# Performance of two quantum-key-distribution protocols

Chi-Hang Fred Fung,* Kiyoshi Tamaki,† and Hoi-Kwong Lo‡
*Center for Quantum Information and Quantum Control, Department of Electrical and Computer Engineering and Department of Physics, University of Toronto, Toronto, Ontario M5S 3G4, Canada*
(Received 12 October 2005; published 25 January 2006)

We compare the performance of Bennett-Brassard 1984 (BB84) and Scarani-Acin-Ribordy-Gisin 2004 (SARG04) protocols, the latter of which was proposed by V. Scarani *et al.* [Phys. Rev. Lett. **92**, 057901 (2004)]. Specifically, in this paper, we investigate the SARG04 protocol with two-way classical communications and the SARG04 protocol with decoy states. In the first part of the paper, we show that the SARG04 scheme with two-way communications can tolerate a higher bit error rate (19.4% for a one-photon source and 6.56% for a two-photon source) than the SARG04 one with one-way communications (10.95% for a one-photon source and 2.71% for a two-photon source). Also, the upper bounds on the bit error rate for the SARG04 protocol with two-way communications are computed in a closed form by considering an individual attack based on a general measurement. In the second part of the paper, we propose employing the idea of decoy states in the SARG04 scheme to obtain unconditional security even when realistic devices are used. We compare the performance of the SARG04 protocol with decoy states and the BB84 one with decoy states. We find that the optimal mean-photon number for the SARG04 scheme is higher than that of the BB84 one when the bit error rate is small. Also, we observe that the SARG04 protocol does not achieve a longer secure distance and a higher key generation rate than the BB84 one, assuming a typical experimental parameter set.

DOI: 10.1103/PhysRevA.73.012337 PACS number(s): 03.67.Dd

## I. INTRODUCTION

Quantum key distribution (QKD) [1,2] provides a way for two parties to expand a secure key that they initially share. The best known QKD is the protocol published by Bennett and Brassard in 1984 (BB84) [1]. The BB84 protocol consists of two phases, the quantum transmission phase and the classical communication phase. In the quantum phase, one of the two legitimate parties, Alice, sends quantum states to the other legitimate party, Bob. The quantum states received by Bob are converted to classical bits by measurements. In the classical communication phase, both parties discuss which bits to keep or discard. They sacrifice some bits to test the error rate on the bit string. If the error rate is too high, they abort the protocol. For the states that are retained, they perform bit error correction with the help of classical communications. After that, Alice and Bob's bit strings are the same, but some information on them might have leaked to a potential eavesdropper, Eve. To remove Eve's information, they apply privacy amplification to distill the final secret key. A comprehensive review of both the theoretical and experimental aspects of quantum key distribution is provided in Ref. [3].

The security of BB84 was not proved until many years after its introduction. Among the proofs [4–7], the one by Shor and Preskill [7] is relevant to this paper. Their simple proof essentially converts an entanglement-distillation-protocol- (EDP-) based QKD proposed by Lo and Chau [6] to the BB84 protocol. The EDP-based QKD has already been shown to be secure by [6] and the conversion successively leads to the security of BB84.

Security proofs of QKD protocols were further extended to explicitly accommodate the imperfection in practical devices [8,9]. One important imperfection is that the laser sources used in practice are coherent sources that occasionally emit more than one photon in each signal. Thus, they are not single-photon sources that the other security proofs [4,5,7] of BB84 assumed. In particular, BB84 may become insecure when coherent sources with strong intensity are used. For instance, Eve can launch an photon-number-splitting (PNS) attack, in which she blocks all single-photon pulses and splits multi-photon pulses. She keeps one copy of each of the split pulses to herself and forwards another copy to Bob. Although [8,9] showed that secure QKD is still possible even with imperfect devices, the PNS attack puts severe limits on the distance and the key generation rate of unconditionally secure QKD.

A novel solution to the problem of imperfect devices in BB84 was proposed by Hwang [10], which uses extra test states—called the decoy states—to learn the properties of the channel and/or the eavesdropping on the key-generating signal states. Our group presented an unconditional security proof of decoy-state QKD [11,12]. By combining the Gottesman-Lo-Lükenhaus-Preskill (GLLP) [8] result with the decoy state idea [10], we showed that decoy state QKD can exhibit dramatic increase in distance and key generation rate compared to nondecoy protocols. Moreover, our group proposed the idea of using the vacua or very weak coherent states as decoy states [12]. Subsequently, practical protocols for QKD using a few decoy states were analyzed by Wang [13,14], by our group [15], and by Harrington *et al.* [16], thereby making the decoy idea more practical. The first experimental implementation of a QKD protocol using one decoy state was demonstrated by our group [17]. Also, a decoy

*Electronic address: cffung@comm.utoronto.ca
†Electronic address: ktamaki@physics.utoronto.ca
‡Electronic address: hklo@comm.utoronto.ca

 

method using two-way classical communications is proposed by our group [18].

Another attempt to combat PNS attacks was by Scarani, Acin, Ribordy, and Gisin in 2004 (SARG04) [19], who introduced a protocol which is very similar to the BB84 protocol. The quantum state transmission phase and the measurement phase of the SARG04 protocol are the same as that of the BB84 protocol, as both use the same four quantum states and the same experimental measurement. The only difference between the two protocols is the classical post-processing phase. Interestingly, with only a change in the post-processing phase, the protocol becomes secure even when Alice emits *two* photons, a situation under which the BB84 scheme is insecure. This was proved by two of us [20], who also proved the security of the SARG04 protocol with a single-photon source. Specifically, we provided lower bounds of the bit error rate when one-way classical communications are used in the error correction and privacy amplification phases. We also proposed a modified SARG04 protocol that uses the same six states as the original six-state protocol [21,22]. The security of the SARG04 scheme with a single-photon source was also proved by Branciard *et al.* [23]. They considered the SARG04 protocol implemented with single-photon sources and with realistic sources. For the single-photon-source case, they provided upper and lower bounds of the bit error rate with one-way classical communications. For the realistic-source case, they considered only incoherent attack by Eve and showed that the SARG04 scheme can achieve a higher secret key rate and a greater secure distance than the BB84 one. The SARG04 protocol was generalized by Koashi [24] to the case of $N$ quantum states. Another protocol that is similar to the SARG04 one is the Bennett 1992 (B92) protocol [25], which uses two nonorthogonal quantum states. The security of the B92 scheme with a single-photon source was proved by Tamaki *et al.* [26,27]. On the other hand, Koashi [28] proposed an implementation of the B92 scheme with strong phase-reference coherent light that was proved secure.

The fact that a modification to the classical communication part (from BB84 to SARG04 protocols) changes the foundation of security, i.e., making two-photon signals secure, is interesting. Note that since the difference between BB84 and SARG04 protocols is only in the classical data processing part, it is not difficult to perform the SARG04 scheme once the experiment of the BB84 protocol is available. Thus, it is important to investigate the performance of the SARG04 scheme in order to determine which protocol one should perform. This is our main motivation.

In this paper, we make an endeavor to study this interesting SARG04 protocol, but in different situations than that considered in Refs. [20,23,24], and thus complementing their results. Specifically, we provide upper and lower bounds of the bit error rate with two-way classical communications for single-photon sources and for two-photon sources. Also, we consider implementations with realistic devices using decoy states with one-way classical communications. Here, we allow the most general attack by Eve and study the key rate and distance properties of the SARG04 scheme in comparison with the BB84 one. Interestingly, under our most general attack assumption which was not considered in Ref. [23], we observe a different phenomenon than [23], that the SARG04 scheme has a lower key rate and a shorter secure distance than the BB84 one. However, our result shows that the SARG04 scheme is interestingly different from the BB84 one in one aspect in the realistic setting. It is that the optimal mean photon number for the SARG04 protocol is higher than that for the BB84 protocol, when the detector error probability is low. This is because when the bit error rate gets smaller, the two-photon contribution to the key generation rate gets higher.

This paper makes use of two important existing techniques: QKD with two-way classical communications and the decoy-state method. QKD with two-way communications in the bit error correction phase was first proposed by Gottesman and Lo [29] as a method to achieve a higher tolerable bit error rate; this method was later improved by Chau [30] to further increase the tolerable bit error rate of a six-state scheme. The essence of QKD with two-way communications is that, by allowing Alice and Bob to communicate with each other, the qubits transmitted by Alice to Bob can be separated into two groups, one with a higher bit error rate than the other. Thus, through two-way communications, they can discard the group with the higher bit error rate and retain the other group for further bit error correction and privacy amplification. Intuitively, a QKD utilizing two-way communications should be superior to the case when only one-way communications are used. This was shown to be true for the BB84 protocol in Ref. [29]. Here, we will show that this is also true for the SARG04 protocol for both single- and two-photon parts. Especially for the single-photon SARG04 scheme, we show that the lower bound with two-way communications is higher than the upper bound with one-way communications provided in Ref. [23]. When we analyze the security of the SARG04 protocol with realistic devices, we will use the decoy-state method of Ref. [11] in order to achieve a long secure distance.

We have tabulated the results of this paper on bounds of bit error rate and secure distance, along with known results, in Table I. The six numbers on the right column are results of this paper, while existing results are cited on the left column. The bounds on the secure distance listed are specific for the experimental parameters from the Gobby-Yuan-Shields (GYS) experiment [31].

The organization of the paper is as follows. We first review some existing techniques for the security proof in Sec. II, which provide a basis for the development of the results of this paper. In Sec. III, we summarize the assumptions we make in this paper. In Sec. IV, we develop a SARG04 protocol with two-way classical communications with one- and two-photon sources. In Sec. V, we consider the SARG04 scheme in a realistic setting, where imperfect laser sources and detectors are used. Finally, concluding remarks are provided in Sec. VI. We note that an independent work on the SARG04 protocol with decoy states was also studied in Ref. [32].

## II. PRELIMINARIES

In this section, we review some bases for the security proof in this paper. First, we briefly review an entanglement

TABLE I. Summary of results for the SARG04 scheme. The bounds on the secure distance are specific for the experimental parameters from the Gobby-Yuan-Shields (GYS) experiment [31].

| Bit error rate of the SARG04 scheme with single-photon source | | |
|---|---|---|
| | one-way | two-way |
| Upper bound | 14.9% [23] | 1/3[a] |
| Lower bound | 9.68% [20,23] and 10.95% (with preprocessing) [23] | 19.9%[a] |
| Bit error rate of the SARG04 scheme with two-photon source | | |
| | one-way | two-way |
| Upper bound | N/A | 22.56%[a] |
| Lower bound | 2.71% [20] | 6.56%[a] |
| Secure distance using decoy states with realistic source | | |
| | BB84 | SARG04 |
| Upper bound | 207.7 (km) [11] | 207.7 (km)[a] |
| Lower bound | 141.8 (km) [11] | 97.2 (km)[a] |

[a]The results of this paper.

distillation protocol (EDP) and its relation with the security of QKD, where we especially review the security proof of the BB84 protocol by Shor and Preskill [7]. Secondly, we explain how the SARG04 scheme works, and we construct an EDP protocol that is equivalent to the SARG04 protocol. We furthermore mention the property of the density matrix in the EDP protocol for the later convenience. Thirdly, we explain the key generation rate for BB84 and SARG04 protocols, assuming realistic devices and one-way classical communications. Next, we describe the decoy method in the BB84 and SARG04 protocols. Finally, we review QKD with two-way classical communications.

### A. EDP and its relation with QKD

#### 1. EDP

The goal of an entanglement distillation protocol (EDP) is to distill nearly perfect EPR pairs from noisy EPR pairs initially shared between two distant parties, Alice and Bob. Any bipartite density matrix describing Alice and Bob's qubit system $\rho$ can be expressed in the Bell basis, which is composed of the four orthogonal Bell states:

$$|\Phi^{\pm}\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2},$$

$$|\Psi^{\pm}\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}. \quad (1)$$

Taking $|\Phi^+\rangle$ as the reference state, the diagonal of $\rho$ in the Bell basis

$$p_I \triangleq \langle\Phi^+|\rho|\Phi^+\rangle,$$

$$p_X \triangleq \langle\Phi^-|\rho|\Phi^-\rangle,$$

$$p_Z \triangleq \langle\Psi^+|\rho|\Psi^+\rangle,$$

$$p_Y \triangleq \langle\Psi^-|\rho|\Psi^-\rangle \quad (2)$$

represent the probabilities of applying, respectively, the Pauli $I$, $X$, $Z$, and $Y$ operators to either one of the qubits of the bipartite system. In the view of an EDP, a pool of $|\Phi^+\rangle_{AB}$ states is prepared by Alice. She keeps system $A$ of every pair and sends system $B$ of every pair to Bob. Due to the presence of noise in the quantum channel, system $B$ may undergo bit and/or phase flip errors and the probabilities of the various types of errors are represented by $p_I$ (no error), $p_X$ (bit flip error), $p_Z$ (phase flip error), and $p_Y$ (bit and phase flip error). In the paper by Bennett, DiVincenzo, Smolin, and Wootters (BDSW) [33], they assume that all of the pairs are described by the same density matrix, and the job of an EDP is to correct the errors using only local operations and classical communications (LOCCs), leaving Alice and Bob with a pool of $|\Phi^+\rangle_{AB}$ states. Several methods of EDP's were proposed in BDSW [33] including the hashing method and the recurrence method. Many of these methods assume that the initial density matrix $\rho$ is Bell diagonal.

#### 2. EDP-based QKD protocol

EDP's are closely related to QKD protocols. The connection between them is that if Alice and Bob share almost perfect EPR pairs that are pure, then the pairs are almost unentangled with Eve's system. Thus, the information leaked to Eve is negligible, and they can obtain an unconditionally secure key by measuring the EPR pairs. Thus, the purpose of a QKD protocol can be viewed as a procedure for Alice and Bob to share almost perfect EPR pairs, which is the purpose of an EDP. In order to run an EDP, they need to know the error rates on the noisy EPR pairs and the job of the error rate estimation is the first part of a QKD protocol. After the error rates are upper bounded, the second part of the QKD protocol involves running an EDP to distill almost perfect EPR pairs. In essence, the QKD scheme can be regarded as consisting of an error rate estimation part and an EDP part. Note that the eavesdropping attack by Eve who has read/write access to the quantum channel appears to Alice and Bob as noise of the channel.

