Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw

Kiyoshi Tamaki,[1,2] Hoi-Kwong Lo,[3] Chi-Hang Fred Fung,[4] and Bing Qi[3]

[1]*NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya Atsugi-Shi, Kanagawa 243-0198, Japan*

[2]*National Institute of Information and Communications Technology, 4-2-1 Nukui-Kita, Koganei, Tokyo 184-8795, Japan*

[3]*Center for Quantum Information and Quantum Control, Department of Electrical & Computer Engineering and Department of Physics, University of Toronto, Toronto, Ontario M5S 3G4, Canada*

[4]*Department of Physics and Center of Computational and Theoretical Physics, University of Hong Kong, Pokfulam Road, Hong Kong*

In this paper, we study the unconditional security of the so-called measurement-device-independent quantum key distribution (MDIQKD) with the basis-dependent flaw in the context of phase encoding schemes. We propose two schemes for the phase encoding: The first one employs a phase locking technique with the use of non-phase-randomized coherent pulses, and the second one uses conversion of standard Bennett-Brassard 1984 (BB84) phase encoding pulses into polarization modes. We prove the unconditional security of these schemes and we also simulate the key generation rate based on simple device models that accommodate imperfections. Our simulation results show the feasibility of these schemes with current technologies and highlight the importance of the state preparation with good fidelity between the density matrices in the two bases. Since the basis-dependent flaw is a problem not only for MDIQKD but also for standard quantum key distribution (QKD), our work highlights the importance of an accurate signal source in practical QKD systems.

PACS number(s): 03.67.Dd

I. INTRODUCTION

Quantum key distribution (QKD) is often said to be unconditionally secure [1–3]. More precisely, QKD can be proven to be secure against any eavesdropping *given* that the users' (Alice and Bob) devices satisfy some requirements, which often include mathematical characterization of users' devices as well as the assumption that there is no side channel. This means that no one can break the mathematical model of QKD, however, in practice, it is very difficult for practical devices to meet the requirements, leading to the breakage of the security of practical QKD systems. Actually, some attacks on QKD have been proposed and demonstrated successfully against practical QKD systems [4,5].

To combat the practical attacks, some countermeasures [6], including the device-independent security proof idea [7], have been proposed. The device-independent security proof is very interesting from the theoretical viewpoint, however, it cannot apply to practical QKD systems where loopholes in testing Bell's inequality [8] cannot be closed. As for the experimental countermeasures, battle testing of the practical detection unit has attracted many researchers' attentions [5] since the most successful practical attack so far is to exploit the imperfections of the detectors.

Recently, a very simple and very promising idea, which is called a measurement-device-independent QKD (MDIQKD) has been proposed by Lo, Curty, and Qi [9]. In this scheme, neither Alice nor Bob performs any measurement, but they only send out quantum signals to a measurement unit (MU). MU is a willing participant of the protocol, and MU can be a network administrator or a relay. However, MU can be untrusted and completely under the control of the eavesdropper (Eve). After Alice and Bob send out signals, they wait for MU's announcement of whether she has obtained the successful detection, and proceed to the standard postprocessing of their sifted data, such as error rate estimation, error correction,

and privacy amplification. The basic idea of MDIQKD is based on a reversed EPR-based QKD protocol [10], which is equivalent to EPR-based QKD [11] in the sense of the security, and MDIQKD is remarkable because it removes *all* the potential loopholes of the detectors without sacrificing the performance of standard QKD since Alice and Bob do not detect any quantum signals from Eve. Moreover, it is shown in Ref. [9] that MDIQKD with an infinite number of decoy states and polarization encoding can cover about twice the distance of standard decoyed QKD, which is comparable to EPR-based QKD. The only assumption needed in MDIQKD is that the preparation of the quantum signal sources by Alice and Bob is (almost) perfect and carefully characterized. We remark that the characterization of the signal source should be easier than that of the detection unit since the characterization of the detection unit involves the estimation of the response of the devices to unknown input signals sent from Eve.

With MDIQKD in our hand, we do not need to worry about imperfections of MU any more, and we should focus our attention more to the imperfections of signal sources. One of the important imperfections of the sources is the basis-dependent flaw that stems from the discrepancy of the density matrices corresponding to the two bases in Bennett-Brassard 1984 (BB84) states. The security of standard BB84 with the basis-dependent flaw has been analyzed in Refs. [12–14] which show that the basis-dependent flaw decreases the achievable distance. Thus, in order to investigate the practicality of MDIQKD, we need to generalize the above works to investigate the security of MDIQKD under the imperfection. Another problem in MDIQKD is that the first proposal is based on polarization encoding [9], however, in some situations where birefringence effect in optical fiber is highly time dependent, we need to consider MDIQKD with phase encoding rather than polarization encoding. In this paper, we study the above issues simultaneously.

We first propose two schemes of the phase encoding MDIQKD, one employs phase locking of two separate laser sources and the other one uses the conversion of phase encoding into polarization encoding. Then, we prove the unconditional security of these schemes with basis-dependent flaw by generalizing the quantum coin idea [12–14]. Based on the security proof, we simulate the key generation rate with realistic parameters; especially we employ a simple model to evaluate the basis-dependent flaw due to the imperfection of the phase modulators. Our simulation results imply that the first scheme covers shorter distances and may require less accuracy of the state preparation, while the second scheme can cover much longer distances when we can prepare the state very precisely. We note that in this paper we consider the most general type of attacks allowed by quantum mechanics and establish unconditional security for our protocols.

This paper is organized as follows. In Sec. II, we give a generic description of MDIQKD protocol, and we propose our schemes in Secs. III and IV. Then, we prove the unconditional security of our schemes in Sec. V, and we present some simulation results of the key generation rate based on realistic parameters in Sec. VI. Finally, we summarize this paper in Sec. VII.

II. PROTOCOL

In this section, we introduce MDIQKD protocol whose description is generic for all the schemes that we will introduce in the following sections. The MDIQKD protocol runs as follows.

Step (1). Each of Alice and Bob prepares a signal pulse and a reference pulse, and each of Alice and Bob applies phase modulation to the signal pulse, which is randomly chosen from 0, $\pi/2$, π, and $3\pi/2$. Here, $\{0,\pi\}$ ($\{\pi/2,3\pi/2\}$) defines the X (Y) basis. Alice and Bob send both pulses through quantum channels to Eve who possesses MU.

Step (2). MU performs some measurement, and announces whether the measurement outcome is successful or not. It also broadcasts whether the successful event is the detection of type 0 or type 1 (the two types of successful outcomes correspond to two specific Bell states [15]).

Step (3). If the measurement outcome is successful, then Alice and Bob keep their data. Otherwise, they discard the data. When the outcome is successful, Alice and Bob broadcast their bases and they keep the data only when the bases match, which we call sifted key. Depending on the type of the successful event and the basis that they used, Bob may or may not perform bit flip on his sifted key.

Step (4). Alice and Bob repeat steps (1)–(3) many times until they have a large enough number of the sifted key.

Step (5). They sacrifice a portion of the data as the test bits to estimate the bit error rate and the phase error rate on the remaining data (code bits).

Step (6). If the estimated bit error and phase error rates are too high, then they abort the protocol; otherwise they proceed.

Step (7). Alice and Bob agree over a public channel on an error correcting code and on a hash function depending on the bit and phase error rate on the code bits. After performing error correction and privacy amplification, they share the key.

The role of the MU in Eve is to establish a quantum correlation (i.e., a Bell state) between Alice and Bob to generate the key. If it can establish the strong correlation, then Alice and Bob can generate the key, and if it cannot, then it only results in a high bit error rate to be detected by Alice and Bob and they abort the protocol. As we will see later, since Alice and Bob can judge whether they can generate a key or not by only checking the experimental data as well as information on the fidelity between the density matrices in the X basis and Y basis, it does not matter who performs the measurement nor what kind of measurement is actually done as long as MU broadcasts whether the measurement outcome was successful together with the information of whether the successful outcome is type 0 or type 1.

In the security proof, we assume that MU is totally under the control of Eve. In practice, however, we should choose an appropriate measurement that establishes the strong correlation under the normal operation (i.e., the situation without Eve who induces the channel losses and noises). In the following sections, we will propose two phase encoding MDIQKD schemes.

III. PHASE ENCODING SCHEME I

In this section, we propose an experimental setup for MDIQKD with a phase encoding scheme, which is depicted in Fig. 1. This scheme will be proven to be unconditionally secure (i.e., secure against the most general type of attacks allowed by quantum mechanics). In this setup, we assume that the intensity of Alice's signal (reference) pulse matches with that of Bob's signal (reference) pulse when they enter MU. In order to lock the relative phase, we use strong pulses as the reference pulses. In the PL unit in the figure, the relative phase
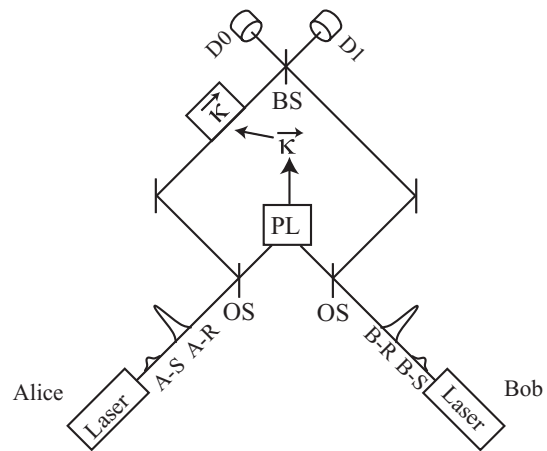

FIG. 1. Schematics of an experimental setup for the phase encoding scheme I. A-S (B-S) and A-R (B-R), respectively, represent Alice's (Bob's) signal and reference pulses. The signal pulses are phase modulated according to Alice's and Bob's choice. OS represents an optical switch, which allows the reference pulse and the signal pulse to be transmitted and to be reflected, respectively. PL represents a unit measuring relative phase of two orthogonal polarization modes and it outputs the two relative phase information $\vec{\kappa}$. Then, the phase shift of $\vec{\kappa}$ for each polarization mode is applied to one of the signal pulses, and they will be detected by D0 and D1 after the interference at the 50:50 beam splitter BS.

between the two strong pulses is measured in two polarization modes separately. The measurement result is denoted by $\vec{\kappa}$ (here, the arrow represents two entries that correspond to the two relative phases). Depending on this information $\vec{\kappa}$, appropriate phase modulations for two polarization modes are applied to the incoming signal pulse from Alice. Then, Alice's and Bob's signal pulses are input into the 50:50 beam splitter which is followed by two single-photon threshold detectors. The successful event of type 0 (type 1) in step (2) is defined as the event where only D0 (D1) clicks. In the case of the type-1 successful detection event, Bob applies bit flip to his sifted key (we define the phase relationship of BS in such a way that D1 never clicks when the phases of the two input signal coherent pulses are the same).

Roughly speaking, our scheme performs double BB84 [16] (i.e., each of Alice and Bob is sending signals in the BB84 states), without phase randomization [14]. Differences between our scheme and the polarization encoding MDIQKD scheme include that Alice and Bob do not need to share the reference frame for the polarization mode, since MU performs the feed-forward control of the polarization, and our scheme intrinsically possesses the basis-dependent flaw.

