Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors

Xiang-Bin Wang*

Department of Physics and State Key Laboratory of Low Dimensional Quantum Physics, Tsinghua University, Beijing 100084, China and Jinan Institute of Quantum Technology, Shandong Academy of Information Technology, Jinan, China

(Received 9 August 2012; revised manuscript received 28 August 2012; published 18 January 2013)

We study the measurement-device-independent quantum key distribution (MDIQKD) in practice with limited resources when there are only three different states in implementing the decoy-state method and when there are basis-dependent coding errors. We present general formulas for the decoy-state method for two-pulse sources with three different states, which can be applied to the recently proposed MDIQKD with imperfect single-photon sources such as the coherent states or the heralded states from the parametric down-conversion. We point out that the existing result for secure MDIQKD with source coding errors does not always hold. We find that very accurate source coding is not necessary. In particular, we loosen the precision of the existing result by several orders of magnitude.

DOI: 10.1103/PhysRevA.87.012320 PACS number(s): 03.67.Dd, 42.81.Gs, 03.67.Hk

I. INTRODUCTION

Security for real setups of quantum key distribution (QKD) [1,2] has become a major problem in the area in recent years. The major problems here include the imperfection of sources and the limited efficiency of the detection device. The decoy-state method [3–12] can help to make a setup with an imperfect single-photon source be as secure as that with a perfect single-photon source [13,14].

Aside from the source imperfection, the limited detection is another threat to the security [15]. Theories of the device-independent security proof [16] have been proposed to overcome the problem. However, these theories can not apply to the existing real setups because violation of Bell's inequality can not be strictly demonstrated by existing setups. Very recently, an idea of measurement-device-independent QKD (MDIQKD) was proposed based on the idea of entanglement swapping [17,18]. There, one can make secure QKD simply by virtual entanglement swapping, i.e., both Alice and Bob send BB84 (Bennett-Brassard 1984) protocol states to the relay which can be controlled by an untrusted third party (UTP). After the UTP announced his measurement outcome, Alice and Bob will post select those bits corresponding to a successful event and prepared in the same basis for further processing. In the realization, Alice and Bob can really use entanglement pairs [17] and measure halves of the pair inside the laboratory before sending another half to the UTP. In this way, the decoy-state method is not necessary even though imperfect entangled pairs (such as the states generated by the type-II parametric down-conversion) are used. Even though there are multipair events with small probability, these events do not affect the security. Alice and Bob only need to check the error rates of their post-selected bits. However, in our existing technologies, high-quality entangled-pair-state generation can not be done efficiently. In the most mature technology, the generation rate is lower than 1 from 1000 pump pulses. If we want to obtain a higher key rate, we can choose to directly use an imperfect single-photon source such as the coherent state [18]. If we choose this, we must be careful for two issues. First, we must implement the decoy-state method for security. Although this has been discussed in Ref. [18], calculation formulas for the practical decoy-state implementation with only a few different states are not given. Second, in this way, the states for coding are prepared actively. If we can not guarantee to make exactly the BB84 states, we must exercise special caution for the security. Although there are already some results for this [19], there are some drawbacks in the practical application of the existing result [19]. First, it requires a very accurate source coding, e.g., an order of magnitude of 10^{-7} for the state errors for MDIQKD over a distance longer than 100 km s. Second, the existing conclusion seems to be not always correct. The existing theory [19] shows that the source coding error affects the key rate only through the fidelity between the density matrices of two bases. According to its conclusion, if the density operators of states in the two bases are identical, then one can calculate the key rate as if an ideal realization of MDIQKD were done. In such a case, the key rate is determined solely by the detected error rate. Consider such a special case: in the protocol, Alice and Bob can produce the perfect BB84 states in the Z basis, $|0_z\rangle$ and $|1_z\rangle$, but they make big errors in preparing states in the X basis. They actually prepared $|0_z\rangle$ or $|1_z\rangle$ whenever they *want* to prepare states $|0_x\rangle$ or $|1_x\rangle$. Given this fact, Eve or the UTP can simply measure each pulse in the Z basis without causing any additional noise. Therefore, correct theory should give a 0 key rate for this. However, the existing theory can result in a considerable key rate for this case because in principle one can obtain many post-selected successful events with *small* error rate in MDIQKD (see erratum in Ref. [19]). Such a problem also exists in the MDIQKD protocol with entangled-pair states [17]. Although the states out of the laboratories are identical for whatever basis, the measurement basis alignment error in detecting the halves of the pair states inside each laboratory can undermine the security. In an extreme example, they make measurement in the Z basis perfectly. But, when they *want* to use the X basis, they actually used the Z basis. Normally, users are not likely to make such big mistakes, however, the existing theory seemed to even *allow* these mistakes.