An EDP-based QKD protocol using quantum computers was proposed in Ref. [6] and a modified version of it [7] (shown in Fig. 1) is as follows: Alice prepares $N$ EPR pairs $|\Psi\rangle_{A_iB_i} = (|0_z\rangle_{A_i}|0_z\rangle_{B_i} + |1_z\rangle_{A_i}|1_z\rangle_{B_1})/\sqrt{2}$, for $i \in [1,N]$. She randomly chooses whether to apply a Hadamard gate $H$ on system $B$ (i.e., $k_i = 0,1$) before sending it to Bob through Eve. Eve may perform the most general attack on all Bob's qubits. Bob randomly chooses whether to apply the Hadamard. They discard the EPR pairs to which Alice and Bob apply different operations. Alice and Bob choose some of the EPR pairs as test qubits. They measure the test qubits in the $Z$ basis and compare the measurement results publicly to estimate the bit error rate of the test qubits. The random sampling theorem then asserts that the rest of the untested qubits (code bits) have asymptotically the same bit error rates as the test bits with high probability. Since the bit errors and the phase errors are symmetrized by the random Hadamard gate on Bob's qubits, the phase error rate on code bits is asymptoti-

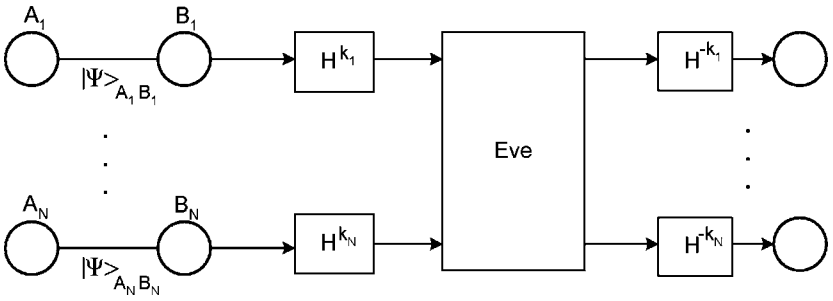


FIG. 1. An EDP version of the BB84 protocol. Shor and Preskill [7] showed that it can be reduced to the BB84 scheme. Note that only the EPR pairs to which Alice and Bob apply the same rotations are shown; EPR pairs with different rotations are discarded.

cally equal to the bit error rate on code bits, i.e., for the BB84 protocol

$$e_p = e_b. \tag{3}$$

Once Alice and Bob know the good estimates the error rates, they can each obtain the bit and phase error syndromes using quantum computers. Alice then sends her syndromes to Bob who will then correct his qubits by applying $Z$ and $X$ operations so that his syndromes match Alice's syndromes. After the successful distillation, they now share EPR pairs that have high fidelity with the pure state $|\Phi^+\rangle_{AB}^{\otimes M}$ (where $M$ is the number of the EPR pairs Alice and Bob share). They each measure their halves of the pair in the $Z$ basis to produce a common secure key on which Eve has negligible information.

We can associate the four probabilities $p_I, p_X, p_Z, p_Y$ with two (dependent) binary random variables $X$ and $Z$ which represent the bit and phase errors, respectively. With this notation, the uncertainty in the bit flip error is $H(X)=H_2(p_X+p_Y)$ and in the phase flip error is $H(Z)=H_2(p_Z+p_Y)$, where $H_2(p)=-p\log_2(p)-(1-p)\log_2(1-p)$ is the binary entropy function. The mutual information between the bit and phase errors is $I(X;Z)=H(X)-H(X|Z)$.

The key generation rate of the EDP-based QKD using one-way classical communications is [33]

$$R = 1 - H(X,Z) \tag{4}$$

$$= 1 - H(X) - H(Z|X). \tag{5}$$

The second term in the last equation is concerned with the number of rounds of random hashing for determining the bit error patterns, and the third term is concerned with the number of rounds of random hashing for determining the phase error patterns given that the bit error patterns are known. One drawback with the EDP-based QKD protocol is that it requires the preparation of EPR pairs and the use of quantum memory and computers, which are challenging to implement in practice in the near future. Thus, it is more desirable to use prepare-and-measure QKD protocols, in which Alice only needs to prepare qubits and send them to Bob, and Bob only needs to measure them immediately after receiving them; no quantum memory and quantum computers are needed.

#### *3. BB84 protocol*

In Shor and Preskill's proof [7], they showed that the EDP-based QKD scheme can be reduced to the BB84 protocol, a prepare-and-measure protocol that does not require the use of quantum computers. Their proof relies on the use of CSS codes to decouple the bit error correction and the phase error correction. They showed that phase error correction is not necessary; as long as phase error correction could have been performed, the protocol is secure. Thus, the phase error correction step with quantum decoding is replaced by a privacy amplification step where classical bits of the raw key are XOR'ed to form the final key. Since the phase error correction step is removed, Bob's final $Z$ measurement in the EDP-based QKD can be moved to before the bit error correction step. Here, note that all of the hashing for the bit error correction is in the $Z$ basis, which commutes with Bob's final $Z$ measurements. Only one-way communications are needed in the bit error correction step in Shor-Preskill's proof. This is because Alice and Bob both compute the bit error syndromes but only Alice sends her syndromes to Bob. Bob then applies the appropriate bit-flip operations on his bit string so as to match his syndromes with Alice's syndromes. Using Eq. (5), the key generation rate of the BB84 protocol resulting from the use of CSS codes is

$$R = 1 - H(X) - [H(Z) - I(Z;X)] \tag{6}$$

$$= 1 - H_2(e_b) - H_2(e_p) + I(Z;X), \tag{7}$$

where $e_b=p_X+p_Y$ is the bit error rate and $e_p=p_Z+p_Y$ is the phase error rate. The bit error rate $e_b$ is estimated in the BB84 protocol through public communications between Alice and Bob. It is important to note that the phase error rate $e_p$ can be estimated from $e_b$ using Eq. (3). The mutual information term in Eq. (7) can be determined by $p_X$, $p_Y$, $p_Z$. However, only $e_b=p_X+p_Y$ and $e_p=p_Z+p_Y$ are known and $p_Y$ is not known. Thus, we consider the worst-case value of $p_Y$ (which corresponds to having no mutual information between bit and phase errors) to find the worst-case value of the key generation rate. In the worst-case scenario, the highest tolerable bit error rate can be found by solving $1=2H_2(e_b)$. This gives $e_b=11.0\%$[7], at which the key generation rate is zero.

### B. The SARG04 protocol

In this paper, we consider the SARG04 protocol [19], which is a prepare-and-measure protocol. In fact, the quantum phase of the SARG04 scheme is the same as that of the BB84 one; so it can easily be seen that the SARG04 scheme is a prepare-and-measure protocol as the BB84 one is.

Let us explain how the SARG04 protocol works. In the SARG04 scheme there are four quantum states $|\varphi_i\rangle, i=0,\ldots,3$:

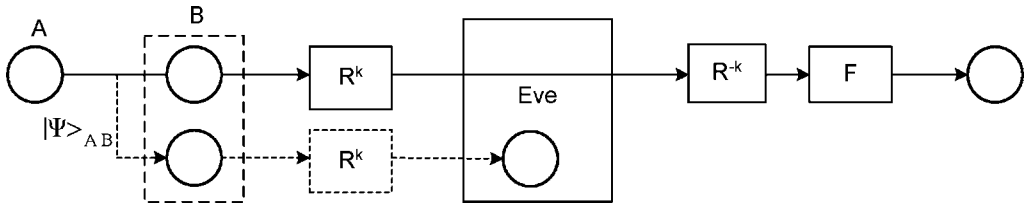


FIG. 2. An EDP version of the SARG04 protocol. Alice prepares an entangled states $|\Psi\rangle_{AB}=(|0_z\rangle_A|\varphi_0^{\otimes\nu}\rangle_B+|1_z\rangle_A|\varphi_1^{\otimes\nu}\rangle_B)/\sqrt{2}$, where $\nu=1,2$ corresponds to the number of photons emitted by Alice. She applies a random rotation on system $B$ before sending it to Bob through Eve. In the case of $\nu=2$, Eve retains one qubit of system $B$ and sends the other to Bob. Although, only one entangled state is shown for simplicify, one should be reminded that Eve may perform the most general attack on the $N$ entangled states as in Fig. 1.

$$|\varphi_0\rangle = \beta|0_x\rangle + \alpha|1_x\rangle,$$

$$|\varphi_m\rangle = R^{-m}|\varphi_0\rangle, \quad m=0,\ldots,3, \tag{8}$$

where $\alpha\equiv\sin(\pi/8)$, $\beta\equiv\cos(\pi/8)$, and $R\equiv\cos(\pi/4)I+\sin(\pi/4)(|1_x\rangle\langle 0_x|-|0_x\rangle\langle 1_x|)$ is a $\pi/2$ rotation around the $Y$ basis. Note that $|\varphi_0\rangle$ and $|\varphi_2\rangle$ are orthonormal, and thus form a basis. The same can be said for $|\varphi_1\rangle$ and $|\varphi_3\rangle$. The four states are divided into four sets $\{R^K|\varphi_0\rangle, R^K|\varphi_1\rangle\}, K\in[0,3]$, in which one represents logic 0 and the other logic 1. The steps for the SARG04 protocol with a $\nu$-photon source ($\nu=1,2$) and one-way communications are as follows.

(1) Alice sends a sequence of $N$ signals to Bob. For each signal, Alice randomly chooses one of the four sets and sends one of the two states in the set to Bob.

(2) For each signal, Bob performs the polarization measurement using one of the two bases randomly. If his detector fails to click, then he broadcasts this fact, and Alice and Bob discard all the corresponding data.

(3) For each signal, Alice publicly announces the choice of the set from which the state was selected.

(4) For each signal, Bob compares his measurement outcome to the two states in the set. If his measurement outcome is orthogonal to one of the states in the set, then he concludes that the other state has been sent, which is a conclusive result. On the other hand, if his measurement outcome is not orthogonal to either of the states in the set, he concludes that it is an inconclusive result. He broadcasts if he got the conclusive result or not for each signal.

(5) Alice randomly chooses some bits as test bits and announces their locations. Bob estimates the bit error rate $e_\nu$ from the test bits by taking the ratio of the number of incorrect conclusive test bits to the total number of conclusive test bits. If $e_\nu$ is too high, they abort the protocol.

(6) Alice and Bob retain only the conclusive untested bits.

(7) They perform bit error correction and privacy amplification on the remaining bit string.

We construct an EDP version of the SARG04 protocol, which is shown in Fig. 2. The EDP version lends itself to an easy extension with two-way classical communications and also a simplified analysis on the bounds on the bit error rates, both of which will be studied in detail later in this paper. We consider Alice having a $\nu$-photon source $\nu=1,2$. For each signal, she first prepares an entangled state $(|0_z\rangle_A|\varphi_0^{\otimes\nu}\rangle_B+|1_z\rangle_A|\varphi_1^{\otimes\nu}\rangle_B)/\sqrt{2}$ and randomly applies a rotation $(R^K)^{\otimes\nu}$ to system B which is then sent to Bob through Eve. Eve applies the most general attack on all the $N$ signals jointly. We assume that Eve always sends a qubit state or a vacuum state to Bob, which is related to the assumption we describe in Sec. III. Bob, upon receiving the qubit, performs the inverse rotation $R^{-K'}$ and a filtering operation whose successful operation is described by the Kraus operator as $F=\sin(\pi/8)|0_x\rangle_B\langle 0_x|+\cos(\pi/8)|1_x\rangle_B\langle 1_x|$. Here, the successful filtering corresponds to a conclusive result [26,27] in the prepare-and-measure SARG04 protocol. Alice and Bob then publicly exchange $K$ and $K'$ and keep the pairs with $K=K'$. They randomly choose some states (test bits) and perform $Z$ measurements on the states. Then, they compare their measurement outcome publicly in order to estimate the bit error rate on the remaining pairs (code bits). This gives us a good estimation of the bit error rate on code bits thanks to the random sampling theorem. On the other hand, the phase error rate on the code bitsis estimated from the bit error rate on the code bits by the theorem below. After the estimation, they choose a CSS code that is sufficient to correct all the bit and phase errors. After the error correction, they share maximally entangled states from which they perform $Z$ measurements to obtain a secure key. It is important to note that the phase error rate of the code bits can be estimated from the bit error rate. Thanks to this estimation, Alice and Bob do not need to perform test bit in $X$ measurement, thus we can equivalently convert our EDP protocol to the prepare-and-measure protocol by the Shor-Preskill's arguments.

*Theorem 1* (*density matrix of one-photon SARG04*). For the one-photon case, the diagonal elements of the density matrix of the EPR pair shared between Alice and Bob in the Bell basis is

$$p_X = e_b - a,$$

$$p_Z = \frac{3}{2}e_b - a,$$

$$p_Y = a, \tag{9}$$

where $e_b$ is the bit error rate and $e_b/2\leqslant a\leqslant e_b$.

*Proof.* See Appendix A. ■

There are two differences between this density matrix and that for the BB84 protocol: (i) There is a factor of $3/2$ in $p_Z$ (whereas the factor is 1 in the BB84 scheme) and (ii) $a$ is no smaller than $e_b/2$ (whereas $a$ can be as small as zero in the BB84 scheme). Such a restriction in $a$ gives rise to mutual information between bit and phase errors (see also Ref. [20]).

This is because for bit and phase errors to be independent (i.e., no mutual information), $p_Y=a$ has be to equal to $3e_b^2/2$. But, this is outside the range $e_b/2 \leqslant a \leqslant e_b$ for $e_b < 1/3$ which is the case of interest. The lower bound on the bit error rate for the one-photon case can be found by solving $0=1-H_2(e_b)-H_2(3e_b/2)+I(X;Z)$, which gives $e_b=9.68\%$ [20,23]. Note that [23] provided a better bound of $e_b=10.95\%$ with data preprocessing.

*Theorem 2* (*density matrix of the two-photon SARG04 protocol*). For the two-photon case, the diagonal elements of the worst case density matrix is

$$p_X = e_b - a,$$

$$p_Z \leqslant x e_b + g(x) - a, \ \forall \ x,$$

$$p_Y = a, \tag{10}$$

where $g(x)=(3-2x+\sqrt{6-6\sqrt{2}x+4x^2})/6$ and $0 \leqslant a \leqslant e_b$.

*Proof.* See Appendix A. □

In this case, $a$ is allowed to be zero. Thus, the lower bound on the bit error rate for the two-photon case can be found by minimizing Eq. (7) over $a$, which leads to having no mutual information between bit and phase errors [i.e., $I(X;Z)=0$]. Solving $0=1-H_2(e_b)-H_2(\min_x x e_b+g(x))$ gives $e_b=2.71\%$ [20].