To see how this particular setup establishes the quantum correlation under the normal operation, it is convenient to consider an entanglement distribution scheme [17], which is mathematically equivalent to the actual protocol. For the simplicity of the discussion, we assume the perfect phase locking for the moment and we only consider the case where both of Alice and Bob use the X basis. We skip the discussion for the Y basis, however, it holds in a similar manner [18]. In this case, the actual protocol is equivalently described as follows. First, Alice prepares two systems in the following state, which is a purification of the X-basis density matrix,

$$|\phi_x^{(+)}(|\sqrt{\alpha_A}\rangle)\rangle \equiv \frac{1}{\sqrt{2}}(|0_x\rangle_{A1}|\sqrt{\alpha_A}\rangle_{A2} + |1_x\rangle_{A1}|-\sqrt{\alpha_A}\rangle_{A2}),$$
(1)

and sends the second system to MU through the quantum channel. Here, $|\sqrt{\alpha_A}\rangle_{A2}$ and $|-\sqrt{\alpha_A}\rangle_{A2}$ represent coherent states that Alice prepares in the actual protocol (α_A represents the mean photon number or intensity), $|0_x\rangle$ and $|1_x\rangle$ are eigenstate of the computational basis (X basis), which is related with the Y-basis eigenstate through $|0_y\rangle \equiv (i|0_x\rangle + |1_x\rangle)/\sqrt{2}$ and $|1_y\rangle \equiv (|0_x\rangle + i|1_x\rangle)/\sqrt{2}$. For the later convenience, we also define Z-basis states as $|0_z\rangle \equiv (|0_x\rangle + |1_x\rangle)/\sqrt{2}$ and $|1_z\rangle \equiv (|0_x\rangle - |1_x\rangle)/\sqrt{2}$. Moreover, the subscript of x in $|\phi_x^{(+)}(|\sqrt{\alpha_A}\rangle)\rangle$ represents that Alice is to measure her qubit along the X basis, the subscript of A in α_A refers to the party who prepares the system, and the superscript $(+)$ represents the relative phase of the superposition. Similarly, Bob also prepares two systems in a similar state $|\phi_x^{(+)}(|\sqrt{\alpha_B}\rangle)\rangle$, sends the second system to MU, and performs the X-basis measurement. Note that the X-basis measurement by Alice and Bob can be delayed after Eve's announcement of the successful event without losing any generalities in the security analysis, and we assume this delay in what follows.

In order to see the joint state of the qubit pair after the announcement, note that the beam splitter converts the joint state $|\phi_x^{(+)}(|\sqrt{\alpha_A}\rangle)\rangle|\phi_x^{(+)}(|\sqrt{\alpha_B}\rangle)\rangle$ into the following

state $|\zeta\rangle_{A1,B1,D0,D1}$.

$$\begin{aligned}|\zeta\rangle_{A1,B1,D0,D1} \equiv \frac{1}{2}(&|0_x\rangle_{A1}|0_x\rangle_{B1}|\sqrt{2\alpha'}\rangle_{D0}|0\rangle_{D1} \\ +&|1_x\rangle_{A1}|1_x\rangle_{B1}|-\sqrt{2\alpha'}\rangle_{D0}|0\rangle_{D1} \\ +&|0_x\rangle_{A1}|1_x\rangle_{B1}|0\rangle_{D0}|\sqrt{2\alpha'}\rangle_{D1} \\ +&|1_x\rangle_{A1}|0_x\rangle_{B1}|0\rangle_{D0}|-\sqrt{2\alpha'}\rangle_{D1}).\end{aligned}$$
(2)

Here, for the simplicity of the discussion, we assume that there are no channel losses, we define $\alpha_A = \alpha_B \equiv \alpha'$, and $|0\rangle$ represents the vacuum state. Moreover, the subscripts D0 and D1 represent the output ports of the beam splitter. If detector D0 (D1) detects photons and the other detector D1 (D0) detects the vacuum state [i.e., the type-0 (type-1) event], it is shown in Appendix A that the joint probability of having the type-0 (type-1) successful event and Alice and Bob share the maximally entangled state $|\Psi^+\rangle$ ($|\Psi^-\rangle$) is $(1 - e^{-4\alpha'})/4$. We note that since $|\sqrt{2\alpha'}\rangle \neq |-\sqrt{2\alpha'}\rangle$, Alice and Bob do not always share this state, and with a joint probability of $(1 - e^{-2\alpha'})^2/4$, they have the type-0 (type-1) successful event and share the maximally entangled state with the phase error (i.e., the bit error in the Y basis) as $|\Phi^+\rangle$ ($|\Phi^-\rangle$).

Note that the bit-flip operation in type-1 successful detection can be equivalently performed by π rotation around the Z basis before Bob performs the X-basis measurement. In other words, π rotation around the Z basis before the X-basis measurement does not change the statistics of the X-basis measurement followed by the bit flip. Thanks to this property, we can conclude that Alice and Bob share $|\Psi^+\rangle$ with the probability of $(1 - e^{-4\alpha'})/2$ and $|\Phi^+\rangle$ with the probability of $(1 - e^{-2\alpha'})^2/2$ after the rotation. This means that even if Alice and Bob are given the successful detection event, they cannot be sure whether they share $|\Phi^+\rangle$ or $|\Psi^+\rangle$, however, if they choose a small enough α, then the phase error rate (the rate of the state $|\Phi^+\rangle$ in the qubit pairs remaining after the successful events or equivalently, the rate of the Y-basis bit error among all the shared qubit pairs) becomes small and they can generate a pure state $|\Psi^+\rangle$ by phase error correction, which is equivalently done by privacy amplification in the actual protocol [3]. We note that the above discussion is valid only for the case without noises and losses, and we will prove the security against the most general attack in Sec. V without relying on the argument given in this section.

We remark that in the phase encoding scheme I, it is important that Alice and Bob know quite well about the four states that they prepare. This may be accomplished by using state tomography with homodyne measurement involving the use of the strong reference pulse [19].

IV. PHASE ENCODING SCHEME II

In this section, we propose the second experimental setup for MDIQKD with a phase encoding scheme. Like scheme I, this scheme will also be proven to be unconditionally secure. In this scheme, the coherent pulses that Alice and Bob send out are exactly the same as those in the standard phase encoding BB84 (i.e., $|e^{i(\zeta+\theta)}\sqrt{\alpha}\rangle_s|e^{i\zeta}\sqrt{\alpha}\rangle_r$), where subscripts s and r, respectively, denote the signal pulse and the reference pulse, ζ is a completely random phase, θ is randomly chosen from $\{0, \pi/2, \pi, 3\pi/2\}$ to encode the information. After entering the
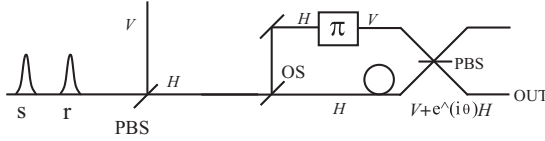
FIG. 2. Schematics of an experimental setup of the converter from phase encoding to polarization encoding. PBS is a polarization beam splitter, and OS represents an optical switch that routes the reference pulse and signal pulses to different paths. The "π" performs the conversion $|H\rangle \rightarrow |V\rangle$. The circle represents time delay. The italic characters along the lines represent the polarization state.

MU, each pulse pair is converted from a phase coding signal to a polarization coding signal by a phase-to-polarization converter (see details below). We note that thanks to the phase randomization by ζ, the joint state of the signal pulse and the reference pulse is a classical mixture of photon number states.

In Fig. 2, we show the schematics of the converter. This converter performs the phase-to-polarization conversion: $\hat{P}_1 |e^{i(\zeta+\theta)} \sqrt{\alpha}\rangle_s |e^{i\zeta} \sqrt{\alpha}\rangle_r$ to $(|V\rangle + e^{i\theta}|H\rangle)/\sqrt{2}$, where $\hat{P}_1$ is a projector that projects the joint system of the signal and reference pulses to a two-dimensional single-photon subspace spanned by $\{|0\rangle_s|1\rangle_r, |1\rangle_s|0\rangle_r\}$ where 0 and 1 represent the photon number, and $|H\rangle$ ($|V\rangle$) represents the horizontal (vertical) polarization state of a single photon. To see how it works, let us follow the time evolution of the input state. At the polarization beam splitter (PBS in Fig. 2), the signal and reference pulses first split into two polarization modes, H and V, and we throw away the pulses being routed to V mode. Then, in H mode, the signal pulse and the reference pulse are routed to different paths by using an optical switch, and we apply π rotation only to one of the paths to convert H to V. At this point, we essentially have $(|V\rangle_{up} + e^{i\theta}|H\rangle_{lw})/\sqrt{2}$, where the subscripts of "up" and "lw," respectively, denote the upper path and the lower path. Finally, these spatial modes up and lw are combined together by using a polarization beam splitter so that we have $(|V\rangle + e^{i\theta}|H\rangle)/\sqrt{2}$ in the output port depicted as "OUT."

In practice, since the birefringence of the quantum channel can be highly time dependent and the polarization state of the input pulses to MU may randomly change with time (i.e., the input polarization state is a completely mixed state), we cannot deterministically distill a pure polarization state, and thus the conversion efficiency can never be perfect. In other words, one may consider the same conversion of the V mode just after the first polarization beam splitter, however, it is impossible to combine the resulting polarization pulses from V mode and the one from H mode into a single mode.

We assume that MU has two converters, one is for the conversion of Alice's pulse and the other one is for Bob's pulse, and the two output ports "OUT" are connected to exactly the same Bell measurement unit [8] in the polarization encoding MDIQKD scheme in Fig. 3 [9]. This Bell measurement unit consists of a 50:50 beam splitter, two polarization beam splitters, and four single-photon detectors, which only distinguishes perfectly two out of the four Bell states of $|\Phi^-\rangle$ and $|\Psi^-\rangle$. The polarization beam splitters discriminate between $|+\rangle \equiv (|H\rangle + |V\rangle)/\sqrt{2}$ and $|-\rangle \equiv (|H\rangle - |V\rangle)/\sqrt{2}$ (note that we choose $+$ and $-$ modes rather than H and V
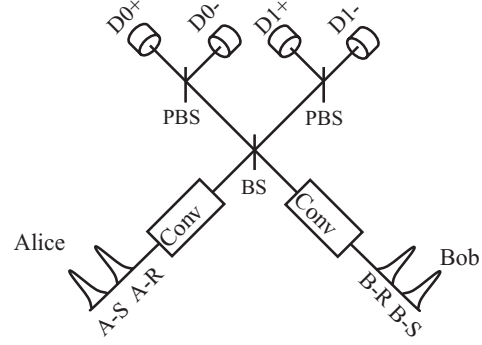

FIG. 3. Schematics of an experimental setup of MU. A-S (B-S) and A-R (B-R), respectively, represent Alice's (Bob's) signal and reference pulses, and MU consists of two converters for each pulse from Alice and Bob (depicted as "Conv"), and the Bell measurement unit consists of a 50:50 beam splitter (BS) followed by two polarization beam splitters (PBSs). See the main text for the explanation.

modes since our computational basis is $+$ and $-$). Suppose that a single photon enters both from Alice and Bob. In this case, the click of D0+ and D0− or D1+ and D1− means the detection of $|\Phi^-\rangle$, and the click of D0+ and D1− or D0− and D1+ means the detection of $|\Psi^-\rangle$ (see Fig. 3). In this scheme, since the use of coherent light induces a nonzero bit error rate in the Y basis $(\{(|H\rangle + i|V\rangle)/\sqrt{2}, (|H\rangle - i|V\rangle)/\sqrt{2}\}$ basis), we consider to generate the key from the $\{|+\rangle, |-\rangle\}$ basis and we use the data in the Y basis only to estimate the bit error rate in this basis conditioned on that both of Alice and Bob emit a single photon, which determines the amount of privacy amplification. By considering a single-photon polarization input both from Alice and Bob, one can see that Bob should not apply the bit flip only when Alice and Bob use the Y basis and Φ^- is detected in MU, and Bob should apply the bit flip in all the other successful events to share the same bit value. Accordingly, the bit error in the X basis is given by the successful detection event conditioned on that Alice and Bob's polarization are identical. As for the Y basis, the bit error is Φ^- detection given the orthogonal polarizations or Ψ^- detection given the identical polarization.