*xbwang@mail.tsinghua.edu.cn

In this work, we shall first present formulas of a three-state decoy-state method for the MDIQKD. We then study the problem of source coding error. Our result presented here does not require source coding as accurate as the existing ones, which require an order of magnitude of 10^{-7} for the state errors; our requirement for the accuracy is several orders of magnitude less precise. Based on the idea of constructing virtual BB84 sources, our result is strict for security.

II. DECOY-STATE METHOD WITH ONLY THREE STATES FOR MDIQKD

In the protocol, each time a pulse pair (two-pulse state) is sent to the relay for detection, the relay is controlled by an untrusted thirty party (UTP). The UTP will announce whether the pulse pair has caused a successful event. Those bits corresponding to successful events will be post selected and further processed for the final key. Since real setups only use imperfect single-photon sources, we need the decoy-state method for security.

We assume Alice (Bob) has three sources o_A,x_A,y_A (o_B,x_B,y_B) which can only emit three different states $\rho_{o_A} = |0\rangle\langle 0|,\rho_{x_A},\rho_{y_A}$ ($\rho_{o_B} = |0\rangle\langle 0|,\rho_{x_B},\rho_{y_B}$), respectively, in photon-number space. Suppose

$$\begin{aligned} \rho_{x_A} &= \sum_k a_k|k\rangle\langle k|;\ \ \rho_{y_A} = \sum_k a'_k|k\rangle\langle k|, \\ \rho_{x_B} &= \sum_k b_k|k\rangle\langle k|;\ \ \rho_{y_B} = \sum_k b'_k|k\rangle\langle k|, \end{aligned} \tag{1}$$

and we require that the states satisfy the following very important condition:

$$\frac{a'_k}{a_k} \geqslant \frac{a'_2}{a_2} \geqslant \frac{a'_1}{a_1}, \quad \frac{b'_k}{b_k} \geqslant \frac{b'_2}{b_2} \geqslant \frac{b'_1}{b_1} \tag{2}$$

for $k \geqslant 2$. The imperfect sources used in practice such as the coherent state source, the heralded source out of the parametric down-conversion, satisfy the above restriction. Given a specific type of source, the above-listed different states have different averaged photon numbers (intensities), therefore the states can be obtained by controlling the light intensities. At each time, Alice will randomly select one of her three sources to emit a pulse, and so does Bob. The pulse from Alice and the pulse from Bob form a pulse pair and are sent to the untrusted relay. We regard equivalently that each time a two-pulse source is selected, a pulse pair (one pulse from Alice, one pulse from Bob) is emitted. There are many different two-pulse sources used in the protocol. We denote $\alpha\beta$ for the two-pulse source when the pulse pair is produced by source α at Alice's side and source β at Bob's side, and α can be one of $\{o_A,x_A,y_A\}$ and β can be one of $\{o_B,x_B,y_B\}$. For example, at a certain time j, Alice uses source o_A and Bob uses source y_B, we say the pulse pair is emitted by source $o_A y_B$.

In the protocol, two different bases, the Z basis consisting of horizontal polarization $|H\rangle\langle H|$ and vertical polarization $|V\rangle\langle V|$ and the X basis consisting of $\pi/4$ and $3\pi/4$ polarizations, are used. The density operator in photon-number space alone does not describe the state in the composite space. We shall apply the decoy-state-method analysis in the same basis (e.g., the Z basis or X basis) for pulses from sources x_A,x_B,y_A,y_B. Therefore, we only need consider the density operators in the photon-number space. For simplicity, we consider pulses from source prepared in the Z basis first.