### C. Privacy amplification for multiphoton signals

In real-life implementation, a weak laser pulse is often used to simulate a single-photon source. However, since it actually emits weak coherent states, the laser outputs contain some multiphoton states in addition to the desired single-photon states. The phases of the coherent pulses are assumed to be randomized in a traditional laser source. Because of this, the coherent states of the laser output reduce to classical mixtures of photon-number states with a Poisson distribution. One important idea from GLLP [8] is that the amount of privacy amplification needed when multiphoton signals are present is the same as if only the key-generating signals are present. To illustrate the idea, let us consider the key-generation rate for the BB84 protocol. For the BB84 protocol, the final key can only be generated by using the single-photon states. If Alice and Bob knew the locations of the single-photon states, they could discard all other multiphoton states and apply error correction and privacy amplification only to the single-photon states. In this case, they could achieve a rate of

$$R_{\mathrm{BB84}} = -Q_1 f(e_1) H_2(e_1) + Q_1[1 - H_2(e_1)], \tag{11}$$

where $e_n$ is the bit error rate of the $n$-photon signal states, $Q_n$ is the gain[1] of the $n$-photon signal state, and $f(x)$ is the error correction efficiency as a function of error rate. The first term is concerned with number of rounds of random hashing for determining the bit error patterns and the $H_2(e_1)$ in the second term is concerned with the privacy amplification. Note that the bit error rate $e_1$ is used for the privacy amplification term because of Eq. (3). For the BB84 scheme, Bob's result is conclusive when Bob obtains bit value by the same measurement basis as the one that Alice has chosen.

Note that the above rate is achieved only when Alice and Bob know the locations of the single-photon states, which is not the case that Bob uses a threshold detector. One method to achieve unconditional security without Alice and Bob knowing the locations of the single-photon states was proposed by Ref. [8]. The idea is that privacy amplification applied to all bit string is equivalent to that applied only to the bit string stemmed from the single-photon states as if the locations of them are known. To show this, we consider the bit value produced by $k_1 \cdot V_1 \oplus k_M \cdot V_M$, where $k_1$ and $k_M$ are the bit string stemmed from the single- and multiple-photon states after bit error correction, and $V_1$ and $V_M$ are random strings in a hash function having the same lengths as $k_1$ and $k_M$, respectively. The first term of $k_1 \cdot V_1 \oplus k_M \cdot V_M$ corresponds to privacy amplification applied to single-photon states only, while the second term is some bit (possibly known to Eve). Since the first term is private to Alice and Bob, even if the second term is completely known to Eve, the sum is still private to Alice and Bob. With this idea, the key generation rate can be improved by considering privacy amplification applied only to single-photon states

$$R_{\mathrm{BB84}} = -Q_\mu f(E_\mu) H_2(E_\mu) + Q_1[1 - H_2(e_1)]. \tag{12}$$

In this paper, we consider the SARG04 protocol which is secure with single-photon and two-photon states. In this case, the key generation rate is [20]

$$R_{\mathrm{SARG04}} = -Q_\mu f(E_\mu) H_2(E_\mu) + Q_1[1 - H(Z_1|X_1)] + Q_2[1 - H(Z_2|X_2)], \tag{13}$$

where the $Z_n$ ($X_n$) is a random variable corresponding to the phase (bit) error for the $n$-photon state. The first term is the fraction of EPR pairs spent for error correction, the second term is the contribution to the key rate from the single-photon states, and the third term is the contribution from the two-photon states. Note that the mutual information between the bit and phase errors is included. According to theorem 2, the mutual information between $X_2$ and $Z_2$ can be zero, meaning $H(Z_2|X_2)=H(Z_2)$.

In Eqs. (12) and (13), the overall gain $Q_\mu$ and the overall bit error rate $E_\mu$ are parameters that Alice and Bob can estimate through public communications. On the other hand, the gain $Q_1$ (and $Q_2$ for the SARG04 protocol), and the bit error rate for the single-photon states $e_1$ (and $e_2$ for the SARG04 protocol) cannot be directly estimated. One way to estimate $e_1$ and $Q_1$ (and $e_2$ and $Q_2$) is to consider the worst situation for Alice and Bob. For instance, in the BB84 scheme, we can pessimistically assume that all the errors happen only in the single-photon detection events, leading to $e_1=E_\mu Q_\mu/Q_1$ and $Q_1=Q_\mu-p_{\mathrm{multi}}/2$, where $p_{\mathrm{multi}}$ is the probability of Alice emitting multiple-photon states (see Ref. [11]). However, this gives a low key generation rate and a short secure distance. Another way to estimate $e_n$ and$Q_n$ is to use the decoy-state

[1]The gain of a particular type is the probability that the transmitted signal of that type is sent by Alice and Bob gets conclusive result.

method in Ref. [11], which we explain next. Using this method, the key generation rate and the secure distance can be greatly increased.

### D. Decoy-state method

In the security analysis with decoy states, we assume using the infinite-decoy-state method of Ref. [11] for the simplicity of analyses. Let us first define the yield $Y_n$, the bit error rate $e_n$, and the gain $Q_n$. The yield, $Y_n$, is defined as the probability that Bob's measurement outcome is conclusive conditional on Alice's $n$-photon emission

$$Y_n \triangleq \Pr\{\text{Bob's result is conclusive} | \text{Alice sent the } n\text{-photon state}\}. \quad (14)$$

The yield is basically a sum of the probabilities of the error events and the error-free events. The fraction of the error-event probability is the bit error rate $e_n$:

$$e_n \triangleq \Pr\{\text{Bob's result is incorrect} | \text{Bob's result is conclusive} \wedge \text{Alice sent the } n\text{-photon state}\}. \quad (15)$$

The gain of the $n$-photon state is

$$Q_n \triangleq \Pr\{\text{Bob's result is conclusive} \wedge \text{Alice sent the } n\text{-photon state}\} \quad (16)$$

$$= Y_n e^{-\mu} \mu^n / n! . \quad (17)$$

The key of the decoy method is to consider the two equations for the overall gain $Q_\mu$ and the overall bit error rate $E_\mu$. The overall gain is the weighted average of the yields of all $n$-photon states:

$$Q_\mu = Y_0 e^{-\mu} + Y_1 e^{-\mu}\mu + \cdots + Y_n e^{-\mu}(\mu^n/n!) + \cdots . \quad (18)$$

The overall QBER is the weight average of the errors of all $n$-photon states:

$$E_\mu = \frac{1}{Q_\mu} \sum_{n=0}^{\infty} Y_n e^{-\mu}(\mu^n/n!) e_n. \quad (19)$$

The main point of the method is to vary the laser intensity $\mu$ over all non-negative values randomly. Each value of $\mu$ is associated with one equation for $Q_\mu$ and one for $E_\mu$. Thus, by varying $\mu$, we have a set of linear equations of $Y_n$ and $e_n$, which can then be solved. The states that are used for the determination of $Y_n$ and $e_n$ with the different $\mu$'s are the decoy states, which will not be used to generate the final key. Another set of states, the signal states, will be used for key generation and are outputs from one laser intensity only. To make sure that $Y_n$ and $e_n$ estimated from the decoy states are good estimates of $Y_n$ and $e_n$ for the signal states, we randomize the locations of both states so that Eve can only act equally on them. Once we have good estimates of $Y_n$ (thus, $Q_n$) and $e_n$, we can determine the achievable key-generation rate by using Eq. (12) for the BB84 scheme and Eq. (13) for the SARG04 scheme. For the SARG04 protocol, we use the relations between the phase and bit error rates in Eqs. (9) and (10) to determine the phase error rates from the bit error rates.

For the BB84 scheme, the expected values for the yields and the bit error rates without any eavesdropping are [11]

$$Y_{n,\mathrm{BB84}} = [\eta_n + (1-\eta_n)p_{\mathrm{dark}}]/2 \quad (20)$$

$$e_{n,\mathrm{BB84}} = \left( \eta_n \frac{e_{\mathrm{detector}}}{2} + (1-\eta_n)p_{\mathrm{dark}}\frac{1}{4} \right) / Y_{n,\mathrm{BB84}}, \quad (21)$$

where $\eta_n$, $p_{\mathrm{dark}}$, and $e_{\mathrm{detector}}$ are the transmission efficiency for an $n$-photon signal, the probability that the detector clicks when the input is a vacuum state, and a parameter representing the misalignment in the detector, respectively. The presence of any eavesdropping would deviate the actual values of them and thus would be caught by Alice and Bob. For the SARG04 protocol, we will derive similar formulas for $Y_n$ and $e_n$ later in this paper, and also we will describe the SARG04 protocol with decoy states.

### E. QKD with two-way classical communications

In Shor-Preskill's proof, they showed that applying the bit and phase error corrections with CSS code followed by $Z$ measurements to a pool of noisy EPR pairs is equivalent to applying the $Z$ measurement followed by bit error correction and privacy amplification. This order swapping is applicable to any pool of noisy EPR pairs characterized by some $(p_X, p_Y, p_Z)$. Imagine that, before the bit and phase error corrections and the final $Z$ measurements, we insert an extra operation on the EPR pairs that changes the pairs to have some other characteristics $(p'_X, p'_Y, p'_Z)$. One reason that we want to insert such an extra operation is to increase the highest tolerable bit error rate of a QKD protocol. Since, after this extra operation, we are also left with a pool of noisy EPR pairs, we can invoke the Shor-Preskill's argument to move the final $Z$ measurements to before the bit and phase error correction steps. However, this is not (yet) a prepare-and-measure protocol since Shor-Preskill's proof only brings the $Z$ measurements to after the extra operation. If this extra operation commutes with the $Z$ measurements, then we can swap their order and turn it into a prepare-and-measure protocol.

A specific operation for this extra operation was considered by Gottesman and Lo [29]. Their operation commutes with the $Z$ measurements (so is compatible with prepare-and-measure protocols) and is composed of a sequence of steps applied to the EPR pairs. There are two types of steps, a B step and a P step. As the names imply, a B step (P step) is meant to improve the bit (phase) error rate of the EPR pairs. A B step requires two-way classical communications for exchanging information between Alice and Bob. Hence, prepare-and-measure protocols derived from using this technique requires two-way classical communications.

*Definition 1* (*B step* [29]). A B step, shown in Fig. 3, consists of Alice and Bob together performing a bilateral XOR on two EPR pairs randomly chosen and comparing their $Z$ measurement results of the target pair. If their results are the same, they keep the source EPR pair and discard the target EPR pair. If they are different, they discard both pairs.

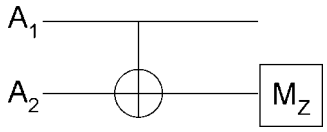


FIG. 3. B step: Alice performs a bilateral XOR on her halves of two EPR pairs (the circuit of which is depicted) and Bob performs the same on his halves of the EPR pairs. They measure the target qubits in the $Z$ basis. If their measurement results are same, they keep the source EPR pair and discard the target; otherwise, they discard both EPR pairs.

When the two EPR pairs initially have no bit error or both have a bit error, the measurement results will be the same. When only one of the two pairs has a bit error, the measurement results will be different. The bilateral XOR is equivalent to two measurements of $Z\otimes Z$, one by Alice and one by Bob. Thus, a B step commutes with the final $Z$ measurements in a prepare-and-measure protocol. Suppose that initially the EPR pairs are in the state $(p_X,p_Y,p_Z)$, applying a B step to every pair of EPR pairs leads to a smaller set of surviving pairs with a new state $(p'_X,p'_Y,p'_Z)$

$$p'_X = (p_X^2 + p_Y^2)/p_S, \tag{22}$$

$$p'_Y = 2p_X p_Y/p_S, \tag{23}$$

$$p'_Z = 2(1 - p_X - p_Y - p_Z)p_Z/p_S, \tag{24}$$

$$p_S = 1 - 2(p_X + p_Y)(1 - p_X - p_Y), \tag{25}$$

where $p_S$ is the probability that a source EPR pair survives the step. Note that half of the EPR pairs are target pairs and are always discarded after a B step.

*Definition 2* (*P step* [29]). A P step, shown in Fig. 4, operates on three EPR pairs randomly chosen, one target and two source pairs. Alice and Bob perform a bilateral XOR on the target and a source pairs and then perform a second bilateral XOR on the target and the second source pairs. The phase error syndrome is the $X$ measurements of the two source pairs, which is not needed in a prepare-and-measure QKD. The target pair is kept for the next step. The P step requires no communications between Alice and Bob and is really a classical circuit. So, the P step commutes with the final $Z$ measurements of a QKD. If the $Z$ measurements is performed before the P step, the P step is equivalent to XOR'ing three bits to generate one bit. Suppose that initially the EPR pairs are in the state $(p_X,p_Y,p_Z)$, a P step leads to a new state

$$p'_X = 3p_I^2(p_X + p_Y) + 6p_I p_X p_Z + 3p_X^2 p_Y + p_X^3, \tag{26}$$

$$p'_Y = 6p_I p_Y p_Z + 3p_X(p_Y^2 + p_Z^2) + 3p_Y p_Z^2 + p_Y^3, \tag{27}$$

$$p'_Z = 3p_I(p_Y^2 + p_Z^2) + 6p_X p_Y p_Z + 3p_Y^2 p_Z + p_Z^3, \tag{28}$$

$$p_I = 1 - p_X - p_Y - p_Z, \tag{29}$$

where $p_I$ is the initial probability of no error. Note that only one-third of the EPR pairs remain after a P step.

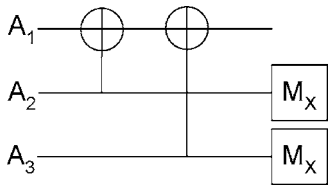


FIG. 4. P step: Alice adds (module 2) her halves of three EPR pairs (the circuit of which is depicted) and Bob performs the same on his halves of the EPR pairs. They keep the target EPR pair and discard the other two. The $X$ measurements of the two source pairs do not need to be performed in a prepare-and-measure QKD.

The reduction from a EDP with B and P steps to the BB84 protocol is possible because these steps satisfy the "no-branching (in $X$ operators) requirement" in Gottesman-Lo's paper [29]. Specifically, the decision of which EPR pairs to discard and which to retain only depends on the outcomes of $Z$ measurements, but not on the outcomes of $X$ measurements. For the BB84 scheme, Gottesman and Lo [29] showed that a sequence of five B steps, followed by six P steps, can give rise to a tolerable bit error rate of 18.9%. Since $p_Y$ cannot be estimated in BB84, it is necessary to consider the worst-case value of $p_Y$ when determining the tolerable bit error rate. They showed that $p_Y=0$ is the worst case for any sequence starting with a B step. In this paper, we consider finding the highest tolerable bit error rate for the SARG04 protocol using Gottesman and Lo's technique. We also prove the worst-case value of $p_Y$ for the SARG04 scheme.