Assuming a completely random input polarization state, our converter successfully converts the single-photon pulse with a probability of 50%. Note in the normal experiment that the birefringence effect between Alice and the converter and the one between Bob and the converter are random and independent, however, it only leads to a fluctuating coincidence rate of Alice's and Bob's signals at the Bell measurement, but does not affect the QBER. Moreover, the fluctuation increases the single-photon loss inserted into the Bell measurement. Especially, the events that the output of the converter for Alice is the vacuum and the one for Bob is a single photon, and vice versa would increase compared to the case where we have no birefringence effect. However, this is not a problem since the Bell measurement does not output the conclusive events in these cases unless the dark counting occurs. Thus, the random and independent polarization fluctuation in the normal experiment is not a problem, and we will simply assume in our simulation in Sec. VI B that this fluctuation can be modeled

just by 50% loss. We emphasize that we do not rely on these assumptions at all when we prove the security, and our security proof applies to any channels and MUs.

For the better performance and also for the simplicity of analysis, we assume the use of an infinite number of decoy states [20] to estimate the fraction of the probability of a successful event conditioned on that both Alice and Bob emit a single photon. One of the differences in our analysis from the work in Ref. [9] is that we will take into account the imperfection of Alice's and Bob's source (i.e., the decay of the fidelity between two density matrices in two bases). We also remark that since the H and V modes are defined locally in MU, Alice and Bob do not need to share the reference frame for the polarization mode, which is one of the qualitative differences from the polarization encoding MIQKD scheme [9].

V. SECURITY PROOF

This section is devoted to the unconditional security proof (i.e., the security proof against the most general attacks) of our schemes. Since both of our schemes are based on BB84 and the basis-dependent flaw in both protocols can be treated in the same manner, we can prove the security in a unified manner.

If the states sent by Alice and Bob were basis independent (i.e., the density matrices of the X basis and Y basis were the same), then the security proof of the original BB84 [1–3] could directly apply (also see [21] for a bit more detailed discussion of this proof), however, they are basis dependent in our case. Fortunately, the security proof of the standard BB84 with a basis-dependent flaw has already been shown to be secure [12–14], and we generalize this idea to our case where we have a basis-dependent flaw from both Alice and Bob. In order to do so, we consider a virtual protocol [12–14,22] that Alice and Bob get together and the basis choices by Alice and Bob are made via measurement processes on the so-called quantum coin. In this virtual protocol of the phase encoding scheme I, Alice and Bob prepare joint systems in the state [23],

$$
\begin{aligned}
|\Psi'\rangle \equiv \tfrac{1}{2}(&|0_z\rangle_E|0_z\rangle_B|0_z\rangle_A|\phi_x^{(+)}(|\sqrt{\alpha_A}\rangle)\rangle|\phi_x^{(+)}(|\sqrt{\alpha_B}\rangle)\rangle \\
&+ |0_z\rangle_E|0_z\rangle_B|1_z\rangle_A|\phi_y^{(+)}(|-i\sqrt{\alpha_A}\rangle)\rangle|\phi_y^{(+)}(|-i\sqrt{\alpha_B}\rangle)\rangle \\
&+ |1_z\rangle_E|1_z\rangle_B|0_z\rangle_A|\phi_x^{(+)}(|\sqrt{\alpha_A}\rangle)\rangle|\phi_y^{(+)}(|-i\sqrt{\alpha_B}\rangle)\rangle \\
&+ |1_z\rangle_E|1_z\rangle_B|1_z\rangle_A|\phi_y^{(+)}(|-i\sqrt{\alpha_A}\rangle)\rangle|\phi_x^{(+)}(|\sqrt{\alpha_B}\rangle)\rangle).
\end{aligned}
$$
(3)

Since just replacing the state, for instance, $|\phi_x^{(+)}(|\sqrt{\alpha_A}\rangle)\rangle \rightarrow |\phi_x^{(+)}(|1\rangle_s|0\rangle_r/\sqrt{2} + |0\rangle_s|1\rangle_r/\sqrt{2})\rangle$, where 1 and 0 in the ket, respectively, represents the single photon and the vacuum, is enough to apply the following proof to the phase encoding scheme II, we discuss only the security of the phase encoding scheme I in what follows. In Eq. (3), the first system denoted by E is given to Eve just after the preparation, and it informs Eve of whether the bases to be used by Alice and Bob match or not. The second system, denoted by B, is a copy of the first system and this system is given to Bob who measures this system with the $\{|0_z\rangle_B, |1_z\rangle_B\}$ basis to know whether Alice's and Bob's bases match or not. If his measurement outcome is $|0_z\rangle_B$ ($|1_z\rangle_B$), then he uses the same (the other) basis to be used by Alice (note that no classical communication is needed in order for Bob to know Alice's basis since Alice and Bob

get together). The third system, which is denoted by A and we call the "quantum coin," is possessed and to be measured by Alice along the $\{|0_z\rangle_A, |1_z\rangle_A\}$ basis to determine her basis choice, and the measurement outcome will be sent to Eve after Eve broadcasts the measurement outcome at MU. Moreover, all the second systems of $|\phi_x^{(+)}(\sqrt{\alpha_A})\rangle$, $|\phi_y^{(+)}(|-i\sqrt{\alpha_A}\rangle)\rangle$, $|\phi_x^{(+)}(|\sqrt{\alpha_B}\rangle)\rangle$, and $|\phi_y^{(+)}(|-i\sqrt{\alpha_B}\rangle)\rangle$ are sent to Eve. Note in this formalism that the information, including classical information and quantum information, available to Eve is the same as those in the actual protocol, and the generated key is also the same as the one of the actual protocol since the statistics of Alice's and Bob's raw data is exactly the same as the one of the actual protocol. Thus, we are allowed to work on this virtual protocol for the security proof.

The first system given to Eve in Eq. (3) allows her to know which coherent pulses contain data in the sifted key and she can postselect only the relevant pulses. Thus, without the loss of any generalities of the security proof, we can concentrate only on the postselected version of the state in Eq. (3) as

$$
\begin{aligned}
|\Psi\rangle \equiv \frac{1}{\sqrt{2}}(&|0_z\rangle_A|\phi_x^{(+)}(|\sqrt{\alpha_A}\rangle)\rangle|\phi_x^{(+)}(|\sqrt{\alpha_B}\rangle)\rangle \\
&+ |1_z\rangle_A|\phi_y^{(+)}(|-i\sqrt{\alpha_A}\rangle)\rangle|\phi_y^{(+)}(|-i\sqrt{\alpha_B}\rangle)\rangle).
\end{aligned}
$$
(4)

The most important quantity in the proof is the phase error rate in the code bits. The definition of the phase error rate is the rate of bit errors along the Y basis in the sifted key if they had chosen the Y basis as the measurement basis when both of them have sent pulses in the X basis. If Alice and Bob have a good estimation of this rate as well as the bit error rate in the sifted key (the bit error rate in the X basis given Alice and Bob have chosen the X basis for the state preparation), they can perform hashing in the Y basis and X basis simultaneously [17,24] to distill pairs of qubits in the state whose fidelity with respect to the product state of the maximally entangled state $|\Psi^+\rangle$ is close to 1.

According to the discussion on the universal composability [26], the key distilled via the X-basis measurement on such a state is composably secure and moreover exactly the same key can be generated only by classical means (i.e., error correction and privacy amplification [3]). Thus, we are left only with the phase error estimation. For the simplicity of the discussion, we assume the large number of successful events n so that we neglect all the statistical fluctuations and we are allowed to work on a probability rather than the relative frequency.

The quantity we have to estimate is the bit error along the Y basis, denoted by δ'_y, given Alice and Bob send the $|\phi_x^{(+)}(|\sqrt{\alpha_A}\rangle)\rangle|\phi_x^{(+)}(|\sqrt{\alpha_B}\rangle)\rangle$ state, which is different from the experimentally available bit error rate along the Y basis given Alice and Bob send the $|\phi_y^{(+)}(|-i\sqrt{\alpha_A}\rangle)\rangle|\phi_y^{(+)}(|-i\sqrt{\alpha_B}\rangle)\rangle$ state. Intuitively, if the basis-dependent flaw is very small, δ'_y and δ_y should be very close since the states are almost indistinguishable. To make this intuition rigorous, we briefly review the idea by [13,14] which applies Bloch sphere bound [27] to the quantum coin. Suppose that we randomly choose the Z basis or X basis as the measurement basis for each quantum coin. Let $n\gamma_z/2$ and $n\gamma_x/2$ be the fraction that those quantum coins result in 1 in the Z-basis and the X-basis measurement, respectively. What Bloch sphere bound [i.e., Eqs. (13) or (14) in Ref. [27] or Eq. (A1) in Ref. [14]] tells us in our case is that

no matter how the correlations among the quantum coins are and no matter what the state for the quantum coins is, thanks to the randomly chosen bases, the following inequality holds with probability exponentially close to 1 in n:

$$(1 - 2\gamma_z)^2 + (1 - 2\gamma_x)^2 \leqslant 1 \,. \tag{5}$$

By applying this bound separately to the quantum coins that are conditional on having phase errors and to those that are conditional on having no phase error, and furthermore by combining those inequalities using Bayes's rule, we have

$$1 - 2\Delta \leqslant \sqrt{\delta_y \delta_y'} + \sqrt{(1-\delta_y)(1-\delta_y')}. \tag{6}$$

Here, Δ is equivalent to the probability that the measurement outcome of the quantum coin along the X basis is $|1_x\rangle$ given the successful event in MU. Note that this probability can be enhanced by Eve who chooses carefully the pulses, and Eve could attribute all the loss events to the quantum coins being in the state $|0_x\rangle$. Thus, we have an upper bound of Δ in the worst-case scenario as

$$\Delta \leqslant \Delta_{\mathrm{ini}}/\gamma_{\mathrm{suc}} \,, \tag{7}$$

and

$$\begin{aligned} \Delta_{\mathrm{ini}} \equiv (1 - \langle \phi_x^{(+)}(|\sqrt{\alpha_A}\rangle)|\phi_y^{(+)}(|-i\sqrt{\alpha_A}\rangle)\rangle \\ \times \langle \phi_x^{(+)}(|\sqrt{\alpha_B}\rangle)|\phi_y^{(+)}(|-i\sqrt{\alpha_B}\rangle)\rangle)/2, \end{aligned} \tag{8}$$

where γ_{suc} is the frequency of the successful event.

