gamma\rangle\langle\Gamma|_{ACE_BE_C} &= \frac{1-\eta_{BC}}{2}\mathcal{N}(\eta_{AB})\Big[\mathrm{Tr}_A|\mathcal{E}_0\rangle\langle\mathcal{E}_0|_{AE_B} \otimes |0\rangle\langle 0|_{E_{C2}} \\
&\quad + \mathrm{Tr}_A|\mathcal{E}_0\rangle\langle\mathcal{E}_1|_{AE_B} \otimes |0\rangle\langle 1|_{E_{C2}} \\
&\quad + \mathrm{Tr}_A|\mathcal{E}_1\rangle\langle\mathcal{E}_0|_{AE_B} \otimes |1\rangle\langle 0|_{E_{C2}} \\
&\quad + \mathrm{Tr}_A|\mathcal{E}_1\rangle\langle\mathcal{E}_1|_{AE_B} \otimes |1\rangle\langle 1|_{E_{C2}} + \Omega(|?_0\rangle, |?_1\rangle)\Big] \otimes \frac{I_{E_{C1}}}{2}.
\end{aligned}
$$

Here, $\Omega(|?_0\rangle, |?_1\rangle)$ is an operator containing $|?_0\rangle_{E_C}$, $|?_1\rangle_{E_C}$. Therefore, in $\forall\, l, m, n \in \{0, 1\}$, we obtain $\langle lmn|I_{E_{C1}} \otimes \Omega(|?_0\rangle, |?_1\rangle)|lmn\rangle = 0$. Then, P_E becomes

$$
\begin{aligned}
&P_{E_BE_C}(l, (m, n)) \\
&= \frac{(1-\eta_{BC})\mathcal{N}(\eta_{AB})}{2}\mathrm{Tr}_{E_BE_C}\Big[|l\rangle\langle l|_{E_B} \otimes |mn\rangle\langle mn|_{E_C} \\
&\quad \times \Big\{\mathrm{Tr}_A|\mathcal{E}_0\rangle\langle\mathcal{E}_0|_{AE_B} \otimes |0\rangle\langle 0|_{E_{C2}} \\
&\quad + \mathrm{Tr}_A|\mathcal{E}_0\rangle\langle\mathcal{E}_1|_{AE_B} \otimes |0\rangle\langle 1|_{E_{C2}} \\
&\quad + \mathrm{Tr}_A|\mathcal{E}_1\rangle\langle\mathcal{E}_0|_{AE_B} \otimes |1\rangle\langle 0|_{E_{C2}} \\
&\quad + \mathrm{Tr}_A|\mathcal{E}_1\rangle\langle\mathcal{E}_1|_{AE_B} \otimes |1\rangle\langle 1|_{E_{C2}}\Big\} \otimes \frac{I_{E_{C1}}}{2}\Big] \\
&= \frac{(1-\eta_{BC})(1-\eta_{AB})\alpha_0}{4\{1 + (-1)^l s\}}\mathcal{N}(\eta_{AB})\delta_{n0} \\
&\quad + \frac{(1-\eta_{BC})(1-\eta_{AB})\alpha_1}{4\{1 + (-1)^l s\}}\mathcal{N}(\eta_{AB})\delta_{n1}.
\end{aligned}
$$

Third, the marginal probability $P_{AC}(i, j)$ is evaluated as follows:

$$\begin{aligned} P_{AC}(i,j) &= \mathrm{Tr}[|i\rangle\langle i|_A \otimes \beta_j|\beta_j\rangle\langle\beta_j|_C \otimes I_{E_BE_C}|\Gamma\rangle\langle\Gamma|] \\ &= \mathrm{Tr}_{AC}[|i\rangle\langle i|_A \otimes \beta_j|\beta_j\rangle\langle\beta_j|_C \mathrm{Tr}_{E_BE_C}|\Gamma\rangle\langle\Gamma|]. \end{aligned}$$