## III. ASSUMPTIONS ON THE DEVICES

In this section, we describe some assumptions we make in this paper. First, note that Bob sometimes has a double click where he cannot determine the measurement outcome. This happens because of the dark counts or detecting multiphotons. In this case, we impose Bob to take one of the bit values randomly [8,9]. Thus, we can regard his measurement outcome as always stemming from the measurement on a qubit state. This operation is so-called "squash operation" in Ref. [8], which is a operation mapping from a multiphoton state to a qubit state. Furthermore, we assume the measurement such that it can be represented by the squash operation followed by a proper operations in a protocol. For instance, Bob's measurement can be described by the squash operation followed by the rotations, the filtering operation and $Z$ basis measurement in the SARG04 protocol. We assume this model based on the squash operation in the whole paper.

In Sec. V, we will consider five types of imperfections in realistic QKD setups: (i) the source is a laser source that generates a Poisson distribution of photon number state, (ii) there is loss in the optical fiber, (iii) Bob's detector is not completely efficient in declaring a detection event, (iv) Bob's detector may generate a false detection when there is no input, and (v) there is misalignment in Bob's detector.

Assuming the phase randomization, the single-mode laser source emits a pulse that is a classical mixtures of the photon number states with a Poisson distribution

$$\sum_{i=0}^{\infty} \frac{\mu}{i!} e^{-\mu} |i\rangle\langle i|, \tag{30}$$

where $\mu$ is the mean photon number. We quantify the loss in the optical fiber by the probability that an input photon is lost at the end of the transmission. Let $\alpha$ in dB/km be the loss coefficient of the optical fiber and $l$ be the fiber length in km. The probability that the input photon is not lost is equal to $10^{-\alpha l/10}$.

It is the case that Bob's detector fails to indicate the presence of an input photon. The effect is similar to the transmission loss. The probability that Bob's detector detects the presence of an input photon is defined as Bob's detection efficiency $\eta_{\text{Bob}}$.

Combining the loss in the quantum channel and the inefficiency of Bob's detector, we have the overall transmission efficiency, $\eta$. It is the probability that a photon is detected given that one has been sent, which is given by

$$\eta = 10^{-\alpha l/10} \eta_{\text{Bob}}. \tag{31}$$

When the input signal contains more than one photons, the signal is detected if at least one photon is detected. Thus, the transmission efficiency for an $n$-photon signal is

$$\eta_n = 1 - (1 - \eta)^n. \tag{32}$$

When there is no input to Bob's detector, there is a possibility that it generates a detection event. This is due to the intrinsic detector's dark counts, the background spray, and the leakage from timing signals. We denote the probability of this false detection event as $p_{\text{detector}}$. Suppose that there are two detectors in the system. We denote the probability of false detection for the system as $p_{\text{dark}}=2p_{\text{detector}}(1-p_{\text{detector}})$, since Alice and Bob disregard any signal generating double detections from the two detectors.

We model the misalignment of the detectors by a rotation in the bases of Bob's projection measurements. We will calculate the probabilities of inconclusive, correct, and incorrect results specifically for the SARG04 protocol using this model in Sec. V.

## IV. SARG04 PROTOCOL WITH ONE- AND TWO-PHOTON SOURCES

In this section, we derive the lower and upper bounds of the tolerable bit error rates for the SARG04 scheme with two-way classical communications, where we consider using perfect one- and two-photon sources.

### A. Lower bounds with two-way communications

To determine the highest tolerable bit error rate, we would like to search for the sequence of B steps and P steps (introduced in Sec. II E) that, when followed by the one-way EDP with random CSS to correct bit and phase errors, gives a positive key generate rate for the bit error rate in question. The sequence of B and P steps renders the initial state $(p_I, p_X, p_Y, p_Z)$ to another state $(p_I', p_X', p_Y', p_Z')$, which is then passed to the one-way protocol for producing almost perfect EPR pairs. The key generation rate, based on the CSS protocol, is

$$R = 1 - H(p_X' + p_Y') - H(p_Z' + p_Y'). \tag{33}$$

Note that we have ignored the mutual information between the bit and phase errors for simplicity of analyses. For the single-photon case of the SARG04 scheme, the initial state is $p_X=e_b-a$, $p_Z=3e_b/2-a$, $p_Y=a$, where Alice and Bob can estimate $e_b$ but not $a$. Thus, for the purpose of determining the highest tolerable bit error rate, we consider the worst-case value of $a$ for a given $e_b$ and a given sequence such that the initial state with this value will lead to the smallest key generation rate. A proof of this for the BB84 protocol was given in Ref. [29]. Here we adapt their proof to the SARG04 scheme and have the following theorem.

Theorem 3. For an initial state of $p_X=e_b-a$, $p_Z=\xi e_b-a$, $p_Y=a$, where $\xi \in \mathbb{R} \geqslant 1$ is some constant, the key generation rate as given in Eq. (33) is an increasing function of $a$ for a fixed $e_b$ and a fixed sequence of B steps and P steps starting with a B step, under the following conditions:

(i) $e_b < (1+4a)/(2(1+\xi))$ $\forall$ $a$ in the valid range and

(ii) $e_b < 1/(2\xi)$.

*Proof.* See Appendix B. ■

Note that theorem 3 is a simple generalization of the result in Appendix III of Ref. [29]. For the single-photon case, we apply theorem 3 with $\xi=3/2$. Given the valid range of $a$ being $[e_b/2, e_b]$, we have the following.

Corollary 1. The worst-case for the single-photon SARG04 scheme is $a=e_b/2$.

We have written a simple computer program in MATHEMATICA to calculate the evolution of the diagonal elements of the marginal density matrix of the EPR pairs shared by Alice and Bob under sequences of B and P steps using Eqs. (22)–(29). With $a=e_b/2$, we exhaustively searched for the step sequence with 15 B/P steps or less that can tolerate the highest bit error rate. For each sequence, we searched for the highest initial value of $e_b$ that gives rise to a positive key generation rate given by Eq. (33). We conclude that $e_b=19.9\%$ is tolerable with nine B steps. We can easily check that this value of $e_b$ satisfies the two conditions of theorem 3. Since in each B step, Alice and Bob discard at least half of the EPR pairs that have survived so far, a protocol with nine B steps leaves only a small number of EPR pairs at the end of the protocol. Thus, a sequence with nine B steps may not be efficient in practice. Therefore, we consider the highest tolerable bit error rates with various maximum numbers of steps allowed, as shown in Fig. 5. As can be seen, even a protocol with two B steps is able to tolerate a bit error rate of 16.1%, which is a great improvement from that of one-way protocols (10.95% from Ref. [23]).

We now consider a two-photon SARG04 scheme, whose density matrix satisfies Eq. (10). Since $p_Z \leqslant x e_b + g(x) - a$, $\forall$ $x$, we can minimize the right-hand side over $x$ to find the worst-case $p_Z$. Substituting in the minimizing $x$ gives us the initial state

$$p_X = e_b - a,$$

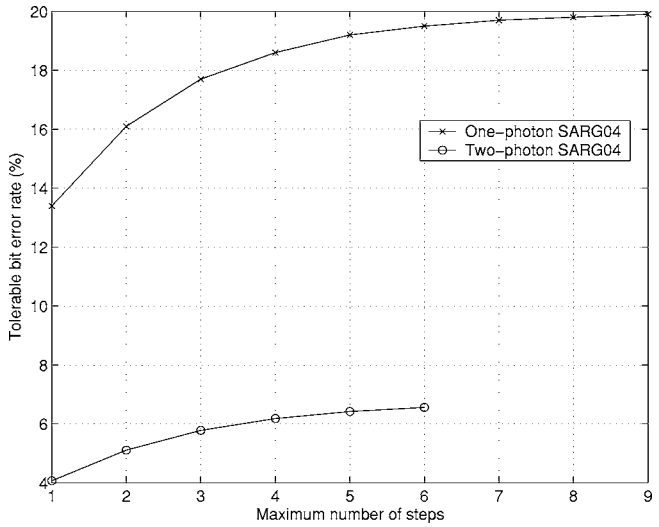


FIG. 5. The highest tolerable bit error rates with various maximum number of B or P steps allowed. It turns out only B steps are used in all cases to achieve the highest bit error rates. Even when a small number of B steps is used, the tolerable bit error rate increase quite substantially compared to the case where no B step is used. Note that only up to nine (six) steps are plotted for the single-photon (two-photon) case since sequences with more steps are less optimal.

$$p_Z = \frac{1}{2} - \frac{1}{2\sqrt{2}}(1-3e_b) + \sqrt{\frac{1-(1-3e_b)^2}{24}} - a,$$

$$p_Y = a, \tag{34}$$

where $0 \leqslant a \leqslant e_b$. Since $p_Z$ can be written as $p_Z = \xi e_b - a$ for some $\xi \geqslant 1$ and for a fixed $e_b$, we can invoke theorem 3 to arrive at the following:

Corollary 2. The worst-case for the two-photon SARG04 protocol is $a=0$.

In the worst case, we found that $e_b=6.56\%$ is tolerable with six B steps for the two-photon SARG04 scheme. This is greater than the tolerable bit error rate of 2.71% using one-way communications [20]. The highest tolerable bit error rates with various maximum numbers of steps allowed for the two-photon scheme is also shown in Fig. 5. As can be seen, even when a smaller number of B steps is used, the tolerable bit error rate increase quite substantially compared to the case where no B step is used.

The steps for the SARG04 protocol with a $\nu$-photon source ($\nu=1,2$) involving B steps are similar to the one-way SARG04 protocol in Sec. II B and are as follows.

(1–6) Same as that in the one-way SARG04 scheme.

(7) B step: Alice randomly divides the bits into pairs and informs this to Bob. They separately compute the parity for each pair and compare their results with each other. If they have the same parity for a pair, they keep one bit and discard the other bit of the pair; otherwise, both bits are discarded. This step is repeated as many times as needed.

(8) They perform bit error correction and privacy amplification on the remaining bit string using the revised bit error rate.

### B. Upper bounds with two-way communications

An upper bound for the single-photon SARG04 scheme with one-way communications was provided in Ref. [23]. This upper bound of 14.9% is lower than our lower bound of 19.9% with two-way communications. In other words, as far as the single-photon component is concerned, the SARG04 scheme with two-way classical communications can tolerate a higher bit error rate than the SARG04 protocol with only one-way classical communications. A similar behavior was previously found in the BB84 scheme [29]. Here, we will investigate the upper bound with two-way communications for both single-photon and two-photon in the SARG04 protocol.

To arrive at an upper bound, we note that security cannot be established between Alice and Bob if there is no entanglement shared between them [34]. Specifically, when the density matrix of Alice and Bob is separable, i.e., $\rho_{AB}=\Sigma_i \rho_{A,i} \otimes \rho_{B,i}$, then there is no entanglement. One result from BDSW [33] is that, for a bipartite state with a density matrix of the form

$$\rho = p_1|\Phi^+\rangle\langle\Phi^+| + p_2|\Phi^-\rangle\langle\Phi^-| + p_3|\Psi^+\rangle\langle\Psi^+| + p_4|\Psi^-\rangle\langle\Psi^-|, \tag{35}$$

if none of the probabilities $p_1,\ldots,p_4$ is greater than 1/2, then $\rho$ can be written as a mixture of separable states and thus no entanglement exists. Using this idea, we may find the bit error rate with which the Bell diagonal elements of our density matrices of the SARG04 scheme in Eq. (9) and Eq. (10) are all no greater than 1/2. We may imagine $e_b$ to be small initially, in which case $p_I$ is close to unity and $p_X$, $p_Y$, and $p_Z$ are close to zero. Then, we gradually increase $e_b$ until $p_I$ goes down to 1/2. Although the BDSW idea applies only to Bell-diagonal density matrix and our density matrices may not be Bell diagonal, we can still apply the BDSW idea to our case since whether the off-diagonal terms are zero or not has no bearing on the B steps, the P steps, the CSS error correction, and the CSS privacy amplification in our protocol. In other words, our entanglement distillation method does not extract entanglement from the off-diagonal terms. Thus, we may safely regard our density matrices as Bell diagonal.

For the single-photon SARG04 protocol, setting $p_I=1/2$ gives $e_b=1/5+2a/5$. Given the valid range of $a$, this suggests that $e_b$ is between 1/4 and 1/3. Eve would like to cause the error rate as low as possible. But she may not be able to choose $a$ freely to induce an error rate of 1/4, since $a$ is an parameter influenced by her and is not in her complete control in any attack strategy by her. Thus, without any reference to a specific attack strategy, the value of $a$ (and the upper bound on $e_b$) cannot be specified. Therefore, we focus on specific intercept-and-resend strategies to determine specific values of $a$ and an upper bound on $e_b$.

In an intercept-and-resend attack, Eve captures and measures the photon sent by Alice to Bob. She then sends another photon with the polarization depending on the measurement result to Bob. Certainly, no entanglement exists between Alice and Bob, since Bob's photon was created by Eve. In a simple intercept-and-resend attack, Eve performs a

photon polarization measurement with a basis randomly chosen from two bases. The first basis consists of $|\varphi_0\rangle$ and $|\varphi_2\rangle$, while the second consists of $|\varphi_1\rangle$ and $|\varphi_3\rangle$. After the measurement, Eve sends the resultant state to Bob. This particular attack causes an error rate of 1/3. The fact that this is at the high end of the range $[\frac{1}{4},\frac{1}{3}]$ prompts us to search for a more sophisticated intercept-and-resend attack.

*Definition 3 (General POVM attack).* A general POVM attack is an individual intercept-and-resend attack by Eve who captures every transmission from Alice (each which may consist of one or more photons), performs an arbitrary POVM measurement on each transmission independently, and sends an arbitrary state to Bob depending on the measurement outcome. The POVM is arbitrary and can be represented by $J+1$ elements $\{M_{\text{vac}}, M_i : i=0,\ldots,J-1\}$, with $M_{\text{vac}}+\Sigma_i M_i = I$. For the outcome corresponding to $M_{\text{vac}}$, Eve sends vacuum to Bob, whereas, for outcome $i$, she sends an arbitrary state $|\sigma_i\rangle$ to Bob.

We consider Eve launching such a general POVM attack for the SARG04 one-photon case and two-photon case. We want to optimize over $M_{\text{vac}}$, $M_i$, and $|\sigma_i\rangle$ so that Eve induces the lowest possible bit error rate, hoping to achieve a rate smaller than $\frac{1}{3}$ caused by the simple attack described above for the one-photon case. Unfortunately, for the one-photon case, even with such a great freedom to choose the POVM and the states sent, this attack cannot do better than the simple attack.

Theorem 4. For single-photon SARG04, the smallest bit error rate $e_b$ caused by Eve using a general POVM attack is $\frac{1}{3}$.