Note that we have not used the explicit form of $|\phi_x^{(\pm)}(\beta)\rangle$ and $|\phi_y^{(\pm)}(\beta)\rangle$, where $\beta = \sqrt{\alpha_A}, -i\sqrt{\alpha_A}, \sqrt{\alpha_B}, -i\sqrt{\alpha_B}$, in the derivation of Eqs. (6)–(8), and the important point is that the state $|\phi_x^{(\pm)}(\beta)\rangle$ and $|\phi_y^{(\pm)}(\beta)\rangle$ are the purification of Alice's and Bob's density matrices for both bases. Since there always exists purification states of $\rho^{(X)}$ and $\rho^{(Y)}$, which are, respectively, denoted by $|\Omega^{(X)}\rangle$ and $|\Omega^{(Y)}\rangle$, such that $\langle \Omega^{(X)}|\Omega^{(Y)}\rangle = F(\rho^{(X)}, \rho^{(Y)}) \equiv \mathrm{Tr}(|\sqrt{\rho^{(X)}}\sqrt{\rho^{(Y)}}|)$, Δ_{ini} can be rewritten by

$$\Delta_{\mathrm{ini}} \equiv \left[1 - F\left(\rho_A^{(X)}, \rho_A^{(Y)}\right) F\left(\rho_B^{(X)}, \rho_B^{(Y)}\right)\right]/2, \tag{9}$$

where $\rho_A^{(X)}$ represents Alice's density matrix of the X basis and all the other density matrices are defined by the same manner. Our expression of Δ_{ini} has the product of two fidelities, while the standard BB84 with the basis-dependent flaw in Refs. [12–14] has only one fidelity (the fidelity between Alice's density matrices in the X and Y bases). The two products may lead to poor performance of our schemes compared to that of standard QKD in terms of the achievable distances, however, our schemes have the huge advantage over the standard QKD in that there is no side channel in the detectors.

Finally, the key generation rate G, given the X basis, in the asymptotic limit of large n is given by

$$G = \gamma_{\mathrm{suc}}^{(x)}(1 - f(\delta_x)h(\delta_x) - h(\delta_y')), \tag{10}$$

where δ_x is the bit error rate in the X basis, $f(\delta_x)$ is the inefficiency of the error correcting code, and $h(x) \equiv -x \log_2 x - (1-x) \log_2 (1-x)$. We can trivially obtain the key generation rate for the Y basis just by interchanging the X basis in all the discussions above to the Y basis. We remark in our security proof that we have assumed nothing about what kind of measurement MU conducts but that it announces

whether it detects the successful event and the type of the event (this announcement allows us to calculate $\gamma_{\mathrm{suc}}^{(x)}$ and the error rates). Thus, MU can be assumed to be totally under the control of Eve.

VI. SIMULATION OF THE KEY GENERATION RATES

In the following subsections, we show some examples of the key generation rate of each of our schemes assuming typical experimental parameters taken from the Gobby-Yuan-Shields (GYS) experiment [28] unless otherwise stated. Moreover, we assume that the imperfect phase modulation is the main source of the decay of the fidelity between the density matrices in two bases, and we evaluate the effect of this imperfection on the key generation rate.

A. Phase encoding scheme I

In the phase encoding scheme I, the important quantity for the security Δ_{ini} can be expressed as

$$\Delta_{\mathrm{ini}} = \tfrac{1}{2}[1 - e^{-(\alpha_A + \alpha_B)}(\cos \alpha_A + \sin \alpha_A)(\cos \alpha_B + \sin \alpha_B)]. \tag{11}$$

Note that this quantity is dependent on the intensity of Alice's and Bob's sources. As we have mentioned in Sec. III, this quantity may be estimated relatively easily via tomography involving homodyne measurement.

To simulate the resulting key generation rate, we assume that the bit error stems from the dark counting as well as alignment errors due to imperfect phase locking or imperfect optical components. The alignment error is assumed to be proportional to the probability of having a correct click caused only by the optical detection not by the dark counting. Moreover, we make assumptions that all the detectors have the same characteristics for the simplicity of the analysis, and Alice and Bob choose the intensities of the signal lights in such a way that the intensities of the incoming pulses to MU are the same. Finally, we assume the quantum inefficiency of the detectors to be part of the losses in the quantum channels. With all the assumptions, we may express the resulting experimental parameters as

$$\begin{aligned} \gamma_{\mathrm{suc}}^{(x)} &= [p_{\mathrm{dark}} + (1 - p_{\mathrm{dark}})(1 - e^{-2\alpha_{\mathrm{in}}})](1 - p_{\mathrm{dark}}) \\ &\quad + (1 - p_{\mathrm{dark}})e^{-2\alpha_{\mathrm{in}}}p_{\mathrm{dark}}, \\ \gamma_{\mathrm{suc}} &= \gamma_{\mathrm{suc}}^{(x)} + \gamma_{\mathrm{suc}}^{(y)}, \\ \delta_x &= \delta_y = [e_{\mathrm{ali}}(1 - p_{\mathrm{dark}})^2(1 - e^{-2\alpha_{\mathrm{in}}}) \\ &\quad + (1 - p_{\mathrm{dark}})e^{-2\alpha_{\mathrm{in}}}p_{\mathrm{dark}}]/\gamma_{\mathrm{suc}}^{(x)}, \\ \alpha_{\mathrm{in}} &\equiv \alpha_A \eta_A = \alpha_B \eta_B, \\ \eta_A &= \eta_{\mathrm{det},A} 10^{-\xi_A l_A/10}, \\ \eta_B &= \eta_{\mathrm{det},B} 10^{-\xi_B l_B/10}. \end{aligned} \tag{12}$$

Here, p_{dark} is the dark count rate of the detector, e_{ali} is the alignment error rate, $\eta_A(\eta_B)$ is Alice's (Bob's) overall transmission rate, $\eta_{\mathrm{det},A}$ $(\eta_{\mathrm{det},B})$ is the quantum efficiency of Alice's (Bob's) detector, $\xi_A(\xi_B)$ is Alice's (Bob's) channel transmission rate, and l_A (l_B) is the distance between Alice (Bob) and MU. The first term and the second term in δ_x or δ_y, respectively, represent the alignment error, which is assumed to be proportional to the probability of having correct bit value
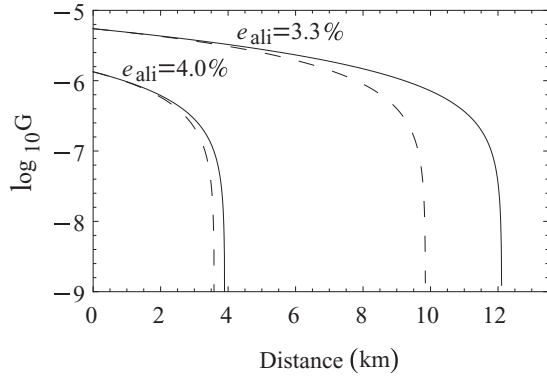
FIG. 4. The key generation rates of each setting as a function of the distance between Alice and Bob with the alignment error rate (e_{ali}) of 3.3% and 4.0%. (Dashed line) (a) MU is at Bob's side (i.e., $l_B = 0$). (Solid line) (b) MU is just in the middle between Alice and Bob. The lines achieving the longer distances correspond to 3.3% of e_{ali}. See also the main text for the explanation.

due to the detection of the light, and errors due to dark counting (one detector clicks due to the dark counting while the other one does not).

We take the following parameters from the GYS experiment [28]: $f(\delta_x) = 1.22$, $p_{\text{dark}} = 8.5 \times 10^{-7}$, $\xi = 0.21$ (dB/km), $\eta_{\text{det},A} = \eta_{\text{det},B} = 0.045$, and $e_{\text{ali}} = 0.033$, and we simulate the key generation rate as a function of the distance between Alice and Bob in Fig. 4. In the figure, we consider two settings: (a) MU is at Bob's side (i.e., $l_B = 0$), and (b) MU is just in the middle between Alice and Bob. The reason why we consider these settings is that the basis-dependent flaw is dependent on intensities that Alice and Bob employ, and it is not trivial where we should place MU for the better performance.

Since the MDIQKD polarization encoding scheme without basis-dependent flaw achieves almost twice the distance of BB84 [9], we may expect that the setting (b) could achieve almost twice the distance of BB84 without phase randomization that achieves about 13 (km) [14] with the same experimental parameters. The simulation result, however, does not follow this intuition since we have the basis-dependent flaw not only from Alice's side but also from Bob's side. Thus, the advantage that we obtain from putting MU between Alice and Bob is overwhelmed by the double basis-dependent flaw. In each setting, we have optimized the intensity of the coherent pulses α_A for each distance (see Fig. 5).

In order to explain why the optimal α_A is so small, note that scheme I intrinsically suffers from the basis-dependent flaw due to Eq. (11). This means that if we use relatively large α_A, then we cannot generate the key due to the flaw. Actually, when we set $\alpha_A = 0.1$, which is a typical order of the amplitude for decoy BB84, one can see that the upper bound of the phase error rate is $1/2$ even in the zero distance (i.e., $l = 0$), and we have no chance to generate the key with this amplitude. Thus, Alice and Bob have to reduce the intensities in order to suppress the basis-dependent flaw. In addition, as the distance gets larger and the losses get increased, Alice and Bob have to use weaker pulses since larger losses can be exploited by Eve to enhance the basis-dependent flaw according to Eq. (7), and they can reduce the intensities until it reaches the cutoff value
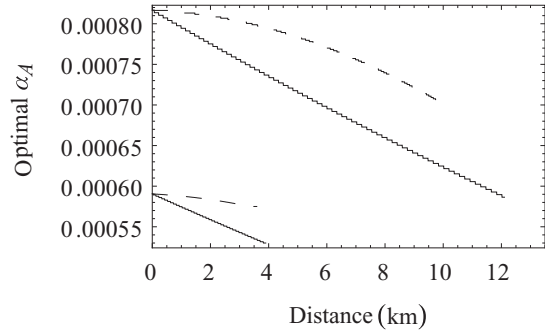

FIG. 5. Optimal mean photon numbers emitted by Alice's source (α_A) that outputs Fig. 4 as a function of the distance between Alice and Bob.

where the detection of the weak pulses is overwhelmed by the dark counts.