Here, $\mathrm{Tr}_{E_BE_C}|\Gamma\rangle\langle\Gamma|$ is given by

$$\begin{aligned} \mathrm{Tr}_{E_BE_C}|\Gamma\rangle\langle\Gamma|_{ACE_BE_C} &= \eta_{BC}\mathcal{N}(\eta_{AB})[\{\eta_{AB}q_0\alpha_0|0\rangle\langle 0|_A \\ &\quad + \frac{(1-\eta_{AB})\alpha_0}{2(1-s^2)}|e_+^{(A\to B)}\rangle\langle e_+^{(A\to B)}|_A\Big\} \otimes |\phi_0^{(B)}\rangle\langle\phi_0^{(B)}|_C \\ &\quad + \{\eta_{AB}q_1\alpha_1|1\rangle\langle 1|_A \\ &\quad + \frac{(1-\eta_{AB})\alpha_1}{2(1-s^2)}|e_+^{(A\to B)}\rangle\langle e_+^{(A\to B)}|_A\Big\} \otimes |\phi_1^{(B)}\rangle\langle\phi_1^{(B)}|_C\Big] \\ &\quad + (1-\eta_{BC})\mathcal{N}(\eta_{AB})\{\eta_{AB}q_0\alpha_0|0\rangle\langle 0|_A + \eta_{AB}q_0\alpha_1|1\rangle\langle 1|_A \\ &\quad + \frac{(1-\eta_{AB})(\alpha_0+\alpha_1)}{2(1-s^2)}|e_+^{(A\to B)}\rangle\langle e_+^{(A\to B)}|_A\Big\} \otimes \frac{I_C}{2}. \end{aligned}$$

Then, $P_{AC}(i,j)$ is expressed as follows:

$$\begin{aligned} P_{AC}(i,j) &= \eta_{BC}\mathcal{N}(\eta_{AB})\frac{\beta_j}{1-s'^2}\Big\{\eta_{AB}q_j\alpha_j\delta_{ij} \\ &\quad + \frac{(1-\eta_{AB})\alpha_j}{2(1-s^2)}(q_0\delta_{i0}+q_1\delta_{i1})\Big\} \\ &\quad + (1-\eta_{BC})\mathcal{N}(\eta_{AB})\frac{\beta_j}{1-s'^2}\{\eta_{AB}q_0\alpha_0\delta_{i0} \\ &\quad + \eta_{AB}q_1\alpha_1\delta_{i1} + \frac{(1-\eta_{AB})(\alpha_0+\alpha_1)}{2(1-s^2)}(q_0\delta_{i0}+q_1\delta_{i1})\Big\}. \end{aligned}$$

Here, s' is an overlap between the post-measurement states of Bob $|\phi_0^{(B)}\rangle$ and $|\phi_1^{(B)}\rangle$.
Fourth, to obtain $P_E(p)$, we can evaluate $I_{AC} \otimes \langle\pi_p|_{E_BE_C}|\Gamma\rangle_{ACE_BE_C}$ as follows:

$$\begin{aligned} &(I_{AC} \otimes \langle\pi_p|_{E_BE_C})|\Gamma\rangle_{ACE_BE_C} \\ &= \Big\{I_{AC} \otimes \sum_{q=1}^{18} V_{pq}^*\langle q|_{E_BE_C}\Big\}|\Gamma\rangle_{ACE_BE_C} \\ &= \sqrt{\eta_{BC}\mathcal{N}(\eta_{AB})}\Big\{\lambda_0 V_{p1}^*|0\rangle_A \otimes |\phi_0^{(B)}\rangle_C \\ &\quad + \mu_0 V_{p7}^*|e_+^{(A\to B)}\rangle_A \otimes |\phi_0^{(B)}\rangle_C \\ &\quad + \nu_0 V_{p13}^*|e_+^{(A\to B)}\rangle_A \otimes |\phi_0^{(B)}\rangle_C \\ &\quad + \lambda_1 V_{p2}^*|1\rangle_A \otimes |\phi_1^{(B)}\rangle_C + \mu_1 V_{p8}^*|e_+^{(A\to B)}\rangle_A \otimes |\phi_1^{(B)}\rangle_C \\ &\quad + \nu_1 V_{p14}^*|e_+^{(A\to B)}\rangle_A \otimes |\phi_1^{(B)}\rangle_C\Big\} \\ &\quad + \sqrt{\frac{(1-\eta_{BC})\mathcal{N}(\eta_{AB})}{2}}\Big\{\lambda_0 V_{p3}^*|0\rangle_A \otimes |0\rangle_C \\ &\quad + \mu_0 V_{p9}^*|e_+^{(A\to B)}\rangle_A \otimes |0\rangle_C \\ &\quad + \nu_0 V_{p15}^*|e_+^{(A\to B)}\rangle_A \otimes |0\rangle_C \\ &\quad + \lambda_1 V_{p4}^*|1\rangle_A \otimes |0\rangle_C + \mu_1 V_{p10}^*|e_+^{(A\to B)}\rangle_A \otimes |0\rangle_C \\ &\quad + \nu_1 V_{p16}^*|e_+^{(A\to B)}\rangle_A \otimes |0\rangle_C \\ &\quad + \lambda_0 V_{p5}^*|0\rangle_A \otimes |1\rangle_C + \mu_0 V_{p11}^*|e_+^{(A\to B)}\rangle_A \otimes |1\rangle_C \\ &\quad + \nu_0 V_{p17}^*|e_+^{(A\to B)}\rangle_A \otimes |1\rangle_C \\ &\quad + \lambda_1 V_{p6}^*|1\rangle_A \otimes |1\rangle_C + \mu_1 V_{p12}^*|e_+^{(A\to B)}\rangle_A \otimes |1\rangle_C \\ &\quad + \nu_1 V_{p18}^*|e_+^{(A\to B)}\rangle_A \otimes |1\rangle_C\Big\}. \end{aligned} \tag{44}$$

Finally, to obtain $P_{CE}(k,p)$, we can evaluate $I_A \otimes \langle\beta_k|_C \otimes \langle\pi_p|_{E_BE_C}|\Gamma\rangle_{ACE_BE_C}$ as follows:

$$
\begin{aligned}
&(I_A \otimes \langle\beta_k|_C \otimes \langle\pi_p|_{E_B E_C})|\Gamma\rangle_{ACE_B E_C} \\
&= \left\{ I_A \otimes \langle\beta_k|_C \otimes \sum_{q=1}^{18} V^*_{pq} \langle q|_{E_B E_C} \right\} |\Gamma\rangle_{ACE_B E_C} \\
&= \sqrt{\eta_{BC}\mathcal{N}(\eta_{AB})} \Big\{ \lambda_0 V^*_{p1} \delta_{k0} |0\rangle_A \\
&\quad + \mu_0 V^*_{p7} \delta_{k0} |e_+^{(A\to B)}\rangle_A + \nu_0 V^*_{p13} \delta_{k0} |e_+^{(A\to B)}\rangle_A \\
&\quad + \lambda_1 V^*_{p2} \delta_{k1} |1\rangle_A + \mu_1 V^*_{p8} \delta_{k1} |e_+^{(A\to B)}\rangle_A \\
&\quad + \nu_1 V^*_{p14} \delta_{k0} |e_+^{(A\to B)}\rangle_A \Big\} \\
&\quad + \sqrt{\frac{(1-\eta_{BC})\mathcal{N}(\eta_{AB})}{2}} \Big\{ \lambda_0 V^*_{p3} \sqrt{\frac{1+s'}{2}} |0\rangle_A \\
&\quad + \mu_0 V^*_{p9} \sqrt{\frac{1+s'}{2}} |e_+^{(A\to B)}\rangle_A + \nu_0 V^*_{p15} \sqrt{\frac{1+s'}{2}} |e_+^{(A\to B)}\rangle_A \\
&\quad + \lambda_1 V^*_{p4} \sqrt{\frac{1+s'}{2}} |1\rangle_A + \mu_1 V^*_{p10} \sqrt{\frac{1+s'}{2}} |e_+^{(A\to B)}\rangle_A \\
&\quad + \nu_1 V^*_{p16} \sqrt{\frac{1+s'}{2}} |e_+^{(A\to B)}\rangle_A \\
&\quad + \lambda_0 V^*_{p5} (-1)^k \sqrt{\frac{1-s'}{2}} |0\rangle_A + \mu_0 V^*_{p11} (-1)^k \sqrt{\frac{1-s'}{2}} |e_+^{(A\to B)}\rangle_A \\
&\quad + \nu_0 V^*_{p17} (-1)^k \sqrt{\frac{1-s'}{2}} |e_+^{(A\to B)}\rangle_A \\
&\quad + \lambda_1 V^*_{p6} (-1)^k \sqrt{\frac{1-s'}{2}} |1\rangle_A \\
&\quad + \mu_1 V^*_{p12} (-1)^k \sqrt{\frac{1-s'}{2}} |e_+^{(A\to B)}\rangle_A \\
&\quad + \nu_1 V^*_{p18} (-1)^k \sqrt{\frac{1-s'}{2}} |e_+^{(A\to B)}\rangle_A \Big\}.
\end{aligned} \tag{45}
$$