*Proof.* See Appendix C. ■

On the other hand, for the two-photon SARG04 scheme, it is not trivial to consider intercept-and-resend attack and thus we only consider a general POVM attack.

Theorem 5. For the two-photon SARG04 protocol, the smallest bit error rate $e_b$ caused by Eve using a general POVM attack is $(3-\sqrt{2})/7 \approx 22.65\%$. Moreover, a POVM that gives rise to this minimum bit error rate is

$$M_m = P(\lambda_+|\varphi_m\rangle|\varphi_m\rangle + \lambda_-|\varphi_{m+2}\rangle|\varphi_{m+2}\rangle), \quad m=0,\ldots,3, \tag{36}$$

$$M_{\text{vac}} = P(|\varphi_0\rangle|\varphi_2\rangle - |\varphi_2\rangle|\varphi_0\rangle)/2 \tag{37}$$

$$= P(|\varphi_3\rangle|\varphi_1\rangle - |\varphi_1\rangle|\varphi_3\rangle)/2, \tag{38}$$

where $\lambda_\pm = (\pm 2+\sqrt{2})/4$, $P(|\Phi\rangle) = |\Phi\rangle\langle\Phi|$ is a projection operator associated with a pure state $|\Phi\rangle$, and the subscript in $\varphi_{m+2}$ is taken in modulo 4. Eve sends $|\varphi_m\rangle$ to Bob when the measurement outcome is $m \in [0,3]$. Note that $M_{\text{vac}}$ never occurs, since the four states sent by Alice, $|\varphi_m\rangle|\varphi_m\rangle, m \in [0,3]$, are orthogonal to the state $M_{\text{vac}}$ projects onto.

*Proof.* See Appendix C. ■

### C. Comparison with the BB84 protocol in depolarizing channels

We compare the lower and upper bounds with two-way communications of the SARG04 and BB84 protocols by assuming that the eavesdropping is realized by a depolarizing channel. A depolarizing channel evolves an $\nu$-photon input $\rho^{\otimes\nu}$ to $(1-4p/3)\rho^{\otimes\nu}+(4p/3)(I/2)^{\otimes\nu}$ with a depolarizing rate $p$. For the SARG04 scheme, the depolarizing rate $p$ is related to the bit error rate $e_b$ by $e_b = 4p/(3+4p)$, whereas, for the BB84 protocol, $e_b = 2p/3$. Using these formulas, we see that the SARG04 protocol is secure up to $p \approx 18.6\%$ for the one-photon scheme and $p \approx 5.27\%$ for the two-photon one, and the BB84 protocol is secure up to $p \approx 28.35\%$ [29] with two-way communications. For the upper bounds, the SARG04 scheme is insecure beyond $p=3/8$ for the one-photon mode and $p = 3(2-\sqrt{2})/8 \approx 22.0\%$ for the two-photon scheme, and the BB84 protocol is insecure beyond $p=3/8$ [29].

## V. SARG04 SCHEME WITH REALISTIC SOURCES USING DECOY STATES

With a realistic phase-randomized laser source, the output pulses are classical mixtures of the photon number states with a Poisson distribution. In this section, we consider using the decoy method of Ref. [11] to operate the SARG04 securely with a realistic source. With this particular decoy method, the mean photon number of the laser source when emitting the decoy states varies over infinitely many values, in order to estimate the statistics for the decoy states. References [12–16] analyzed practical decoy schemes with only a few decoy states. Here, we consider applying the infinite-decoy idea to SARG04 for the simplicity of analyses.

The steps for the SARG04 protocol with decoy states are as follows.

(1) Alice randomly chooses the locations of the decoy states and the signal states.

(2) For the decoy states, Alice adjusts the power of the laser to have a random mean-photon number $\mu$ and she records this value of $\mu$. For signal states, Alice operates the laser at a fixed mean-photon number.

(3) Alice randomly chooses one of the four sets and sends one of the two states in the set to Bob.

(4) Bob performs the polarization measurement using one of the two bases randomly. If his detector fails to click, then he broadcasts this fact, and Alice and Bob discard all the corresponding data.

(5) Alice announces the sets of states for both decoy and signal states to Bob. She also announces the locations of the decoy states, their values of $\mu$, and their states.

(6) Bob, based on the information on the sets of states, broadcasts which bits are conclusive or not.

(7) For all the decoy states having the same $\mu$, Bob estimates $Q_\mu$ by taking the ratio of the number of conclusive events to the total number of conclusive, inconclusive, and no-detection events. He estimates $E_\mu$ by taking the ratio of the number of incorrect conclusive events to the total number of conclusive events.

(8) Bob then estimates $e_1$ and $e_2$ based on $Q_\mu$'s and $E_\mu$'s over all values of $\mu$'s.

(9) If both of $e_1$ and $e_2$ are too high, they abort the protocol.

(10) Alice and Bob discard all events concerned with inconclusive and all decoy states.

(11) They perform bit error correction on the remaining bit string and apply privacy amplification.

In this section, we analyze the key generation rate of this protocol under the same situation as was considered in Ref. [11], in which (i) the source is a phase randomized coherent source, (ii) there is loss in the optical fiber, (iii) Bob's detection is not completely efficient in declaring a detection event, (iv) there are dark counts, and (v) there is misalignment in Bob's detector. We first develop a specific detector error model for the SARG04 scheme, which can then be used to formulate the yield and the error rate equations for the SARG04 protocol. With the yields and the error rates, we can compute the achievable key-generation rates.

### A. Model for detector errors in the SARG04 protocol

We consider a specific error model for detections in the SARG04 protocol. We have chosen this model because it is also a simple model for explaining errors in the BB84 scheme and thus would provide a reasonable performance comparison with the BB84 scheme. In the decoy paper for the BB84 protocol [11], they used the Gobby-Yuan-Shields (GYS) [31] experimental results to characterize the probability of detector error in the BB84 scheme, denoted by $e_{\text{detector}}$. The value of this probability is specific to the setup in the GYS experiment which is for the BB84 protocol. Although an experimental setup for the SARG04 scheme might be the same as that for the BB84 one (since their quantum phases are the same), their interpretations of errors are different and thus there is no reason to believe that the error probabilities describing both setups are exactly the same. Nevertheless, in order to facilitate a reasonable comparison between the SARG04 and BB84 protocols, we attribute the probability of detector error to a rotation of the detector by a small angle. Specifically, we model the misalignment of the detectors by a rotation of angle $\theta$ in the two projection measurements at Bob's side. Using the same model for both the SARG04 and BB84 protocols, we can compare their results on a common ground. For the SARG04 scheme, we can calculate the probabilities of getting the inconclusive, incorrect, and correct outcomes for each of the four bases. For example, Fig. 6 shows the calculation for the basis $\{\leftrightarrow, \nearrow\}$. In the end, we conclude that given a successful detection event at Bob's detector, $\Pr\{\text{conclusive}\}=\sin^2(\theta)/2+1/4$, $\Pr\{\text{incorrect}\}=\sin^2(\theta)/2$, and $\Pr\{\text{correct}\}=1/4$. For the BB84 scheme, the probability of detection error can easily be seen to be $\sin^2(\theta)$. Similarly, we perform the same calculations when Bob detects a vacuum state and a dark count occurs. We arrive at $\Pr\{\text{inconclusive}\}=1/2$, $\Pr\{\text{correct}\}=1/4$, and $\Pr\{\text{incorrect}\}=1/4$. These probabilities are used later in the calculations of the yields and the bit error rates for the SARG04 protocol.

### B. Key generation rate using decoy

Recall that the key generation rate for the SARG04 scheme with decoy is

$$R_{\text{SARG04}} \geqslant -Q_\mu f(E_\mu) H_2(E_\mu) + Q_1[1 - H_2(Z_1|X_1)] + Q_2[1 - H_2(e_{p,2})], \quad (39)$$

where the subscript $\mu$ denotes the mean photon number for the signal states, $Q_\mu$ is the gain of the signal states, $E_\mu$ is the QBER of the signal states, $Q_j$ and $e_{p,j}, (j=1,2)$ are the gains and the phase error rates of the single-photon states $(j=1)$ and the two-photon states $(j=2)$, $Z_1$ and $X_1$ are random variables characterizing the phase and bit errors for the single-photon states (see Sec. II for definition), $f(x)$ is the error correction efficiency as a function of error rate, and $H_2(x)$ is the binary entropy function.

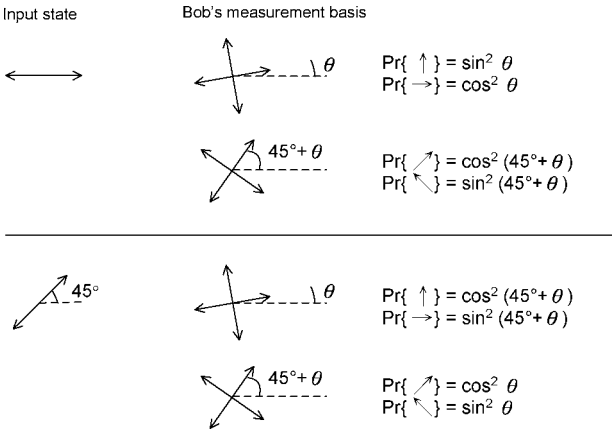


FIG. 6. Calculation of measurement probabilities with misalignment of the detectors for the basis $\{\leftrightarrow, \nearrow\}$. The misalignment is modeled by a rotation of the two measurement bases $\theta$. For this basis, the conclusive results are $\updownarrow$ and $\nwarrow$.

We note that both single-photon and two-photon states have positive contributions to the key generation rate, in contrast to the BB84 protocol, the key generation rate of which has only the single-photon-state contribution. Also, since there is mutual information between the bit and phase errors for the single-photon case, we have included this contribution to the key generation in Eq. (39). The parameters $Q_\mu$ and $E_\mu$ in Eq. (39) can be estimated through public communications. The phase error rates $e_{p,1}$ and $e_{p,2}$ can be estimated, respectively, from the bit error rates $e_1$ and $e_2$ [using the relations in Eqs. (9) and (10) with the worst-case values of $a=e_1/2$ and $a=0$, respectively]. The bit error rates $e_1$ and $e_2$, along with $Q_1$ and $Q_2$, can in turn be estimated using the decoy state idea. In what follows, we derive the formulas for these parameters for the SARG04 scheme, and thus, using these parameters, we can determine the key generation rate using Eq. (39).

### C. Yields and bit error rates

We now determine the yields and the bit error rates of the transmitted qubits for the SARG04 protocol. Using the definition of the yield in Eq. (14), the yield for the SARG04 scheme is

$$Y_{n,\text{SARG04}} = \eta_n \left( \frac{e_{\text{detector}}}{2} + \frac{1}{4} \right) + (1 - \eta_n) p_{\text{dark}} \frac{1}{2}, \quad (40)$$

where $e_{\text{detector}}=\sin^2(\theta)$. The fraction of $1/4$ corresponds to the probability of getting a conclusive result. Compared to the yield for the BB84 protocol in Eq. (20), we see that the yield stemmed from the signal for the SARG04 scheme is

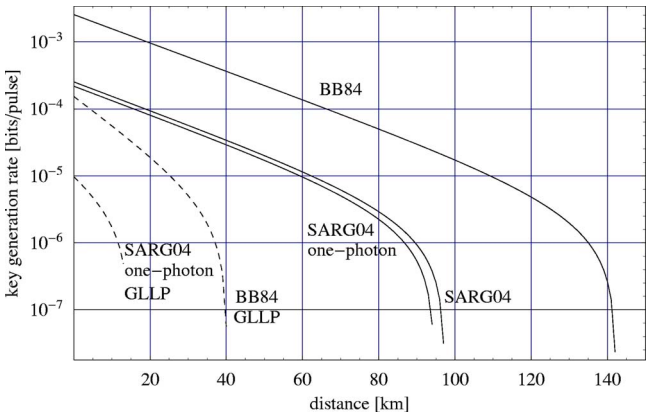


FIG. 7. (Color online) Simulation using the GYS parameters listed in Table II and $f(E_\mu)=1.22$, for both SARG04 and BB84 protocols. We compare the key generation rates of SARG04 and BB84 protocols with decoy states (solid curves) and without decoy states (dashed curves). The optimal mean photon numbers $\mu$ for all curves are used at all distances. Two curves of the SARG04 scheme using decoy are plotted, one with both single- and two-photon contributions and the other with only single-photon contributions. Also, curves of single-photon SARG04 and of BB84 protocols using GLLP without decoy are plotted. The maximal secure distance is 97.2 km for the SARG04 scheme and 141.8 km for BB84. However, the upper bounds for SARG04 and for BB84 protocols are exactly the same, namely, 207.68 km.

approximately half of that for the BB84 protocol. On the other hand, the yields stemmed from the dark count are the same for SARG04 and BB84. Similarly, for the bit error rate,

$$e_{n,\mathrm{SARG04}} = \left[ \eta_n \frac{e_{\mathrm{detector}}}{2} + (1-\eta_n) p_{\mathrm{dark}} \frac{1}{4} \right] / Y_{n,\mathrm{SARG04}}. \tag{41}$$

Thus, the overall gain and the overall QBER for the coherent state $|\sqrt{\mu}\rangle$ are, respectively,

$$Q_{\mu,\mathrm{SARG04}} = \frac{1}{2} p_{\mathrm{dark}} e^{-\eta\mu} + \left( \frac{e_{\mathrm{detector}}}{2} + \frac{1}{4} \right) (1 - e^{-\eta\mu}) \quad \text{and} \tag{42}$$

$$E_{\mu,\mathrm{SARG04}} = \left[ \frac{1}{4} p_{\mathrm{dark}} e^{-\eta\mu} + \frac{e_{\mathrm{detector}}}{2} (1 - e^{-\eta\mu}) \right] / Q_{\mu,\mathrm{SARG04}}. \tag{43}$$

Using these formulas for the error rates and the gains, we can compute the key generation rate for the SARG04 scheme with one-way decoy using Eq. (39).