In the above simulation, we have assumed that Alice and Bob can prepare states very accurately, however, in reality, they can only prepare approximate states due to the imperfection of the sources. This imperfection gives more basis-dependent flaw, and in order to estimate the effect of this imperfection, we assume that the fidelity between the two actually prepared density matrices in two bases is approximated by the fidelity between the following density matrices (see Appendix B for the detail):

$$\rho_X^{(\text{Act})}(\alpha,\delta) = (|\sqrt{\alpha}\rangle\langle\sqrt{\alpha}| + |-e^{i|\delta|}\sqrt{\alpha}\rangle\langle -e^{i|\delta|}\sqrt{\alpha}|)/2, \quad (13)$$

and

$$\begin{aligned}\rho_Y^{(\text{Act})}(\alpha,\delta) = (&|ie^{i|\delta|/2}\sqrt{\alpha}\rangle\langle ie^{i|\delta|/2}\sqrt{\alpha}| \\ &+ |-ie^{-i|\delta|/2}\sqrt{\alpha}\rangle\langle -ie^{-i|\delta|/2}\sqrt{\alpha}|)/2, \quad (14)\end{aligned}$$

where we assume an imperfect phase modulator whose degree of the phase modulation error is proportional to the target phase modulation value, and δ represents the imperfection of the phase modulation that is related with the extinction ratio η_{ex} as

$$\left|\tan\frac{\delta}{2}\right|^2 = \eta_{\text{ex}}. \quad (15)$$

In this equation, we assume that the nonzero extinction ratio is only due to the imperfection of the phase modulators. Since imperfect phase modulation results in the same effect as the alignment errors (i.e., the pulses are routed to a wrong output port), we assume that the alignment error rate is increased with this imperfection. Thus, in the simulation accommodating the imperfection of the phase modulation, we replace e_{ali} with $e_{\text{ali}} + 16\eta_{\text{ex}}$. Here, we have used a pessimistic assumption that the effect of the phase modulation becomes 16 times higher than before since each of Alice and Bob has one phase modulator and MU has two phase modulators for the phase shift of two polarization modes [note from Eq. (15) that η_{ex} is approximately proportional to δ^2, thus 4 times degradation in terms of the accuracy of the phase modulation results in 16 times degradation in terms of the extinction ratio]. We also remark that in practice, it is more likely that the phase encoding errors are independent, in which case a factor of 4 will suffice and the key rate will actually be higher than what is presented in our paper. On the other hand, we have to use the following
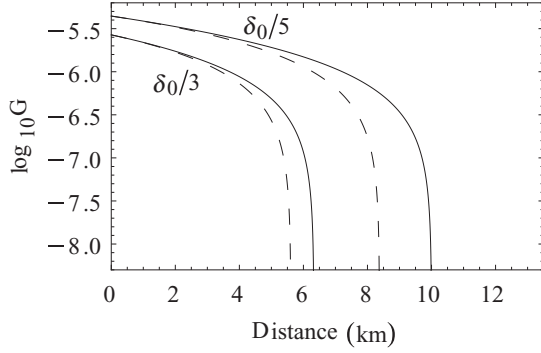
FIG. 6. The key generation rates of each setting as a function of the distance between Alice and Bob with a baseline alignment error rate (e_{ali}) of 3.3% and imperfect phase modulators. $\delta_0 = 0.063$ represents the typical amount of the phase modulation error, and we plot the key rate for smaller imperfection of $\delta_0/3$ and $\delta_0/5$. (Dashed line) MU is at Bob's side (i.e., $l_B = 0$). (Solid line) MU is just in the middle between Alice and Bob.

Δ_{ini} when we consider the security:

$$\Delta_{\text{ini}} = \big[1 - F\big(\rho_X^{(\text{Act})}(\alpha_A, \delta), \rho_Y^{(\text{Act})}(\alpha_A, \delta)\big)$$
$$\times F\big(\rho_X^{(\text{Act})}(\alpha_B, \delta), \rho_Y^{(\text{Act})}(\alpha_B, \delta)\big)\big]/2. \quad (16)$$

In Figs. 6 and 7, we plot the key generation rate and the corresponding optimal Alice's mean photon numbers (α_A) as a function of the distance between Alice and Bob. In the figures, we define $|\delta|$ that satisfies $\eta_{\text{ex}} = |\tan\frac{\delta}{2}|^2 = 10^{-3}$ as $\delta_0 (\sim 0.063)$, where $\eta_{\text{ex}} = 10^{-3}$ is the typical order of η_{ex} in some experiments [29]. We have confirmed that we cannot generate the key when $\eta_{\text{ex}} = 10^{-3}$. However, we can see in the figures that if the accuracy of the phase modulation is increased three times or five times (i.e., $\delta = \delta_0/3$ and $\delta = \delta_0/5$), then we can generate the key. Like the case in Fig. 5, the small optimal mean photon number can be intuitively understood by the arguments that we have already made in this section.

In order to investigate the feasibility of the phase encoding scheme I with the current technologies, we replace $p_{\text{dark}} = 8.5 \times 10^{-7}$, $\eta_{\text{det},A} = \eta_{\text{det},B} = 0.045$, and $e_{\text{ali}} = 0.033$ with $p_{\text{dark}} = 1.0 \times 10^{-7}$, $\eta_{\text{det},A} = \eta_{\text{det},B} = 0.15$ [30], and $e_{\text{ali}} = 0.0075$ [9]. We see in Fig. 8 that the key generation is possible over much longer distances with those parameters assuming
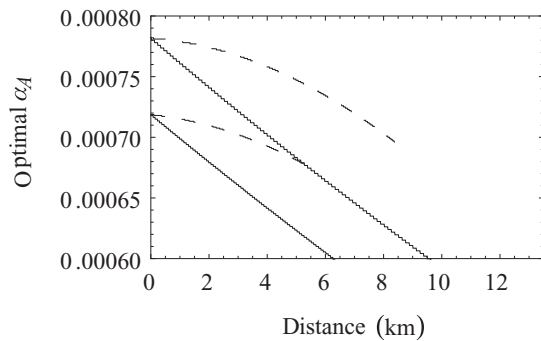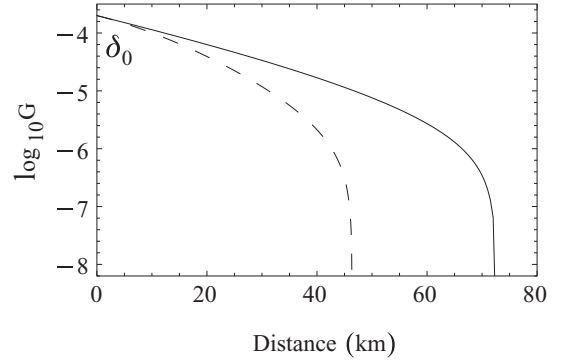

FIG. 8. The key generation rates of each setting as a function of the distance between Alice and Bob with the latest parameters such as $e_{\text{ali}} = 0.0075$ with $p_{\text{dark}} = 1.0 \times 10^{-7}$, $\eta_{\text{det},A} = \eta_{\text{det},B} = 0.15$ [30], and $\delta_0 = 0.063$. (Dashed line) MU is at Bob's side (i.e., $l_B = 0$). (Solid line) MU is just in the middle between Alice and Bob.

the precise control of the intensities of the laser source. We also show the corresponding optimal mean photon number α_A in Fig. 9. We note that thanks to the higher quantum efficiency, the success probability becomes higher, following that Alice and Bob can use larger mean photon number α_A compared to those in Figs. 7 and 9.

B. Phase encoding scheme II

In the phase encoding scheme II, note that we can generate the key only from the successful detection event in MU given both Alice and Bob send out a single-photon since if either or both Alice and Bob emit more than one photon, then Eve can employ the so-called photon number splitting attack [31]. Thus, the important quantities to estimate are $Q_x^{(1,1)}$, $\delta_y^{(1,1)}$, δ_x, Q_x, which, respectively, represent gain in the X basis given both Alice and Bob emit a single photon, the phase error rate given Alice and Bob emit a single photon, overall bit error rate in the X basis, and overall gain in the X basis. To estimate these quantities stemming from the simultaneous single-photon emission, we assume the use of an infinite number of decoy states for the simplicity of analysis [20]. Another important quantity in our study is the fidelity $F_A^{(1)}$ ($F_B^{(1)}$) between Alice's (Bob's) X-basis and Y-basis density matrices of only a single-photon component, *not* whole optical

FIG. 7. Optimal mean photon numbers emitted by Alice's source (α_A) that outputs Fig. 6 as a function of the distance between Alice and Bob.
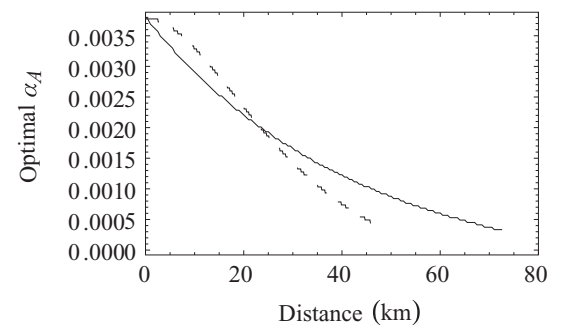

FIG. 9. Optimal mean photon numbers emitted by Alice's source (α_A) that outputs Fig. 8 as a function of the distance between Alice and Bob.

modes. If this fidelity is given, then we have

$$\Delta_{\mathrm{ini}}^{(1,1)} = \tfrac{1}{2}\big(1 - F_A^{(1)} F_B^{(1)}\big). \tag{17}$$

For the simplicity of the discussion, we consider the case of $F_A^{(1)} = F_B^{(1)} \equiv F^{(1)}$ in our simulation. The estimation of the fidelity only in the single-photon part is very important, however, to the best of our knowledge we do not know any experiment directly measuring this quantity. This measurement may require photon number resolving detectors and very accurate interferometers. Thus, we again assume that the degradation of the fidelity is only due to the imperfect phase modulation given by Eq. (15), and we presume that the fidelity of the two density matrices between the two bases is approximated by the fidelity between the following density matrices (see Appendix B for the detail):

$$\rho_X^{(1)} = \frac{1}{2}\left[\hat{P}\left(\frac{|0_z\rangle + |1_z\rangle}{\sqrt{2}} \right) + \hat{P}\left(\frac{|0_z\rangle - e^{i|\delta|}|1_z\rangle}{\sqrt{2}} \right) \right],$$

$$\rho_Y^{(1)} = \frac{1}{2}\left[\hat{P}\left(\frac{|0_z\rangle + i e^{i|\delta|/2}|1_z\rangle}{\sqrt{2}} \right) \right.$$
$$\left. + \hat{P}\left(\frac{|0_z\rangle - i e^{-i|\delta|/2}|1_z\rangle}{\sqrt{2}} \right) \right]. \tag{18}$$

With these parameters, we can express the key generation rate given Alice and Bob use the X basis as [12]

$$G = Q_x^{(1,1)}\big[1 - h\big(\delta_y^{(1,1)'}\big)\big] - f(\delta_x)Q_x h(\delta_x), \tag{19}$$

where $\delta_y^{(1,1)'}$ is the (1,1) version of δ_y' in Eq. (10).