In Eqs. (44) and (45), δ_{ij} is Kronecker delta. And, λ_i, μ_i, and ν_i are defined as follows:

$$
\lambda_i = \sqrt{\eta_{AB} q_i \alpha_i}, \quad \mu_i = \frac{1}{2}\sqrt{\frac{(1-\eta_{AB})\alpha_i}{1+s}}, \quad \nu_i = \frac{1}{2}\sqrt{\frac{(1-\eta_{AB})\alpha_i}{1-s}}.
$$

Simulation method to search for critical channel efficiency ($\bar{\eta}_{crit}$). When the unitary transformation V and overlap s are determined, the secret key rate is expressed as follows:

$$
K_{AC:E_B E_C} = \max\{0, f(\bar{\eta})\}.
$$

Here, $f(\eta) = I(A\colon C) - I(C\colon E)$ is a function of the single variable $\bar{\eta}$. In Fig. 17, when V is an identity and $s \in \{0.05,\ 0.10,\ 0.15\}$, $f(\bar{\eta})$ is a monotonically increasing function. Therefore, in the region of $\bar{\eta} \in [0,\ 1]$, there is only one value of $\bar{\eta}_{crit}$ satisfying $f(\bar{\eta}_{crit}) = 0$. And, if $\bar{\eta} > \bar{\eta}_{crit}$, because of $f(\bar{\eta}) > 0$, the secret key rate becomes nonzero. In this case, $\bar{\eta}_{crit}$ can be obtained by a bisection method[49].