### D. Simulations

Figure 7 compares the key generation rates of SARG04 and BB84 protocols, both using the one-way infinite-decoy method. For this simulation, we take $f(E_\mu)=1.22$ for simplicity and use the parameters from the experiments by Gobby *et al.* [31] as shown in Table II. We assumed that the detectors in both cases are rotated by the same angle in our model. The optimal mean photon numbers $\mu$ for the SARG04 and BB84 protocols are used at all distances. Two curves of the SARG04 scheme using decoy are plotted, one with both single- and two-photon contributions and the other with only single-photon contributions. Comparing these two curves, it can be seen that the two-photon part has a small contribution to the key generation rates at all distances. Also, curves of the single-photon SARG04 and the BB84 schemes using GLLP without decoy are plotted. We see that, by using decoy, higher key generation rates and longer secure distance can be achieved. A similar behavior for the BB84 protocol was shown in Ref. [11]. We note that the key generation rate for the BB84 scheme with GLLP in Fig. 1 of Ref. [11] is smaller than ours. This is because we used the optimal $\mu$ for all distances in Fig. 7 while $\mu$ proportional to $\eta$ was used in Ref. [11]. The maximal secure distance for the SARG04 protocol using decoy is 97.2 km, compared to 141.8 km for the BB84 scheme. The upper bound of the distance in the SARG04 scheme can be determined by finding the distances corresponding to $e_1=1/3$ and to $e_2=0.2265$; they are, respectively, 207.68 and 201.43 km. Thus, the upper bound of the distance is 207.68 km, at which the two-photon part is not secure but the single-photon part is. Interestingly, this bound of 207.68 km is exactly the same as the upper bound for the BB84 protocol [11]. It can be shown analytically that setting $e_1=1/3$ for the SARG04 case and setting $e_1=1/4$ for the BB84 case both give the same formula for $\eta_1$, specifically, $\eta_1=p_{\mathrm{dark}}/(1-4e_{\mathrm{detector}}+p_{\mathrm{dark}})$. (The formulas for $e_n$ and $Y_n$ of the BB84 scheme are of course different from that of the SARG04 scheme.) The optimal $\mu$'s for achieving the highest key generation rate at each distance for the SARG04 and BB84 protocols using decoy are plotted in Fig. 8. We can see that, when the misalignment of the detector is large (i.e., large $e_{\mathrm{detector}}$), the optimal mean photon number for the BB84 scheme is higher than that of the SARG04 one. On the other hand, when the misalignment is small, the optimal $\mu$ of the SARG04 scheme is higher at short and medium distances. In addition, the optimal $\mu$ of the SARG04 protocol can be higher than one in this case. This is reasonable since at short or medium distances, the bit error rate is not high and thus the key contribution from the two-photon part in the SARG04 scheme is relatively high; on the other hand, at long distances, the two-photon contribution is relatively small. Since the optimal $\mu$ for SARG04 and BB84 protocols is approximately constant for a large range of distances, the key generation rates for both SARG04 and BB84 schemes are in the order of $O(\eta)$.

TABLE II. Simulation parameters from Gobby-Yuan-Shields (GYS) experiments [31].

| Wavelength (nm) | $\alpha$ (dB/km) | $\eta_{\mathrm{Bob}}$ | $e_{\mathrm{detector}}$ | $p_{\mathrm{dark}}$ |
|---|---|---|---|---|
| 1550 | 0.21 | 4.5% | 3.3% | $1.7\times10^{-6}$ |

Figure 9 shows the simulation using the parameters from Fig. 4 of Ref. [23]. Our result shows that, under our assumption that Eve may perform the most general attack, the BB84 scheme is able to achieve both a higher secret key rate and a greater secure distance than the SARG04 one, whereas, un-

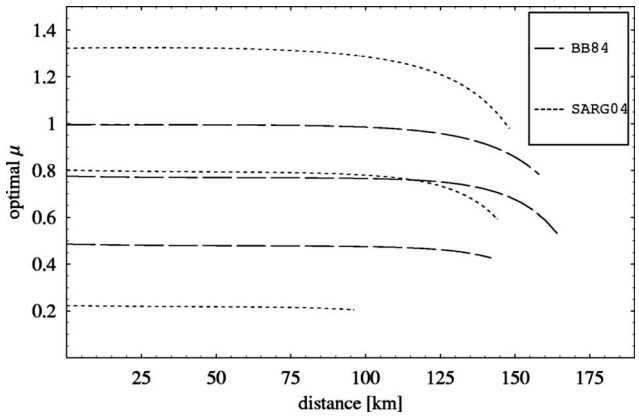


FIG. 8. The optimal $\mu$'s for achieving the highest key generation rate at each distance for the SARG04 scheme using Eq. (13) and for BB84 using Eq. (12). Three sets of parameters are plotted. The bottom two, middle two, and top two curves for BB84 and SARG04 protocols used the same parameters except for $e_{\text{detector}}$ (which are 0.033, 0.01, and 0.0001, respectively). The other common parameters are listed in Table II and $f(E_\mu)=1.22$. When the misalignment of the detector is large (i.e., large $e_{\text{detector}}$) as in the bottom two curves, the BB84 protocol uses a laser with a higher optimal mean photon number than the SARG04 one. When the misalignment becomes smaller as in the top two curves, the situation is reversed; the SARG04 protocol operates optimally with a higher $\mu$ than the BB84 one does. Also, note that the optimal $\mu$ for the SARG04 scheme can be higher than one.

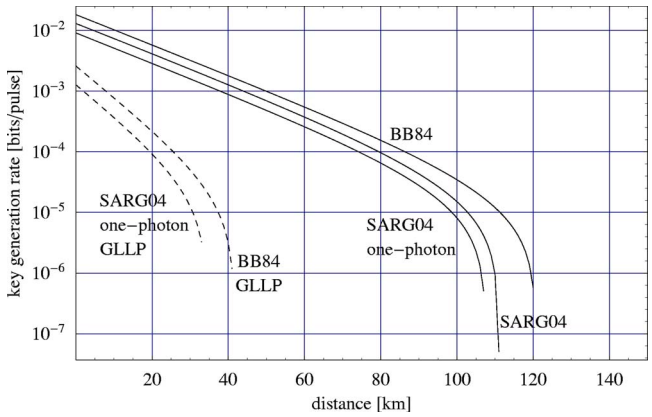


FIG. 9. (Color online) Simulation using $\alpha=0.25$, $\eta_{\text{Bob}}=0.1$, $e_{\text{detector}}=0$, $p_{\text{dark}}=10^{-5}$ (from Ref. [23]), and $f(E_\mu)=1$, for both SARG04 and BB84. We compare the key generation rates of SARG04 and BB84 with decoy states (solid curves) and without decoy states (dashed curves). The optimal mean photon numbers $\mu$ for all curves are used at all distance. Two curves of the SARG04 protocol using decoy are plotted, one with both single- and two-photon contributions and the other with only single-photon contributions. Also, curves of single-photon SARG04 and of BB84 schemes using GLLP without decoy are plotted.

der the assumption considered by Ref. [23] that Eve may only perform incoherent attacks, they observed the reverse phenomenon in Fig. 4 of their paper (i.e., the SARG04 protocol has a higher key rate and greater distance than the BB84 one). Another difference between our result and that of Ref. [23] is that we also consider contributions from the two-photon part.

In both Figs. 7 and 9, there are gaps between the one-photon SARG04 curves and the BB84 curves whether or not decoy is used. These gaps are mainly due to the decrease in the gain $Q_n$ and the increase in the bit error rate $e_n$ in the SARG04 scheme relative to the BB84 one. We can see this as follows. By comparing the yields of the SARG04 scheme in Eq. (40) and of the BB84 protocol in Eq. (20), in both the case of a large $e_{\text{detector}}$ (i.e., $\eta_n e_{\text{detector}} \gg (1-\eta_n)p_{\text{dark}}$, corresponding to Fig. 7) and the case of $e_{\text{detector}}=0$ (corresponding to Fig. 9), we can see that the yields in the SARG04 scheme is about half of that in the BB84 protocol; this means that $Q_n$ in the SARG04 scheme is also about half of that in the BB84 protocol. Similarly, by comparing the bit error rates of the SARG04 protocol in Eq. (41) and of the BB84 scheme in Eq. (21), we can see that $e_n$ in the SARG04 protocol is about twice of that in the BB84 scheme for both figures; this means that the amount of privacy amplification needed for the one-photon part of the SARG04 scheme is higher than that for the BB84 one (even when the mutual information between the bit and phase errors in the one-photon SARG04 scheme is taken into account). From the key generation rate equations in Eqs. (12) and (13), the decrease in $Q_n$ and the increase in $e_n$ both reduce the key generation rate of one-photon SARG04 scheme relative to the BB84 one, whether or not the decoy method is used. Furthermore, based on our simulations, we observe that the gap between SARG04 and BB84 protocols decreases as $e_{\text{detector}}$ decreases.

## VI. SUMMARY AND CONCLUDING REMARKS

We have provided lower and upper bounds on the bit error rates for the SARG04 scheme with two-way classical communications. Both the single-photon part and the two-photon part were considered. For the single-photon part, we have shown that the SARG04 protocol with two-way communications can tolerate a higher bit error rate than the SARG04 one with one-way communications. However, it does not mean that for some smaller bit error rate, the two-way SARG04 protocol has a higher key generation rate than the one-way version.

The upper bounds were found by considering a general intercept-and-resend attack by Eve. In this attack, she performs an arbitrary POVM and sends arbitrary states to Bob according to the measurement outcome. For the one-photon case, we have shown that such generality in her attack does not offer any advantage over a simple intercept-and-resend attack where she only performs measurement and sends the measurement results to Bob.

We have also studied the SARG04 scheme with a coherent source using the decoy-state method to achieve unconditional security. The key generation rate is significantly improved by combining the GLLP and the decoy-state ideas compared to the nondecoy protocols. This improved key rate for SARG04 is given by [20]

$$R_{\text{SARG04}} = -Q_\mu f(E_\mu) H_2(E_\mu) + Q_1[1 - H(Z_1|X_1)] + Q_2[1 - H(Z_2|X_2)]. \quad (44)$$

The first term is the fraction of EPR pairs spent for bit error

correction, the second term is the contribution to the key rate from the single-photon states, and the third term is the contribution from the two-photon states. In all our simulations, we found that the SARG04 protocol has a smaller key generation rate and a shorter secure distance than the BB84 scheme, using the combined GLLP and decoy formulation. Our results apply to the case where Eve performs the most general attack. This situation is different from that in Ref. [23], where they assumed that Eve performs an individual attack. We have shown that optimal mean photon number for the SARG04 scheme can be higher than that of the BB84 protocol for small misalignment errors in the detectors. Also, we observed that the optimal $\mu$ for the SARG04 and BB84 protocols is approximately constant for a large of distances. This means that the key generation rates for both the SARG04 and BB84 protocols increase linearly with the transmission efficiency $\eta$.

It is interesting to generalize our formulation of the SARG04 scheme with infinite decoys to the case of finite decoys, and to the case of using two-way classical communications with decoy. Also, our work can be extended to generalizations of the SARG04 scheme, the six-state SARG04 protocol [20] and the $N$-state protocol [24]. We leave them for future studies.

## APPENDIX A: DENSITY MATRICES OF ONE- AND TWO-PHOTON SARG04 PROTOCOLS

### 1. One-photon case

We consider the most general attack by Eve on all qubits sent by Alice. We focus on the density matrix of one qubit, denoted as $\rho_{\text{qubit}}$, which is obtained by tracing out all other qubits. Alice initially prepares $|\Psi\rangle_{AB}=(|0_z\rangle_A|\varphi_0\rangle_B+|1_z\rangle_A|\varphi_1\rangle_B)/\sqrt{2}$ and applies a random rotation $R^k$ on system $B$. After Eve's attack and Bob's inverse rotation and successful filtering, the final qubit pair state for a particular pair is

$$\rho_{\text{qubit}}=\sum_{k=0}^{3}\sum_{f}P((FR^{-k}E^{(f)}R^k)_B|\Psi\rangle_{AB}), \tag{A1}$$

where $P(|\Phi\rangle)=|\Phi\rangle\langle\Phi|$ is a projection operator associated with a pure state $|\Phi\rangle$, and $E^{(f)}$ is an arbitrary matrix indexed by $f$ that includes Eve's action on this qubit. Note that $E^{(f)}$ can be dependent on Eve's action on all the other pairs. For the moment, we consider the case that there is only one action by Eve (i.e., $f$ takes on one value). The (unnormalized) probability of $X$, $Y$, and $Z$ errors on $\rho_{\text{qubit}}$ due to $E$ can be explicitly computed using Eq. (2) as follows:

$$p_I=\frac{1}{2}|a_{11}+a_{22}|^2, \tag{A2}$$

$$p_X=\frac{1}{4}(|a_{12}+a_{21}|^2+|a_{11}-a_{22}|^2), \tag{A3}$$

$$p_Y=\frac{1}{4}((5a_{12}-3a_{21})a_{12}^*+(-3a_{12}+5a_{21})a_{21}^*+|a_{11}-a_{22}|^2), \tag{A4}$$

$$p_Z=(|a_{12}|^2+|a_{21}|^2)+\frac{1}{2}(|a_{11}-a_{22}|^2), \tag{A5}$$

where $E=\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}$. The bit error probability is $p_{bit}=p_X+p_Y$ and the phase error probability is $p_{\text{phase}}=p_Z+p_Y$. It can easily be shown that

$$p_{\text{phase}}=\frac{3}{2}p_{\text{bit}}, \tag{A6}$$

$$p_Y=p_{\text{bit}}/2+|a_{12}-a_{21}|^2/2. \tag{A7}$$

Note that the above equations involve the error *probabilities* of the particular pair conditioned on any configurations of the events including $X$, $Y$, and $Z$ errors for all the other pairs, but not the actual error rate of a realization of the protocol. In an actual protocol, the actual bit error rate $e_b$ is estimated and we want to relate it to the actual phase error rate $e_p$ and also to the actual $Y$ error rate $a$ (which is the counterpart of $p_Y$). However, we may not immediately conclude that $e_p=3e_b/2$ and $a\geqslant e_b/2$ since $p_{I/X/Y/Z}$ are only the probabilities of errors conditional on the events for other pairs; the errors of all the EPR pairs could be arbitrarily correlated. Nevertheless, both $e_p=3e_b/2$ and $a\geqslant e_b/2$ can be justified by using Azuma's inequality [35]. Let $N$ be the number of EPR pairs, $L=\{I,X,Y,Z\}$ be a label for a Pauli operator $n_L^{(l)}, l\in[1,N]$ be the actual number of $L$ errors on the first $l-1$ pairs, and $p_L^{(l)}$ be the probability of having an $L$ error on the $l$th pair conditional on any configuration of the events including the actual $X$, $Y$ or $Z$ error patterns on the first $l-1$ pairs. Note that we can identify $p_L^{(l)}$ to $p_L$. Applying Azuma's inequality to the random variable $n_L^N-\Sigma_{l=1}^N p_L^{(l)}$, one can show that $\Sigma_{l=1}^N p_L^{(l)}\to n_L^N$ with exponentially increasing probability as $N$ increases. Thus, after the bit error rate estimation, Alice and Bob perceive that fractions $e_b-a$, $3e_b/2-a$, and $a$ of EPR pairs suffer from $X$, $Z$, and $Y$ errors, respectively. They can associate this information with a density matrix to arrive at Eq. (9). A similar security analysis can be found in Ref. [36].