To simulate the resulting key generation rate, the bit errors are assumed to stem from a multiphoton component, the dark counting, and the misalignment that is assumed to be proportional to the probability of obtaining the correct bit values only due to the detection by optical pulses. Like before, we also assume that all the detectors have the same characteristics, Alice and Bob choose the intensities of the signal lights in such a way that the intensities of the incoming pulses to MU are the same, and all the quantum inefficiencies of the detectors can be attributed to part of the losses in the quantum channel. Finally, Alice's and Bob's coherent light sources are assumed to be phase randomized, and the imperfect phase modulation is represented by the increase of the alignment error rate. With these assumptions, we may have the following resulting experimental parameters:

$$Q_x^{(1,1)} = 4\alpha_A \alpha_B \eta_A \eta_B e^{-2(\alpha_A+\alpha_B)}$$
$$\times \left[\frac{(1 - p_{\mathrm{dark}})^2}{2} + \frac{p_{\mathrm{dark}}(1 - p_{\mathrm{dark}})^2}{2} \right]$$
$$+ W^{(2,1)} + W^{(2,0)},$$
$$\delta_x^{(1,1)} = \{4\alpha_A\alpha_B\eta_A\eta_B e^{-2(\alpha_A+\alpha_B)} p_{\mathrm{dark}}(1-p_{\mathrm{dark}})^2/2$$
$$+ 2(e_{\mathrm{ali}} + 4\eta_{\mathrm{ex}})\alpha_A\alpha_B\eta_A\eta_B e^{-2(\alpha_A+\alpha_B)}(1-p_{\mathrm{dark}})^2$$
$$+ (W^{(2,1)} + W^{(2,0)})/2\}/Q_x^{(1,1)},$$
$$Q_y^{(1,1)} = Q_x^{(1,1)},$$
$$\delta_y^{(1,1)} = \delta_x^{(1,1)},$$
$$W^{(2,1)} \equiv 8\alpha_A\alpha_B e^{-2(\alpha_A+\alpha_B)}[\eta_A(1-\eta_B) + (1-\eta_A)\eta_B]$$
$$\times p_{\mathrm{dark}}(1-p_{\mathrm{dark}})^2,$$

$$W^{(2,0)} \equiv 16\alpha_A\alpha_B(1-\eta_A)(1-\eta_B)e^{-2(\alpha_A+\alpha_B)}$$
$$\times p_{\mathrm{dark}}^2(1-p_{\mathrm{dark}})^2,$$
$$Q_x = 2[1 - (1-p_{\mathrm{dark}})e^{-\alpha_{\mathrm{in}}}]^2(1-p_{\mathrm{dark}})^2 e^{-2\alpha_{\mathrm{in}}} + V,$$
$$\delta_x = V + (e_{\mathrm{ali}} + 4\eta_{\mathrm{ex}})2(1 - e^{-\alpha_{\mathrm{in}}})^2(1-p_{\mathrm{dark}})^2 e^{-2\alpha_{\mathrm{in}}},$$
$$V \equiv \frac{p_{\mathrm{dark}}(1-p_{\mathrm{dark}})}{2\pi}\int_0^{2\pi} d\theta\big[1 - (1-p_{\mathrm{dark}})e^{-\alpha_{\mathrm{in}}|1+e^{i\theta}|^2}\big]$$
$$\times \big[(1-p_{\mathrm{dark}})e^{-\alpha_{\mathrm{in}}|1-e^{i\theta}|^2}\big] + \frac{p_{\mathrm{dark}}(1-p_{\mathrm{dark}})}{2\pi}$$
$$\times \int_0^{2\pi} d\theta\big[1 - (1-p_{\mathrm{dark}})e^{-\alpha_{\mathrm{in}}|1-e^{i\theta}|^2}\big]$$
$$\times \big[(1-p_{\mathrm{dark}})e^{-\alpha_{\mathrm{in}}|1+e^{i\theta}|^2}\big],$$
$$\alpha_{\mathrm{in}} \equiv \alpha_A\eta_A = \alpha_B\eta_B,$$
$$\eta_A = \eta_{\mathrm{det},A}10^{-\xi_A l_A/10}/2,$$
$$\eta_B = \eta_{\mathrm{det},B}10^{-\xi_B l_B/10}/2. \tag{20}$$

Note that α_A (α_B) represents each of the intensity of Alice's (Bob's) signal light and the reference light, *not* the total intensity of them, and η_A and η_B are divided by 2 since the conversion efficiency of our converter is 50%. 4 in $4\eta_{\mathrm{ex}}$ again comes from the pessimistic assumption that each of Alice's and Bob's phase modulator is imperfect, and $W^{(2,1)}$ ($W^{(2,0)}$) represents the probability of the event where both Alice and Bob emit a single photon and only one (zero) photon is detected but the successful detection event is obtained due to the dark counting. On the other hand, the quantity that quantifies the basis-dependent flaw Δ in the present case is upper bounded by

$$\Delta \leqslant \Delta_{\mathrm{ini}}^{(1,1)}\big/[Q^{(1,1)}/(4\alpha_A\alpha_B e^{-2(\alpha_A+\alpha_B)})],$$
$$Q^{(1,1)} \equiv \big(Q_x^{(1,1)} + Q_y^{(1,1)}\big)/2, \tag{21}$$

where $Q^{(1,1)}/4\alpha_A\alpha_B e^{-2(\alpha_A+\alpha_B)}$ is the probability that MU receives a single photon both from Alice and Bob simultaneously conditioned on that each of Alice and Bob sends out a single photon. We remark that Δ_{ini} in this scheme is only dependent on the accuracy of the phase modulation. This is different from scheme I where the manipulation of the intensities of the pulses can affect the basis-dependent flaw.

In the simulation, we again assume GYS experimental parameters and we consider two settings: (a) MU is at Bob's side and (b) MU is just in the middle between Alice and Bob. Note that Δ_{ini} is independent of α_A and α_B in the phase encoding scheme II case.

In Fig. 10, we plot the key generation rates of (a) and (b) for $\delta = 0$, $\delta = \delta_0/50$, $\delta = \delta_0/20$, $\delta = \delta_0/10$ [recall from Eq. (15) that $\delta_0 \sim 0.0063224$ that corresponds to the typical extinction ratio of 0.1%], which, respectively, correspond to $F^{(1)} = 1.0$, $F^{(1)} \sim 1-1.0 \times 10^{-7}$, $F^{(1)} \sim 1-6.6 \times 10^{-7}$, and $F^{(1)} \sim 1-2.5 \times 10^{-6}$, and the achievable distances of (a) and (b) increase with the improvement of the accuracy (i.e., with the decrease of δ). We have confirmed that no key can be distilled in (a) and (b) when $\delta \geqslant \delta_0/7$. The figure shows that the achievable distance drops significantly with the degradation of the accuracy of the phase modulator, and the main reason of this fast decay is that Δ is approximated by $\Delta_{\mathrm{ini}}/O(\eta_A\eta_B)$ and this dominator decreases exponentially with the increase of the distance.
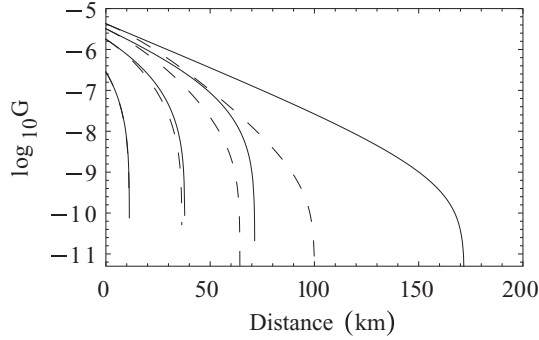
FIG. 10. The key generation rates of each setting as a function of the distance. (Dashed line) (a) MU is at Bob's side (i.e., $l_B = 0$). (Solid line) (b) MU is just in the middle between Alice and Bob. We plot the key generation rates of each case when $\delta = 0$, $\delta = \delta_0/50$, $\delta = \delta_0/20$, $\delta = \delta_0/10$ where δ is proportional to the amount of the phase modulation error, and for each case of (a) and (b) the key generation rates monotonously increase with the decrease of δ (i.e., with the improvement of the phase modulation). The key rates of (a) and (b) when $\delta_0/10$ are almost superposed. See also the main text for the explanation.

We also plot the corresponding optimal α_A in Fig. 11. Notice that the mean photon number increases in some regime in some cases of (a), and recall that this increase does not change Δ_{ini}. If we increased the intensity in scheme I with the distance, then we would have more basis-dependent flaw, resulting in shortening of the achievable distance. This may be an intuitive reason why we see no such increase in Figs. 5, 7, and 9.

Like in the phase encoding scheme I, we investigate the feasibility of the phase encoding scheme II with the current technologies by replacing $p_{\text{dark}} = 8.5 \times 10^{-7}$, $\eta_{\text{det},A} = \eta_{\text{det},B} = 0.045$, and $e_{\text{ali}} = 0.033$ with $p_{\text{dark}} = 1.0 \times 10^{-7}$, $\eta_{\text{det},A} = \eta_{\text{det},B} = 0.15$ [30], and $e_{\text{ali}} = 0.0075$ [9]. With this upgrade, we have confirmed the impossibility of the key generation, however, if we double the quantum efficiency of the detector or equivalently, if we assume the polarization encoding so that the factor of 1/2, which is introduced by the phase-to-polarization converter, is removed both from η_A and η_B in Eq. (20), then we can generate the key, which is shown in Fig. 12 (also see Fig. 13).

Finally, we note that our simulation is essentially the same as the polarization coding since the fact that we use phase
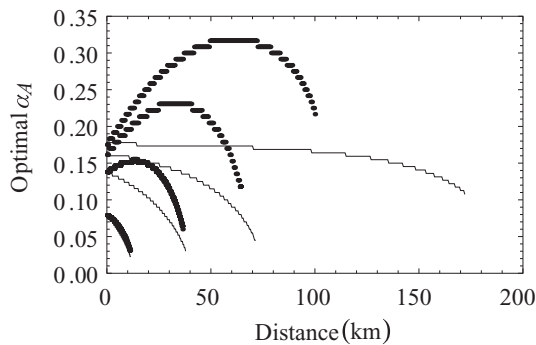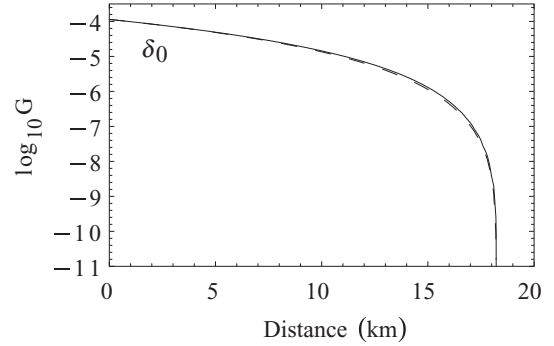

FIG. 12. The key generation rates of each setting as a function of the distance with $p_{\text{dark}} = 1.0 \times 10^{-7}$, $\eta_{\text{det},A} = \eta_{\text{det},B} = 0.30$, and $\delta_0 = 0.063$. Note that we double $\eta_{\text{det},A} = \eta_{\text{det},B}$ compared to the one of [30], or we effectively consider the polarization encoding [9]. (Dashed line) (a) MU is at Bob's side (i.e., $l_B = 0$). (Solid line) (b) MU is just in the middle between Alice and Bob. The key rates are almost superposed. See also the main text for the explanation.

encoding is only reflected by the dominator of 2 in η_A and η_B in Eq. (20). Thus, the behavior of the key generation rate against the degradation of the state preparation is the same also in polarization-based MDIQKD. Also note that even in the standard BB84, Δ decays exponentially with increasing distance. Thus, we conclude that very precise state preparation is very crucial in the security of not only MDIQKD but also in standard QKD. We also note that our estimation of the fidelity might be too pessimistic since we have assumed that the degradation of the extinction ratio is only due to imperfect phase modulation. In reality, the imperfection of Mach-Zehnder interferometer and other imperfections should contribute to the degradation, and the fidelity should be closer to 1 than the one based on our model.