Received: 13 August 2019; Accepted: 24 March 2020;
Published online: 19 May 2020

References

1. Helstrom, C. W. *Quantum Detection and Estimation Theory* (Academic Press, 1976).
2. Holevo, A. S. *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, 1979).
3. Bae, J. & Kwek, L. C. Quantum stte discrimination and its applications. *J. Phys. A: Math. Theor.* **48**, 083001 (2015).
4. Ha, D. & Kwon, Y. Complete analysis for three-qubit mixed-state discrimination. *Phys. Rev. A* **87**, 062302 (2013).
5. Ha, D. & Kwon, Y. Discriminating *N*–qudit states using geometric structure. *Phys. Rev. A* **90**, 022330 (2014).
6. Chefles, A. Unambiguous discrimination between linearly independent quantum states. *Phys. Lett. A* **239**, 339 (1998).
7. Rudolph, T., Spekkens, R. W. & Turner, P. S. Unambiguous discrimination of mixed states. *Phys. Rev. A* **68**, 010301(R) (2003).
8. Ivanovic, I. D. How to diferentiate non-orthogonal states. *Phys. Lett. A* **123**, 257 (1987).
9. Dieks, D. Overlaps and distinguishability of quantum states. *Phys. Lett. A* **126**, 303 (1988).
10. Peres, A. How to diferentiate non-orthogonal states. *Phys. Lett. A* **126**, 303 (1988).
11. Jaeger, G. & Shimony, A. Optimal distinction between two non-orthogonal quantum states. *Phys. Lett. A* **197**, 83 (1995).
12. Ha, D. & Kwon, Y. Analysis of optimal unambiguous discrimination of three pure quantum states. *Phys. Rev. A* **91**, 062312 (2015).
13. Croke, S., Andersson, E., Barnett, S. M., Gilson, C. R. & Jefers, J. Maximal Confdence Quantum Measurement. *Phys. Rev. Lett.* **96**, 070401 (2006).
14. Touzel, M. A. P., Adamson, R. B. A. & Steinberg, A. M. Optimal bounded-error strategies for projective measurements in nonorthogonal state discrimination. *Phys. Rev. A* **76**, 062314 (2007).
15. Hayashi, A., Hashimoto, T. & Horibe, M. State discrimination with error margin and its locality. *Phys. Rev. A* **78**, 012333 (2008).
16. Sugimoto, H., Hashimoto, T., Horibe, M. & Hayashi, A. Discrimination with error margin between two states: Case of general occurrence probabilities. *Phys. Rev. A* **80**, 052322 (2009).
17. Sugimoto, H., Taninaka, Y. & Hayashi, A. Discrimination with an error margin among three symmetric states of a qubit. *Phys. Rev. A* **86**, 042311 (2012).
18. Chefes, A. & Barnett, S. Quantum state separation, unambiguous discrimination and exact cloning. *J. Mod. Opt.* **45**, 1295 (1998).