### 2. Two-photon case

In the two-photon case, Alice prepares a three-photon system $|\Psi\rangle_{ABE1}=(|0_z\rangle_A|\varphi_0\rangle_B|\varphi_0\rangle_{E1}+|1_z\rangle_A|\varphi_1\rangle_B|\varphi_1\rangle_{E1})/\sqrt{2}$ and applies a random rotation $R^k\otimes R^k$ on systems $B$ and $E1$. System $B$ is sent to Bob through Eve while system $E1$ is kept by Eve. We analyze this case in the same as in the one-photon case. We obtain $\rho_{\text{qubit}}$ by tracing out all other EPR pairs and system $E1$ of the pair under consideration and we arrive at $e_p\leqslant xe_b+g(x)$, $\forall\, x$, where $g(x)=(3-2x+\sqrt{6-6\sqrt{2}x+4x^2})/6$. In this case, we could not find any constraint on the actual fraction of $Y$ errors $a$. This means $e_b\geqslant a\geqslant 0$.

## APPENDIX B: PROOF OF THEOREM 3

Given two initial states $(p_{X_\alpha},p_{Y_\alpha},p_{Z_\alpha})=(e_b-a_\alpha,a_\alpha,\xi e_b-a_\alpha)$ and $(p_{X_\beta},p_{Y_\beta},p_{Z_\beta})=(e_b-a_\beta,a_\beta,\xi e_b-a_\beta)$, where $a_\beta$

$> a_\alpha$, we apply the same sequence of B and P steps starting with a B step to the two initial states, thus giving rise to two sequences of states (the $\alpha$ sequence and the $\beta$ sequence). We want to show that the final state of the $\alpha$ sequence leads to a smaller key generation rate in Eq. (33) than that of the $\beta$ sequence. This implies that the key generation rate is an increasing function of $a$.

Starting with a pool of EPR pairs with state $(p_X, p_Y, p_Z)$, applying a B step leads to a smaller set of surviving pairs with a new state $(p'_X, p'_Y, p'_Z)$ described by Eqs. (22)–(25). Similarly, beginning with $(p_X, p_Y, p_Z)$, a P step leads to a new state described by Eqs. (26)–(29).

We apply a change of variables:

$$t_Z = p_X + p_Y, \tag{B1}$$

$$t_X = p_Y + p_Z, \tag{B2}$$

$$\Delta = p_Z - p_Y. \tag{B3}$$

We start with the hypothesis that in any stage of the $\alpha$ and $\beta$ sequences, $t_{Z_\beta} = t_{Z_\alpha}$, $t_{X_\beta} \leqslant t_{X_\alpha}$, and $\Delta_\beta \leqslant \Delta_\alpha$. If this is true and if $t_{X_\alpha} \leqslant 1/2$, the key generation rate, $1 - H_2(t_Z) - H_2(t_X)$, at any stage of the $\alpha$ sequence is smaller and theorem 3 follows.

First, we can verify that the hypothesis is true initially by noticing that $t_{Z_\beta} = t_{Z_\alpha} = e_b$, $t_{X_\beta} = t_{X_\alpha} = \xi e_b$ and $\Delta_\beta = \xi e_b - 2a_\beta < \Delta_\alpha = \xi e_b - 2a_\alpha$. Next, we show that given the hypothesis is true for the current stage, it is also true for the next stage when a B step is applied. In the new variables, the new state after a B step becomes

$$t'_Z = t_Z^2 / p_S, \tag{B4}$$

$$t'_X = [t_X - t_X^2 + \Delta(1 - 2t_Z - \Delta)]/p_S, \tag{B5}$$

$$\Delta' = [t_X(1 - 2t_Z) + \Delta(1 - 2t_X)]/p_S, \tag{B6}$$

$$p_S = 1 - 2t_Z + 2t_Z^2. \tag{B7}$$

Given that $t_{X_\beta} \leqslant t_{X_\alpha}$ and $\Delta_\beta \leqslant \Delta_\alpha$, we express the state of sequence $\beta$ in terms of that of sequence $\alpha$:

$$t'_{Z_\beta} = t'_{Z_\alpha}, \tag{B8}$$

$$t'_{X_\beta} = t'_{X_\alpha} - [t_{X_{\alpha-\beta}}(1 - 2t_{X_\alpha} + t_{X_{\alpha-\beta}}) + \Delta_{\alpha-\beta}(1 - 2t_{Z_\beta} - \Delta_\alpha - \Delta_\beta)]/p_S, \tag{B9}$$

$$\Delta'_\beta = \Delta'_\alpha - [t_{X_{\alpha-\beta}}(1 - 2t_{Z_\beta} - 2\Delta_\beta) + \Delta_{\alpha-\beta}(1 - 2t_{X_\alpha})]/p_S, \tag{B10}$$

$$p_S = 1 - 2t_Z + 2t_Z^2, \tag{B11}$$

where $t_{X_{\alpha-\beta}} = t_{X_\alpha} - t_{X_\beta} \geqslant 0$ and $\Delta_{\alpha-\beta} = \Delta_\alpha - \Delta_\beta \geqslant 0$. Obviously, the hypothesis for the primed variables is true if $(1 - 2t_Z - 2\Delta) \geqslant 0$, $t_X \leqslant 1/2$, and $t_Z \leqslant 1/2$ at any stage of the $\alpha$ and $\beta$ sequence. We will show the first inequality later and impose the last two inequalities as condition (ii) of the theorem.

We consider the new state after a P step is applied and show that the hypothesis is also true for this new state. The new state after a P step is

$$t'_Z = 3t_Z(1 - t_Z)^2 + t_Z^3, \tag{B12}$$

$$t'_X = 3t_X^2(1 - t_X) + t_X^3, \tag{B13}$$

$$\Delta' = 3\Delta^2(1 - 2t_Z - \Delta) + \Delta^3. \tag{B14}$$

It is obvious that $t'_X$ increases with $t_X$, which implies that $t'_{X_\beta} \leqslant t'_{X_\alpha}$. Also, $\Delta'$ increases with $\Delta$ provided that $(1 - 2t_Z - \Delta) \geqslant 0$ and $\Delta \geqslant 0$, which implies that $\Delta'_\beta \leqslant \Delta'_\alpha$. The first inequality is satisfied if $(1 - 2t_Z - 2\Delta) \geqslant 0$, which will be shown later. We first show that $\Delta \geqslant 0$.

*Claim 1.* After the initial B step, or after any B/P step that follows, $\Delta \geqslant 0$ holds.

*Proof.* Before the initial B step is applied, we have

$$\Delta = \xi e_b - 2a, \tag{B15}$$

$$\geqslant \xi e_b - 2e_b, \tag{B16}$$

$$\geqslant -e_b, \tag{B17}$$

where the last inequality is due to $\xi \geqslant 1$. After the initial B step, from Eq. (B6), we have $\Delta' \geqslant 0$ if the following condition is satisfied:

$$\Delta \geqslant -\frac{\xi e_b(1 - 2e_b)}{1 - 2\xi e_b}. \tag{B18}$$

Since the right-hand side is smaller than $-e_b$, this condition is satisfied after the first B step, which means that $\Delta' \geqslant 0$ after the first B step. Furthermore, from Eq. (B6) and Eq. (B14), we conclude that $\Delta' \geqslant 0$ after any B step or P step following the initial B step. ■

*Claim 2.* $1 - 2t_Z - 2\Delta \geqslant 0$ always holds if $e_b \leqslant (1 + 4a)/(2(1 + \xi))$ [which is condition (i) of the theorem].

*Proof.* Before the initial B step, we can easily see

$$1 - 2t_Z - 2\Delta = 1 - 2(1 + \xi)e_b + 4a \geqslant 0 \tag{B19}$$

because $e_b \leqslant (1 + 4a)/(2(1 + \xi))$. After a B step

$$1 - 2t'_Z - 2\Delta' = 1 - [2t_Z^2 + 2t_X(1 - 2t_Z) + 2\Delta(1 - 2t_X)]/p_S \tag{B20}$$

$$= (1 - 2t_Z - 2\Delta)(1 - 2t_X)/p_S, \tag{B21}$$

which is non-negative when $1 - 2t_Z - 2\Delta \geqslant 0$.

After a P step,

$$1 - 2t'_Z = (1 - 2t_Z)^3 \tag{B22}$$

so

$$1 - 2t'_Z - 2\Delta' = (1 - 2t_Z)^3 - 6\Delta^2(1 - 2t_Z) + 4\Delta^3 \tag{B23}$$

$$= (1 - 2t_Z - 2\Delta)[(1 - 2t_Z)^2 + 2\Delta(1 - 2t_Z - \Delta)], \tag{B24}$$

which is non-negative when $1 - 2t_Z - 2\Delta \geqslant 0$ and $\Delta \geqslant 0$. □

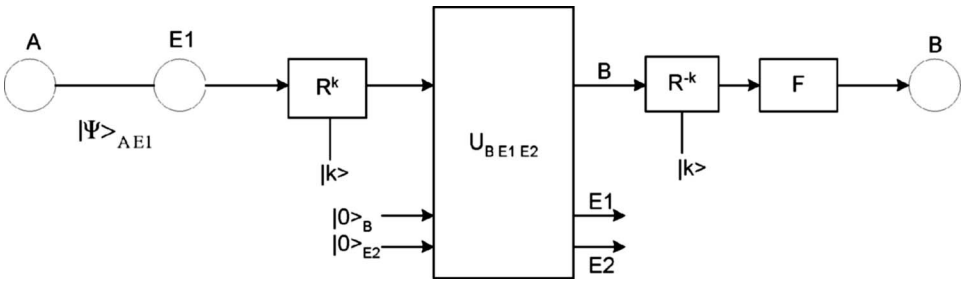


FIG. 10. A POVM attack by Eve realized by $U_{BE_1E_2}$.

## APPENDIX C: PROOF OF THEOREMS 4 AND 5

In this appendix, we will prove that a general POVM attack by Eve induces a bit error rate of at least $\frac{1}{3}$ for the single-photon case. To do this, we will first consider a special case of this attack where Eve always sends only SARG04 states to Bob. Then building on the proof of this special case, we will show that the minimum bit error rate is $\frac{1}{3}$ for the general POVM attack where Eve sends arbitrary states to Bob. At last, we will generalize the proof to the case of two photons, showing that it is possible to derive the minimum bit error rate even for this case.

Before we begin, we note that $R^4=I$. This allows us to adopt the following notation:

$$|\varphi_{m+k}\rangle = R^{-m}|\varphi_k\rangle, \quad \forall\, m,\, k \in \mathbb{Z}, \tag{C1}$$

where the subscripts of the SARG04 states are taken in module 4.

### 1. Eve sending SARG04 states

A block diagram showing an attack by Eve is depicted in Fig. 10. First, Alice prepares a bipartite entangled state $|\Psi\rangle_{AE_1}=|0_z\rangle_A|\varphi_0\rangle_{E_1}+|1_z\rangle_A|\varphi_1\rangle_{E_1}$. After randomly applying a rotation $R^k$, she sends the $E_1$ qubit to Eve, who will then perform a POVM $\{W_m^\dagger W_m : m=0,\ldots,3\}$ on $E_1$, which is realized by an unitary operator $U_{BE_1E_2}$. When the measurement result is $m$, Eve sends the state $|\varphi_m\rangle_B$ to Bob. We will obtain the density matrix of Alice and Bob $\rho_{AB}$ and minimize the bit error rate $[\mathrm{Tr}(\rho_{AB})]^{-1}[\langle\Psi^+|\rho_{AB}|\Psi^+\rangle+\langle\Psi^-|\rho_{AB}|\Psi^-\rangle]$ over $W_m$'s.

The input state transforms as follows:

$$\sum_k (\mathbf{I}_A \otimes R_{E_1}^k)|\Psi\rangle_{AE_1}|k\rangle_K \tag{C2}$$

$$\xrightarrow{U} \sum_k \sum_{m=0}^{3} [\mathbf{I}_A \otimes (W_m R^k)_{E_1}]|\Psi\rangle_{AE_1}|m\rangle_{E_2}|\varphi_m\rangle_B|k\rangle_K \tag{C3}$$

$$\xrightarrow{R^{-k}F} \sum_k \sum_{m=0}^{3} [|0_z\rangle_A(W_m R^k|\varphi_0\rangle_{E_1}) + |1_z\rangle_A(W_m R^k|\varphi_1\rangle_{E_1})] \otimes |m\rangle_{E_2}(FR^{-k}|\varphi_m\rangle_B)|k\rangle_K. \tag{C4}$$

We then trace out systems $E_1$, $E_2$, and $K$ to get the final density matrix between Alice and Bob:

$$\rho_{AB} = \sum_{k=0}^{3}\sum_{m=0}^{3} (a_{mk}^{00}|0_z\rangle_A\langle 0_z| + a_{mk}^{01}|0_z\rangle_A\langle 1_z| + a_{mk}^{10}|1_z\rangle_A\langle 0_z| + a_{mk}^{11}|1_z\rangle_A\langle 1_z|) \tag{C5}$$

$$\otimes F|\varphi_{m+k}\rangle_B\langle\varphi_{m+k}|F^\dagger, \tag{C6}$$

where

$$a_{mk}^{00} = |\langle 0_z|W_m|\varphi_{-k}\rangle|^2 + |\langle 1_z|W_m|\varphi_{-k}\rangle|^2, \tag{C7}$$

$$a_{mk}^{01} = \langle 0_z|W_m|\varphi_{-k}\rangle\langle 0_z|W_m|\varphi_{1-k}\rangle^* + \langle 1_z|W_m|\varphi_{-k}\rangle\langle 1_z|W_m|\varphi_{1-k}\rangle^*, \tag{C8}$$

$$a_{mk}^{10} = (a_{mk}^{01})^*, \tag{C9}$$

$$a_{mk}^{11} = |\langle 0_z|W_m|\varphi_{1-k}\rangle|^2 + |\langle 1_z|W_m|\varphi_{1-k}\rangle|^2. \tag{C10}$$

Here, we have used the notation in Eq. (C1). Note that $\rho_{AB}$ is a separable density matrix as we have explicitly constructed it to be, and because of that, no entanglement exists and thus no secure key can be distilled. We can compute the unnormalized bit error rate $p_X+p_Y$ as

$$p_X + p_Y = {}_{AB}\langle 0_z 1_z|\rho_{AB}|0_z 1_z\rangle_{AB} + {}_{AB}\langle 1_z 0_z|\rho_{AB}|1_z 0_z\rangle_{AB} \tag{C11}$$

$$= \sum_{k+m=0} a_{mk}^{11}\frac{1}{4} + \sum_{k+m=1} a_{mk}^{00}\frac{1}{4} + \sum_{k+m=2}\left(a_{mk}^{00}\frac{1}{2} + a_{mk}^{11}\frac{1}{4}\right) + \sum_{k+m=3}\left(a_{mk}^{11}\frac{1}{2} + a_{mk}^{00}\frac{1}{4}\right) \tag{C12}$$

$$= \sum_{m=0}^{3}\sum_{j=0}^{1} \langle j_z|W_m L_m W_m^\dagger|j_z\rangle, \tag{C13}$$

where

$$L_m = \frac{1}{2}|\varphi_{1+m}\rangle\langle\varphi_{1+m}| + |\varphi_{2+m}\rangle\langle\varphi_{2+m}| + \frac{1}{2}|\varphi_{3+m}\rangle\langle\varphi_{3+m}|. \tag{C14}$$

Since $W_m$ is some $2\times 2$ matrix (not necessary Hermitian), the problem of finding $W_m$ is broken into finding two independent $1\times 2$ vectors $\langle 0_z|W_m$ and $\langle 1_z|W_m$.