VII. SUMMARY AND DISCUSSION

In summary, we have proposed two phase encoding MDIQKD schemes. The first scheme is based on the phase locking technique and the other one is based on the conversion of the pulses in the standard phase encoding BB84 to polarization modes. We proved the security of the first scheme, which intrinsically possesses a basis-dependent flaw, as well as
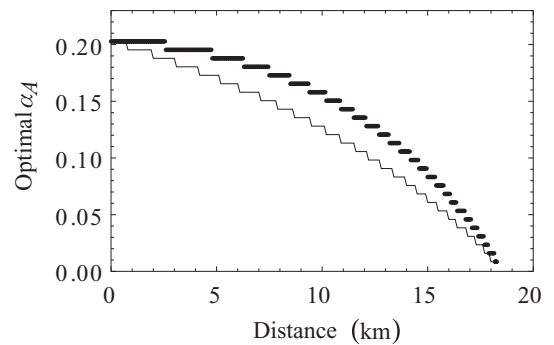

FIG. 11. The optimal mean photon number emitted by Alice (α_A) that outputs Fig. 10. The bold lines correspond to (a). See also the main text for the explanation.

FIG. 13. The optimal mean photon number emitted by Alice (α_A) that outputs Fig. 12. The bold lines correspond to (a). See also the main text for the explanation.

the second scheme with the assumption of the basis-dependent flaw in the single-photon part of the pulses. Based on the security proof, we also evaluate the effect of imperfect state preparation, and especially we focus our attention to the imperfect phase modulation.

While the first scheme can cover relatively short distances of the key generation, this scheme has an advantage that the basis-dependent flaw can be controlled by the intensities of the pulses. Thanks to this property, we have confirmed based on a simple model that 3 or 5 times the improvement in the accuracy of the phase modulation is enough to generate the key. Moreover, we have confirmed that the key generation is possible even without these improvements if we implement this scheme by using the up-to-date technologies and the control of intensities of the laser source is precise. On the other hand, it is not so clear to us how accurate we can lock the phase of two spatially separated laser sources, which is important for the performance of scheme I. Our result still implies that scheme I can tolerate up to some extent the imperfect phase locking errors, which should be basically the same as the misalignment errors, but further analysis of the accuracy from the experimental viewpoint is necessary. We leave this problem for future studies.

The second scheme can cover much longer distances when the fidelity of the *single-photon components* of the Y-basis and X-basis density matrices is perfect or extremely close to perfect. When we consider the slight degradations of the fidelity, however, we find that the achievable distances drop significantly. This suggests that we need a photon source with a very high fidelity, and very accurate estimation of the fidelity of the single-photon subspace is also indispensable.

In our estimation of the imperfection of the phase modulation, we simply assume that the degradation of the extinction ratio is only due to imperfect phase modulation, which might be too pessimistic, and the imperfection of the Mach-Zehnder interferometer and other imperfections contribute to the degradation. Thus, the actual fidelity between the density matrices of the single-photon part in two bases might be very close to 1, which should be experimentally confirmed for the secure communication. We note that the use of the passive device to prepare the state [32] may be a promising way for the very accurate state preparation.
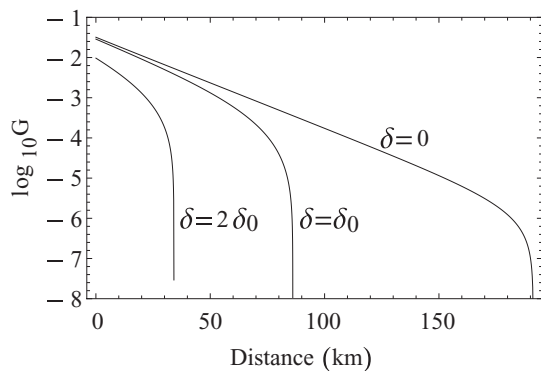

FIG. 15. The optimal mean photon number emitted by Alice (α_A) that outputs Fig. 14.

We remark that the accurate preparation of the state is very important not only in MDIQKD but also in standard QKD where Eve can enhance the imbalance of the quantum coin exponentially with the increase of the distance. To see this point, we, respectively, plot in Figs. 14 and 15 the key generation rate of standard BB84 with infinite decoy states in the X basis and its optimal mean photon number assuming $p_{\text{dark}} = 1.0 \times 10^{-7}$, $\eta_{\text{det},A} = 0.15$ [30], $e_{\text{ali}} = 0.0075$, $f(\delta_x) = 1.22$, and $\xi = 0.21$. Again, $\delta_0 \sim 0.063$ is the typical value of the phase modulation error, and we see in the figure that the degradation of the phase modulator in terms of the accuracy significantly decreases the achievable distance of secure key generation. One notices that standard decoy BB84 is more robust against the degradation since the probability that the measurement outcome of the quantum coin along the X basis is $|1_x\rangle$ given the successful detection of the signal by Bob is written as $\Delta_{\text{ini}} = \frac{1}{2}(1 - F_A^{(1)})$ rather than $\Delta_{\text{ini}} = \frac{1}{2}(1 - F_A^{(1)} F_B^{(1)})$. On the other hand, one has to remember that we trust the operation of Bob's detectors in this simulation, which may not hold in practice.

Finally, we neglect the effect of the fluctuation of the intensity and the center frequency of the laser light in our study, which we will analyze in future works. In summary, our work highlights the importance of very accurate preparation of the states to avoid basis-dependent flaws.

FIG. 14. The key generation rates of the standard BB84 with infinite decoy states from the X basis when $\delta = 0$, $\delta = \delta_0$, $\delta = 2\delta_0$ where δ is the amount of the phase modulation error.
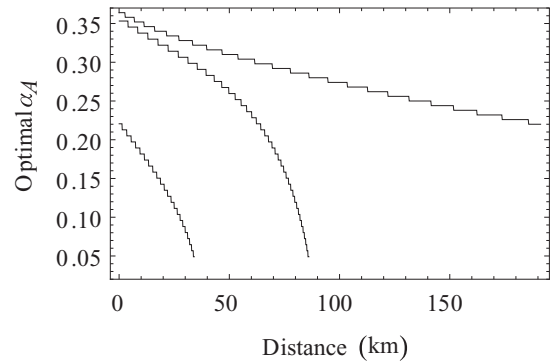
APPENDIX A: SCHEME I WITHOUT NOISES AND LOSSES

In this Appendix, we give a detailed calculation about how scheme I works when there are no channel losses and noises. In order to calculate the joint probability that Alice and Bob obtain the type-0 successful event, where only the detector D0 clicks, and they share the maximally entangled state $|\Psi^+\rangle$, we introduce a projector $\hat{\Pi}_{D_0} \equiv \hat{P}(|\bar{0}\rangle_{D_0})\hat{P}(|0\rangle_{D_1})$ that corresponds to the type-0 successful event. Here, $\bar{0}$ represents the nonvacuum state. The state after Alice and Bob have the type-0 successful event $\hat{\Pi}_{D_0}|\zeta\rangle_{A1,B1,D0,D1}$ [see Eq. (2) for the definition of $|\zeta\rangle_{A1,B1,D0,D1}$] can be expressed by

$$\hat{\mathbb{1}}_{A1,B1}\hat{\Pi}_{D_0}|\zeta\rangle_{A1,B1,D0,D1} = \frac{a}{\sqrt{2}}|\Phi^+\rangle_{A1,B1}|\phi_0\rangle_{D0}|0\rangle_{D1}$$
$$+ \frac{b}{\sqrt{2}}|\Psi^+\rangle_{A1,B1}|\phi_1\rangle_{D0}|0\rangle_{D1}.$$
(A1)

Here, $\hat{\mathbb{1}}_{A1,B1}$ is an identity operator on $A1$ and $B1$, a and b are complex numbers, and $|\phi_0\rangle$ and $|\phi_1\rangle$ are orthonormal bases, which are related with each other through

$$\hat{P}(|\bar{0}\rangle)|\sqrt{2\alpha'}\rangle \equiv a|\phi_0\rangle + b|\phi_1\rangle,$$
$$\hat{P}(|\bar{0}\rangle)|-\sqrt{2\alpha'}\rangle \equiv a|\phi_0\rangle - b|\phi_1\rangle.$$
(A2)

By a direct calculation, one can show that

$$|a|^2 = \frac{(1 - e^{-2\alpha'})^2}{2},$$
$$|b|^2 = \frac{(1 - e^{-4\alpha'})}{2}.$$
(A3)

Finally, by taking the partial trace over the system D0 and D1 in Eq. (A1), we can see that Alice and Bob share either $|\Phi^+\rangle$ or $|\Psi^+\rangle$ probabilistically, and the joint probability that they obtain the type-0 successful event and share the maximally entangled state $|\Psi^+\rangle$ is given by $|b|^2/2$. In the same manner, we can readily calculate the other joint probabilities.

APPENDIX B: IMPERFECTION OF THE PHASE MODULATOR

In this Appendix, we give an estimation of the fidelity between the density matrices in the X and Y bases by using the extinction ratio. In this estimation, we assume that the source of the imperfections is only due to the imperfect phase modulation and the stability of the intensity control of the coherent light source is negligible.

Imagine that we generate two pulses, one of which is the reference light and the other one of which is the signal light, and these pulses are spatially separated. Then, we input these pulses into a Mach-Zehnder interferometer, which is composed of two 50:50 beam splitters, and the output from one of the two output ports gives us the desired state and the other output port gives a wrong state. Let T and t be transmission rates of the pulses to the correct port and the wrong port, which

satisfies

$$T + t = 1, \quad \eta_{ex} \equiv \frac{t}{T},$$
(B1)

where η_{ex} is the extinction ratio. In typical experiments, η_{ex} is in the order of 10^{-3} [29]. We assume that the Mach-Zehnder interferometer is perfect and the imperfection of the extinction ratio is only due to imperfect phase modulations.

Now, suppose that we plug $|\sqrt{\alpha}\rangle$ and $|e^{i(\pi+\delta)}\sqrt{\alpha}\rangle$ into the perfect Mach-Zehnder interferometer, where δ represents the imperfect phase modulation when we want to apply the phase shift of π. Since the Mach-Zehnder interferometer is composed of 50:50 beam splitters, η_{ex} can be represented by $|\tan\frac{\delta}{2}|^2$, and thus we can obtain the imperfection of δ by solving the following equation:

$$\left|\tan\frac{\delta}{2}\right|^2 = \eta_{ex}.$$
(B2)

For instance, when $\eta_{ex} = 10^{-3}$, we have $|\delta| \sim 0.063 \equiv \delta_0$ that is equivalent to about $3.62°$. We rely on this equation to estimate the accuracy of the phase modulator, and we assume that the actual phase modulation is $\theta + |\delta|\theta/\pi$ (i.e., the degree of the imperfect phase modulation is proportional to the desired phase modulation). We remark that $3.62°$ seems rather large to us, and we believe that this can be substantially improved through careful calibration and/or engineering of the preparation process.