19. Zhang, C.-W., Li, C.-F. & Guo, G.-C. General strategies for discrimination of quantum states. *Phys. Lett. A* **261**, 25 (1999).
20. Fiurasek, J. & Jezek, M. Optimal discrimination of mixed quantum states involving inconclusive results. *Phys. Rev. A* **67**, 012321 (2003).
21. 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).
22. Bagan, E., Munoz-Tapia, R., Olivares-Renteria, G. A. & Bergou, J. A. Optimal discrimination of quantum states with a fxed rate of inconclusive outcomes. *Phys. Rev. A* **86**, 040303(R) (2012).
23. Ha, D. & Kwon, Y. An optimal discrimination of two mixed qubit states with a fxed rate of inconclusive results. *Quant. Inf. Process.* **16**, 273 (2017).
24. Bennett, C. H. Quantum Cryptography Using Any Two Nonorthogonal States. *Phys. Rev. Lett.* **68**, 3121 (1992).
25. Brask, J. B., Martin, A., Esposito, W., Houlmann, R., Bowles, J., Zbinden, H. & Brunner, N. Megahertz-Rate Semi-Device-Independent Quantum Random Number Generators Based on Unambiguous State Discrimination. *Phys. Rev. App.* **7**, 054108 (2017).
26. Ha, D. & Kwon, Y. A minimal set of measurements for qudit-state tomography based on unambiguous discrimination. *Quant. Inf. Process.* **17**, 232 (2018).
27. Bergou, J. A., Feldman, E. & Hillery, M. Extracting Information from a Qubit by Multiple Observers: Toward a Teory of Sequential State Discrimination. *Phys. Rev. Lett.* **111**, 100501 (2013).
28. 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).
29. Solis-Prosser, M. A., Gonzales, P., Fuenzalida, J., Gomez, S., Xavier, G. B., Delgado, A. & Lima, G. Experimental multiparty sequential state discrimination. *Phys. Rev. A* **94**, 042309 (2016).
30. Zhang, J.-H., Zhang, F.-L. & Liang, M.-L. Sequential state discrimination with quantum correlation. *Quant. Inf. Process.* **17**, 260 (2018).
31. Hillery, M. & Mimih, J. Sequential discrimination of qudits by multiple observers. *J. Phys. A: Math. Teor.* **50**, 435301 (2017).
32. Namkung, M. & Kwon, Y. Analysis of Optimal Sequential State Discrimination for Linearly Indepenent Pure Quantum States. *Sci. Rep.* **8**, 6515 (2018).
33. Namkung, M. & Kwon, Y. Optimal sequential state discrimination between two mixed quantum states. *Phys. Rev. A* **96**, 022318 (2017).
34. Namkung, M. & Kwon, Y. Sequential state discrimination of coherent states. *Sci. Rep.* **8**, 16915 (2018).
35. Eldar, Y. C. A Semidefinite Programming Approach to Optimal Unambiguous Discrimination of Quantum States. *IEEE Trans. Inform. Theory* **49**, 446 (2003).
36. Herzog, U. Optimum unambiguous discrimination of two mixed states and application to a class of similar states. *Phys. Rev. A* **75**, 052309 (2007).
37. Kleinmann, M., Kampermann, H. & Bruss, D. Structural approach to unambiguous discrimination of two mixed quantum states. *J. Math. Phys* **51**, 032201 (2010).
38. Duan, L.-M. & Guo, G.-C. Probabilistic Cloning and Identification of Linearly Independent Quantum States. *Phys. Rev. Lett.* **80**, 4999 (1998).
39. Li., L., Qiu, D., Li, L., Wu, L. & Zou, X. Probabilistic broadcasting of mixed states. *J. Phys. A: Math. Theor.* **42**, 175302 (2009).
40. Banaszek, K. Optimal receiver for quantum cryptography with two coherent states. *Phys. Lett. A* **253**, 12 (1999).
41. Huttner, B., Imoto, N., Gisin, N. & Mor, T. Quantum cryptography with coherent states. *Phys. Rev. A* **57**, 1863 (1995).
42. Cariolaro, G. *Quantum Communications*. (Springer, Switzerland, 2015).
43. Sasaki, H., Matsumoto, R. & Uyematsu, M. Key Rate of the B92 Quantum Key Distribution Protocol with Finite Qubits. In *IEEE Int. Symposium on Information Theory* (2015).
44. Csiszar, I. & Korner, J. Broadcast channel with confidential messages. *IEEE Trans. Inf. Theory* **24**, 339 (1978).
45. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing* (1984).
46. Bechmann-Pasquinucci, H. & Gisin, N. Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. *Phys. Rev. A* **59**, 4238 (1999).
47. Bhatia, R. *Positive Definite Matrices* (Princeton University Press, 2006).
48. Kraus, K. *States, Effects and Operations: Fundamental Notions of Quantum Theory*. (Wiley, New York, 1991).
49. Kiusalaas, J. *Numertical Methods in Engineering with MATLAB* (Cambridge University Press, 2005).
50. Herzog, U. & Benson, O. Generalized measurements for optimally discriminating two mixed states and their linearoptical implementation. *J. Mod. Opt.* **57**, 188 (2010).
51. Chefles, A. Unambiguous Discrimination Between Linearly Dependent States with Multiple Copies. *Phys. Rev. A* **64**, 062305 (2001).
52. Zhang, W.-H. & Ren, G. Unambiguous discrimination between linearly dependent equidistant states with multiple copies. *Quantum Inf. Process.* **17**, 155 (2018).

Acknowledgements

This work is supported by the Basic Science Research Program through the National Research Foundation of Korea funded by the Ministry of Education, Science and Technology (NRF2015R1D1A1A01060795 & NRF2018R1D1A1B07049420) and Institute for Information and Communication Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No. R0190-15-2028, PSQKD).

Author contributions

M.N. and Y.K. analyzed the result and wrote the manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to M.N. or 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.