In order to normalize the bit error rate, we find

$$\mathrm{Tr}(\rho_{AB}) = \sum_{i,j\in\{0,1\}} {}_{AB}\langle i_z j_z|\rho_{AB}|i_z j_z\rangle_{AB} \tag{C15}$$

$$= \sum_{m=0}^{3} \sum_{j=0}^{1} \langle j_z | W_m B_m W_m^\dagger | j_z \rangle, \tag{C16}$$

where

$$B_m = \frac{1}{2} |\varphi_{0+m}\rangle\langle\varphi_{0+m}| + |\varphi_{1+m}\rangle\langle\varphi_{1+m}| + \frac{3}{2} |\varphi_{2+m}\rangle\langle\varphi_{2+m}| + |\varphi_{3+m}\rangle\langle\varphi_{3+m}|. \tag{C17}$$

Therefore, the normalized bit error rate is

$$e_b = \frac{\sum_{m=0}^{3} \sum_{j=0}^{1} \langle j_z | W_m L_m W_m^\dagger | j_z \rangle}{\sum_{m=0}^{3} \sum_{j=0}^{1} \langle j_z | W_m B_m W_m^\dagger | j_z \rangle}. \tag{C18}$$

We want to minimize $e_b$ over the eight independent $1 \times 2$ vectors $\langle j_z | W_m$. At least one of the eight must be nonzero, otherwise all $W_m$ would be zero and there would be no qubits sent to Bob. Since $e_b$ is not a sum of eight independent ratios, i.e.,

$$e_b \neq \sum_{m=0}^{3} \sum_{j=0}^{1} \frac{\langle j_z | W_m L_m W_m^\dagger | j_z \rangle}{\langle j_z | W_m B_m W_m^\dagger | j_z \rangle}, \tag{C19}$$

it may appear at first sight that the minimization of $e_b$ is not trivial. However, it turns out that we can minimize each ratio independently and set $e_b$ to be the smallest ratio by assigning zeros to the other seven vectors. We show this by the following claim.

*Claim 3.* Given two ratios $a_1/a_2$ and $b_1/b_2$, if $a_1/a_2 \leq b_1/b_2$, then $a_1/a_2 \leq (a_1+b_1)/(a_2+b_2)$.

Therefore, we consider separately minimizing each ratio, which can be written as

$$\frac{\langle c_{jm} | B_m^{-1/2} L_m B_m^{-1/2} | c_{jm} \rangle}{\langle c_{jm} | c_{jm} \rangle}, \tag{C20}$$

where $\langle c_{jm}| = \langle j_z | W_m B_m^{1/2}$ is a $1 \times 2$ vector. The minimizing $c_{jm}$ is the eigenvector of $B_m^{-1/2} L_m B_m^{-1/2}$ corresponding to the minimum eigenvalue. The two eigenvalues are 0.6 and $\frac{1}{3}$ for all $m$. Thus, the minimum $e_b$ is $\frac{1}{3}$. A POVM $\{W_m^\dagger W_m\}$ that is compatible with these eigenvectors is $W_m^\dagger W_m = |\varphi_m\rangle\langle\varphi_m|/2, m=0,\ldots,3$, which is the trivial intercept-and-resend attack.

### 2. Eve sending arbitrary states

Now, instead of sending the four SARG04 states $|\varphi_i\rangle, i=0,\ldots,3$, we assume Eve sends any number $G$ of arbitrary states. We label these states as $|\sigma_0^g\rangle$, $g=0,\ldots,G-1$. For the sake of making the analysis of this case parallel to that of the previous case of sending SARG04 states, we associate three extra states (with certain symmetry) to each arbitrary state and we label all states as follows:

$$|\sigma_i^g\rangle, \quad i=0,\ldots,3, g=0,\ldots,G-1. \tag{C21}$$

We can view the states as divided into sets of four with a total of $G$ sets. The $i=0$ states are the original arbitrary states and are called the representative states of its set; the $i=1,2,3$ states are the extra states introduced. The POVM elements $\{W_i^{g\dagger} W_i^g\}$ corresponding to the states are also indexed in the same way. Along the same lines as the SARG04 states, we define the extra states to have a rotational symmetry that satisfies $|\sigma_{m+k}^g\rangle = R^{-k} |\sigma_m^g\rangle, \forall\ g$. This symmetry requirement makes the analysis much easier since it resembles the analysis for the case of sending SARG04 states. Note that the introduction of the three extra states in each set does not lose any generality, since if the extra states are not needed in the minimization of the bit error rate, their corresponding POVM elements will eventually be found to be zeros.

The analysis of this case basically goes as before by replacing $|\varphi_i\rangle$ with $|\sigma_i^g\rangle$. The final normalized bit error rate is

$$e_b = \frac{\sum_{g=0}^{G-1} \sum_{m=0}^{3} \sum_{j=0}^{1} \langle j_z | W_m^g L_m^g W_m^{g\,\dagger} | j_z \rangle}{\sum_{g=0}^{G-1} \sum_{m=0}^{3} \sum_{j=0}^{1} \langle j_z | W_m^g B_m^g W_m^{g\,\dagger} | j_z \rangle}, \tag{C22}$$

which has the same form as before but with different $L_m^g$'s and $B_m^g$'s. As before, both of them are weighted sums of the outer products of the SARG04 states $\Sigma_{i=1}^4 \kappa_{im} |\varphi_{i+m}\rangle\langle\varphi_{i+m}|$. ($\kappa_{im}$'s for $B_m^g$ and $L_m^g$ are different.) The difference is that now $\kappa_{im}$'s are no longer constant, but dependent on the representative state of each set sent by Eve $|\sigma_0^g\rangle$. Thus, $W_m^g$ is also a function of this state. Since claim 3 says that we can minimize each term of $e_b$ separately and since $|\sigma_0^g\rangle$ is arbitrary anyway, we only need to focus on $L_0^0$ and $B_0^0$ and minimize the eigenvalues of $(B_0^0)^{-1/2} L_0^0 (B_0^0)^{-1/2}$ (which correspond to the bit error rate). The two eigenvalues are

$$\frac{2-c}{4-c} \quad \text{and} \quad \frac{2+c}{4+c}, \tag{C23}$$

where $|\sigma_0^0\rangle \triangleq \sigma_{00}|0_z\rangle + \sigma_{01}|1_z\rangle$, $c = |\sigma_{00}^2 + \sigma_{01}^2| / (|\sigma_{00}|^2 + |\sigma_{01}|^2) \leq 1$. The minimum of the first eigenvalue is $\frac{1}{3}$ at $c=1$ and the second eigenvalue is in $[0.5, 0.6]$. Therefore, we conclude that, for the one-photon SARG04 case, the minimum bit error rate caused by Eve using a general POVM intercept-and-resend attack with arbitrary states sent is $\frac{1}{3}$. Note that $c=1$ corresponds to the phase difference between $\sigma_{00}$ and $\sigma_{01}$ being 0 or $\pi$, under our specific choice of the SARG04 states. Also, the bit error rate of $1/3$ can be achieved with any assignment of $\sigma_{00}$ and $\sigma_{01}$ (of course, different assignments of them give rise to different POVM elements), as long as they are in phase or completely out of phase.

### 3. Two-photon case

We can extend this proof to the two-photon SARG04 case easily. The initial state becomes $|\Psi\rangle_{AE_1} = |0_z\rangle_A |\varphi_0\varphi_0\rangle_{E_1} + |1_z\rangle_A |\varphi_1\varphi_1\rangle_{E_1}$, as Alice emits two photons to Eve. Alice applies rotation $R^k \otimes R^k$ to the two-qubit system $E_1$ before it is sent to Eve. Eve then performs a POVM on $E_1$ and, based on the measurement outcome, sends system $B$ to Bob as before. The analysis for this case is the same as the one-photon case, with the change of $E_1$ being a two-qubit system.

Because of this change, the matrices $W_m^g$, $L_m^g$, and $B_m^g$ in the analysis are subsequently changed to have dimension $4\times 4$. Both $L_m^g$ and $B_m^g$ are enlarged by replacing every tensor product of the form $|\varphi_m\rangle\langle\varphi_m|$ by $|\varphi_m\varphi_m\rangle\langle\varphi_m\varphi_m|$, with no change to the corresponding coefficients. We can carry the same analysis as the single-photon case and arrive at the eigenvalues of $(B_0^0)^{-1/2}L_0(B_0^0)^{-1/2}$ to determine the bit error rate.[2] Because of the increased dimension in this case, we could not directly solve for the eigenvalues in terms of $|\sigma_0^g\rangle$. Instead, we parameterize the eigenvalues with two parameters $\theta_z$ and $\theta_y$ and plot the eigenvalues against these two parameters. These two parameters come from the fact that any state can be written as a rotation about the $z$ axis on $|\varphi_0\rangle$ (which is not equal to $|0_z\rangle$ or $|1_z\rangle$) followed a rotation about the $y$ axis, i.e., $|\sigma_0^0\rangle = R_y(\theta_y)R_z(\theta_z)|\varphi_0\rangle$. Using this definition for $|\sigma_0^0\rangle$, we found, from plots of the eigenvalues as functions of $\theta_y$ and $\theta_z$, that the eigenvalues are not dependent on $\theta_y$ and reach minimum when $\theta_z = 0, \pi$. The minimum eigenvalue (and thus the minimum bit error rate) is $(3-\sqrt{2})/7 \approx 22.65\%$. A POVM that gives rise to this minimum bit error rate is

$$W_m^\dagger W_m = P(\lambda_+|\varphi_m\rangle|\varphi_m\rangle + \lambda_-|\varphi_{m+2}\rangle|\varphi_{m+2}\rangle), \quad m = 0, \ldots, 3, \tag{C24}$$

$$W_{\text{vac}}^\dagger W_{\text{vac}} = P(|\varphi_0\rangle|\varphi_2\rangle - |\varphi_2\rangle|\varphi_0\rangle)/2 \tag{C25}$$

$$= P(|\varphi_3\rangle|\varphi_1\rangle - |\varphi_1\rangle|\varphi_3\rangle)/2, \tag{C26}$$

where $\lambda_\pm = (\pm 2 + \sqrt{2})/4$ and $P(|\Phi\rangle) = |\Phi\rangle\langle\Phi|$ is a projection operator associated with a pure state $|\Phi\rangle$. Eve sends $|\varphi_m\rangle$ to Bob when the measurement outcome is $m \in [0,3]$. Note that $W_{\text{vac}}^\dagger W_{\text{vac}}$ never occurs, since the four states sent by Alice, $|\varphi_m\rangle|\varphi_m\rangle, m \in [0,3]$, are orthogonal to the state $W_{\text{vac}}^\dagger W_{\text{vac}}$ projects onto.

[2] Actually, the pseudoinverse of $B_0^0$ is used since $B_0^0$ (and $L_0^0$) has rank 3. The analysis is not affected since the nullspaces of $B_0^0$ and $L_0^0$ are the same.


[1] C. H. Bennett and G. Brassard, in Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing (IEEE Press, New York, 1984), pp. 175–179.
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[4] D. Mayers, J. ACM **48**, 351 (2001); preliminary version in D. Mayers, *Advances in Crytology–Proceedings of Crypto '96*, Vol. 1109 of Lecture Notes in Computer Science, edited by N. Koblitz (Springer-Verlag, New York, 1996), pp. 343–357.
[5] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, in Proceedings of the 32nd Annual ACM Symposium on Theory of Computing (ACM Press, New York, 2000), pp. 715–724.
[6] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[7] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[8] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **5**, 325 (2004).
[9] H. Inamori, N. Lütkenhaus, and D. Mayers, e-print quant-ph/0107017.
[10] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[11] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[12] H.-K. Lo, e-print quant-ph/0509076.
[13] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[14] X.-B. Wang, Phys. Rev. A **72**, 012322 (2005).
[15] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).
[16] J. W. Harrington, J. M. Ettinger, R. J. Hughes, and J. E. Nordholt, e-print quant-ph/0503002.
[17] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, e-print quant-ph/0503192.
[18] X. Ma, C.-H. F. Fung, F. Dupuis, K. Chen, K. Tamaki, and H.-K. Lo (in preparation).
[19] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).
[20] K. Tamaki and H.-K. Lo, e-print quant-ph/0412035.
[21] D. Bruss, Phys. Rev. Lett. **81**, 3018 (1998).
[22] H.-K. Lo, Quantum Inf. Comput. **1**, 81 (2001).
[23] C. Branciard, N. Gisin, B. Kraus, and V. Scarani, Phys. Rev. A **72**, 032301 (2005).
[24] M. Koashi, e-print quant-ph/0507154.
[25] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[26] K. Tamaki, M. Koashi, and N. Imoto, Phys. Rev. Lett. **90**, 167904 (2003).
[27] K. Tamaki and N. Lütkenhaus, Phys. Rev. A **69**, 032316 (2004).
[28] M. Koashi, Phys. Rev. Lett. **93**, 120501 (2004).
[29] D. Gottesman and H.-K. Lo, IEEE Trans. Inf. Theory **49**, 457 (2003).
[30] H. F. Chau, Phys. Rev. A **66**, 060302(R) (2002).
[31] C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004).
[32] J.-B. Li and X.-M. Fang, e-print quant-ph/0509077.
[33] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[34] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).
[35] K. Azuma, Tohoku Math. J. **19**, 357 (1967).
[36] J.-C. Boileau, K. Tamaki, J. Batuwantudawe, R. Laflamme, and J. M. Renes, Phys. Rev. Lett. **94**, 040503 (2005).