In the case of scheme I, the ideal density matrix for the X basis $\rho_X^{(Ideal)}$ is $(|\alpha\rangle\langle\alpha| + |-\alpha\rangle\langle-\alpha|)/2$ and the one for the Y basis $\rho_Y^{(Ideal)}$ is $(|i\alpha\rangle\langle i\alpha| + |-i\alpha\rangle\langle-i\alpha|)/2$. Based on our imperfect phase modulation model, we have the density matrix for the actually generated states in the X basis as

$$\rho_X^{(Act)}(\alpha,\delta) = (|\sqrt{\alpha}\rangle\langle\sqrt{\alpha}| + |-e^{i\delta}\sqrt{\alpha}\rangle\langle-e^{i\delta}\sqrt{\alpha}|)/2,$$
(B3)

and the one for the Y basis as

$$\rho_Y^{(Act)}(\alpha,\delta) = (|ie^{i|\delta|/2}\sqrt{\alpha}\rangle\langle ie^{i|\delta|/2}\sqrt{\alpha}|$$
$$+ |-ie^{-i|\delta|/2}\sqrt{\alpha}\rangle\langle-ie^{-i|\delta|/2}\sqrt{\alpha}|)/2.$$
(B4)

Here, note that when we want to prepare $|\sqrt{\alpha}\rangle$, we do not apply any phase modulation.

In the case of scheme II, the ideal single-photon density matrix for the X basis $\rho_X^{(Ideal,1)}$ is $(|0_x\rangle\langle 0_x| + |1_x\rangle\langle 1_x|)/2$ and the one for the Y basis $\rho_Y^{(Ideal,1)}$ is $(|0_y\rangle\langle 0_y| + |1_y\rangle\langle 1_y|)/2$. With the assumption on the accuracy of the phase modulator, we have the density matrix for the actually generated states in the X basis as

$$\rho_X^{(Act,1)} = (\hat{P}[(|0_z\rangle + |1_z\rangle)/\sqrt{2}]$$
$$+ \hat{P}[(|0_z\rangle - e^{i|\delta|}|1_z\rangle)/\sqrt{2}])/2,$$
(B5)

and the one for the Y basis as

$$\rho_Y^{(Act,1)} = (\hat{P}[(|0_z\rangle + ie^{i|\delta|/2}|1_z\rangle)/\sqrt{2}]$$
$$+ \hat{P}[(|0_z\rangle - ie^{-i|\delta|/2}|1_z\rangle)/\sqrt{2}])/2.$$
(B6)

[1] D. Mayers, J. ACM **48**, 351 (2001).

[2] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).

[3] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[4] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quantum Inf. Comput. **7**, 73 (2007); Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A **78**, 042333 (2008); C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, *ibid.* **75**, 032314 (2007); F. Xu, B. Qi, and H.-K. Lo, New J. Phys. **12**, 113026 (2010).

[5] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nature Photonics **4**, 686 (2010); Z. L. Yuan, J. F. Dynes, and A. J. Shields, *ibid.* **4**, 800 (2010); L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, *ibid.* **4**, 801 (2010); I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Nature Comm. **2**, 349 (2011); L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov, New J. Phys. **13**, 113042 (2011).

[6] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, Quantum Inf. Comput. **9**, 131 (2009); L. Lydersen and J. Skaar, *ibid.* **10**, 0060 (2010); Ø. Marøy, L. Lydersen, and J. Skaar, Phys. Rev. A **82**, 032337 (2010).

[7] D. Mayers and A. C.-C. Yao, in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS98)* (IEEE, Washington, DC, 1998), p. 503; A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).

[8] J. Bell, Physics **1**, 195 (1964).

[9] H.-K. Lo, M. Curty, and B. Qi, e-print arXiv:1109.1473 (to be published in Phys. Rev. Lett).

[10] H. Inamori, Algorithmica **34**, 340 (2002).

[11] E. W. Kolb and M. S. Turner, Phys. Rev. Lett. **67**, 661 (1991).

[12] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **5**, 325 (2004).

[13] M. Koashi, New J. Phys. **11**, 045018 (2009); e-print arXiv:cond-mat/0505108 (to be published).

[14] H.-K. Lo and J. Preskill, Quantum Inf. Comput. **8**, 431 (2007).

[15] The definition of the four Bell state is as follows: $|\Psi^+\rangle \equiv \frac{1}{\sqrt{2}}[|0_z\rangle_{A1}|1_z\rangle_{B1} + |1_z\rangle_{A1}|0_z\rangle_{B1}] = \frac{1}{\sqrt{2}}[|0_x\rangle_{A1}|0_x\rangle_{B1} - |1_x\rangle_{A1}|1_x\rangle_{B1}]$, $|\Phi^-\rangle \equiv \frac{1}{\sqrt{2}}[|0_z\rangle_{A1}|0_z\rangle_{B1} - |1_z\rangle_{A1}|1_z\rangle_{B1}] = \frac{1}{\sqrt{2}}[|0_x\rangle_{A1}|1_x\rangle_{B1} + |1_x\rangle_{A1}|0_x\rangle_{B1}]$, $|\Phi^+\rangle \equiv \frac{1}{\sqrt{2}}[|0_z\rangle_{A1}|0_z\rangle_{B1} + |1_z\rangle_{A1}|1_z\rangle_{B1}] = \frac{1}{\sqrt{2}}[|0_x\rangle_{A1}|0_x\rangle_{B1} + |1_x\rangle_{A1}|1_x\rangle_{B1}]$, and $|\Psi^-\rangle \equiv \frac{1}{\sqrt{2}}(|0_z\rangle_{A1}|1_z\rangle_{B1} - |1_z\rangle_{A1}|0_z\rangle_{B1}) = \frac{1}{\sqrt{2}}(|0_x\rangle_{A1}|1_x\rangle_{B1} - |1_x\rangle_{A1}|0_x\rangle_{B1})$.

[16] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE Press, New York, 1984), pp. 175–179.

[17] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

[18] In the case of the Y basis, we replace the following discussion with the one starting with $|\phi_y^{(+)}(|-i\sqrt{\alpha_A}\rangle)\rangle|\phi_y^{(+)}(|-i\sqrt{\alpha_B}\rangle)\rangle$ instead of $|\phi_x^{(+)}(|\sqrt{\alpha_A}\rangle)\rangle|\phi_x^{(+)}(|\sqrt{\alpha_B}\rangle)\rangle$. See Eq. (1) for the definition of the state.

[19] S. L. Braunstein, Phys. Rev. A **42**, 474 (1990); W. Vogel and J. Grabow, *ibid.* **47**, 4227 (1993); D. T. Smithey, M. Beck, M. G. Raymer, and A. Faridani, Phys. Rev. Lett. **70**, 1244 (1993).

[20] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003); H.-K. Lo, X. Ma, and K. Chen, *ibid.* **94**, 230504 (2005); X.-B. Wang, *ibid.* **94**, 230503 (2005).

[21] One of the simplest proofs is Shor-Preskill's proof [3]. The intuition of this proof is as follows. Note that if Alice and Bob share some pairs of $|\Psi^+\rangle$ (i.e., Alice has one half of each pair and Bob has the other half), then they can generate a secure key by performing the X-basis measurement. The reason for the security is that this state is a pure state, which means that this state has no correlations with the third system including Eve's system. Due to the intervention by Eve, Alice and Bob do not share this pure state in general, but instead they share noisy pairs. The basic idea of the proof is to consider the distillation of $|\Psi^+\rangle$ from the noisy pairs. For the distillation, note that $|\Psi^+\rangle$ is only a one-qubit pair state that has no bit errors in the X basis (we call this error the bit error) and has no bit errors in the Y basis (we call this error the phase error). It is known that if Alice and Bob employ the so-called Calderbank-Shor-Steane (CSS) code [25], then the noisy pairs are projected to a classical mixture of the four Bell states (i.e., $|\Psi^+\rangle$, $|\Phi^+\rangle$ ($|\Psi^+\rangle$ with the phase error, $|\Psi^-\rangle$ ($|\Psi^+\rangle$) with the bit error, and $|\Phi^-\rangle$ ($|\Psi^+\rangle$) with both the phase and bit errors). Moreover, if Alice and Bob choose a correct CSS code, which can be achieved by a random sampling procedure, then the CSS code can detect the position of the erroneous pair with high probability. Thus, by performing a bit and phase flip operation depending on the detected error positions, Alice and Bob can distill some qubit pairs that are very close in fidelity to the product state of $|\Psi^+\rangle$. In general, implementation of the above scheme requires a quantum computer. Fortunately, Shor-Preskill showed that the bit error detection and bit flip operation can be done classically, and the phase error detection and phase flip operation need not be done, but exactly the same key can be obtained by the privacy amplification, so that we do not need to possess a quantum computer for the key distillation.

[22] S. L. Braunstein and S. Pirandola, e-print arXiv:1109.2330 (to be published).

[23] We have chosen $|\phi_y^{(+)}(|-i\sqrt{\alpha_A}\rangle)\rangle|\phi_y^{(+)}(|-i\sqrt{\alpha_B}\rangle)\rangle$ rather than $|\phi_y^{(+)}(i\sqrt{\alpha_A}\rangle)\rangle|\phi_y^{(+)}(i\sqrt{\alpha_B}\rangle)\rangle$ to maximize the inner product with $|\phi_x^{(+)}(|\sqrt{\alpha_A}\rangle)\rangle|\phi_x^{(+)}(|\sqrt{\alpha_B}\rangle)\rangle$. This large inner product is important for the security proof.

[24] K. Tamaki and G. Kato, Phys. Rev. A **81**, 022316 (2010).

[25] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996); A. M. Steane, Proc. R. Soc. London A **452**, 2551 (1996).

[26] R. Renner and R. Koenig, *Proceedings of TCC 2005, LNCS*, Vol. 3378 (Springer, New York, 2005); M. Ben-Or and Dominic Mayers, e-print arXiv:cond-mat/0409062 (to be published); M. Ben-Or, Michal Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, in *Theory of Cryptography: Second Theory of Cryptography Conference, TCC 2005*, Vol. 3378 of Lecture Notes in Computer Science, edited by J. Kilian (Springer Verlag, New York, 2005), pp. 386–406.

[27] K. Tamaki, M. Koashi, and N. Imoto, Phys. Rev. Lett. **90**, 167904 (2003).

[28] C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004).

[29] T. Honjo, K. Inoue, and H. Takahashi, Opt. Lett. **29**, 23 (2004); G. Li, Advances in Optics and Photonics **1**, 279 (2009).

[30] See NTT-NICT system in M. Sasaki *et al.*, Opt. Express **19**, 10387 (2011).

[31] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

[32] M. Curty, M. Jofre, V. Pruneri, and M. W. Mitchell, e-print arXiv:1108.0841 (to be published); M. Curty, X. Ma, H. K. Lo, and N. Lütkenhaus, Phys. Rev. A **82**, 052325 (2010).