According to the decoy-state theory, the yield of a certain set of pulse pairs is defined as source $\alpha\beta$ is defined as the happening rate of a successful event (announced by the UTP) corresponding to pulse pairs out of the set. Mathematically, the yield is n/N where n is the number of successful events happened corresponding to pulse pairs from the set and N is the number of pulse pairs in the set. Obviously, if we regard the pulse pairs of two-pulse source $\alpha\beta$ as a set, the yield $S_{\alpha\beta}$ for source $\alpha\beta$ is $S_{\alpha\beta} = \frac{n_{\alpha\beta}}{N_{\alpha\beta}}$, where $n_{\alpha\beta}$ is the number of successful events that happened corresponding to pulse pairs from source $\alpha\beta$ and $N_{\alpha\beta}$ is the number of times source $\alpha\beta$ is used. In the protocol, there are nine different two-pulse sources. The yields of these nine sources can be directly calculated from the observed experimental data $n_{\alpha\beta}$ and $N_{\alpha\beta}$. We use capital letter $S_{\alpha\beta}$ for these *known* values.

We can regard any source as a composite source that consists of many (virtual) subsources if the source state can be be written in a convex form of different density operators. For example, two-pulse source $y_A y_B$ includes a subsource of pulse pairs of state $\rho_1 \otimes \rho_1$ ($\rho_1 = |1\rangle\langle 1|$) with weight $a'_1 b'_1$. This is to say, after we have used source $y_A y_B$ for N times, we have actually used subsource of state $\rho_1 \otimes \rho_1$ for $a'_1 b'_1 N$ times, asymptotically. Similarly, the source $x_A x_B$ also includes a subsource of state $\{\rho_1 \otimes \rho_1\}$ with weight $a_1 b_1$. These two subsources of state $\rho_1 \otimes \rho_1$ must have the same yield s_{11} because they have the same two-pulse state and the pulse pairs are randomly mixed. Most generally, denote s,s' as the yields of two sets of pulses if pulse pairs of these two sets are randomly mixed and all pulses have the same density operator, then

$$s = s' \tag{3}$$

asymptotically. This is the elementary assumption of the decoy-state theory.

In the protocol, since each source is randomly chosen, pulses from each subsource or source are also randomly mixed. Therefore, the yield of a subsource or a source is dependent on the *state* only; it is independent of which physical source the pulses are from. Therefore, we can also define the yield of a certain state: whenever a pulse pair of that state is emitted, there is a probability that a successful event happens. Denote

$$\Omega_{\alpha\beta} = \rho_\alpha \otimes \rho_\beta \tag{4}$$

for a two-pulse state. The yield of such a state is also the yield of any source which produces state $\Omega_{\alpha\beta}$ only, or the yield of a subsource from *any* source, provided that the state of the pulse pairs of the subsource is $\Omega_{\alpha\beta}$. Note that we do not always know the value of yield of a state because we do not know which subsource was used at which time. We shall use the lower-case symbol $s_{\alpha,\beta}$ to denote the yield of state $\Omega_{\alpha,\beta}$. In general, the yields of a subsource (a state) such as s_{11} is not directly known from the experimental data. But, some of them can be deduced from the yields of different real sources. Define $\rho_0 = |0\rangle\langle 0|$. According to Eq. (3), if $\alpha \in \{0,x_A,y_A\}$ and $\beta \in \{0,x_B,y_B\}$, we have

$$s_{\alpha\beta} = S_{\tilde{\alpha}\tilde{\beta}} \tag{5}$$

with the mapping of $\tilde{\alpha} = (o_A, x_A, y_A)$ for $\alpha = (0, x_A, y_A)$, respectively, and $\tilde{\beta} = (o_B, x_B, y_B)$ for $\beta = (0, x_B, y_B)$, respectively. To understand the meaning of the equation above, we take an example for pulses from source $y_A y_B$. By writing the state of this source in the convex form, we immediately know that it includes a subsource of state $\rho_0 \otimes \rho_{y_B}$. By observing the results caused by source $y_A y_B$ itself, we have no way to know the yield of this subsource because we do not know exactly which time source y_A emits a vacuum pulse when we use it. However, the state of this subsource is the same with the state of the real source $o_A y_B$, therefore, the yield of any subsource of state $\rho_0 \otimes \rho_{y_B}$ must be just the yield of the real source $o_A y_B$, which can be directly observed in the experiment. Mathematically, this is $s_{0y_B} = S_{o_A y_B}$, where the right-hand side is the known value of yield of real source $o_A y_B$ and the left-hand side is the yield of a virtual subsource from real source $y_B y_B$.

Our first major task is to deduce s_{11} from the known values, i.e., to formulate s_{11}, the yield of state $|1\rangle\langle 1| \otimes |1\rangle\langle 1|$ in capital-letter symbols $\{S_{\alpha\beta}\}$. We shall use the following convex proposition to do the calculation. Denote S to be the yield of a certain source of state Ω. If Ω has the convex forms of $\Omega = \sum_{\alpha\beta} c_{\alpha\beta}\Omega_{\alpha\beta}$, we have

$$S = \sum_{\alpha,\beta} c_{\alpha\beta} s_{\alpha\beta}. \tag{6}$$

This equation is simply the fact that the total number of successful events caused by pulses from a certain set is equal to the summation of the numbers of successful events caused by pulses from each subset.

Consider the convex forms of sources $x_A x_B$ and $y_A y_B$. Explicitly,

$$\begin{aligned}\Omega_{x_A x_B} = {} & \tilde{c}_0\tilde{\Omega}_0 + a_1 b_1 \rho_1 \otimes \rho_1 + a_1 c_B \rho_1 \otimes \rho_{c_B} \\ & + b_1 c_A \rho_{c_A} \otimes \rho_1 + c_A c_B \rho_{c_A} \otimes \rho_{c_B},\end{aligned} \tag{7}$$

where $\tilde{c}_0\tilde{\Omega}_0 = (a_0\Omega_{0,x} + b_0\Omega_{x,0} - a_0 b_0 \Omega_{0,0})$, $c_A\rho_{c_A} = (\sum_{k\geqslant 2} a_k |k\rangle\langle k|)$, and $c_B\rho_{c_B} = (\sum_{k\geqslant 2} b_k |k\rangle\langle k|)$. According to Eq. (6), this leads to

$$S_{x_A x_B} = \tilde{S}_0 + a_1 b_1 s_{11} + a_1 c_B s_{1c_B} + b_1 c_A s_{c_A 1} + c_A c_B s_{c_A c_B} \tag{8}$$

and

$$\tilde{S}_0 = a_0 S_{o_A x_B} + b_0 S_{x_A o_B} - a_0 b_0 S_{o_A o_B}. \tag{9}$$

We also have

$$\begin{aligned}\Omega_{y_A y_B} = {} & \tilde{c}'_0\tilde{\Omega}'_0 + a'_1 b'_1 \rho_1 \otimes \rho_1 + a'_1 c'_B \rho_1 \otimes \rho_{c'_B} \\ & + b'_1 c'_A \rho_{c'_A} \otimes \rho_1 + c'_A c'_B \rho_{c'_A} \otimes \rho_{c'_B},\end{aligned} \tag{10}$$

where $\tilde{c}'_0\tilde{\Omega}'_0 = (a'_0\Omega_{0,y_B} + b'_0\Omega_{y_A,0} - a'_0 b'_0 \Omega_{0,0})$, $c'_A\rho_{c'_A} = (\sum_{k\geqslant 2} a'_k |k\rangle\langle k|)$, and $c'_B\rho_{c'_B} = (\sum_{k\geqslant 2} b_k |k\rangle\langle k|)$. According to these, there exists $d_A \geqslant 0$ and $d_B \geqslant 0$ and normalized density operators ρ_{d_A} and ρ_{d_B} so that

$$c'_A\rho_{c'_A} = \frac{a'_2}{a_2} c_A\rho_{c_A} + d_A\rho_{d_A}, \quad c'_B\rho_{c'_B} = \frac{b'_2}{b_2} c_B\rho_{c_B} + d_B\rho_{d_B}. \tag{11}$$

Here, we have used the condition of Eq. (2). According to the definitions of $c_A\rho_{c_A}$ and $c'_A\rho_{c'_A}$, we have

$$d_A\rho_{d_A} = c'_A\rho_{c'_A} - \frac{a'_2}{a_2} c_A\rho_{c_A} = \sum_{k\geqslant 2}\left(a'_k - \frac{a'_2}{a_2} a_k\right)|k\rangle\langle k|. \tag{12}$$

Using the condition of Eq. (2), we find $a'_k - \frac{a'_2}{a_2} a_k = a_k(\frac{a'_k}{a_k} - \frac{a'_2}{a_2}) \geqslant 0$ for all $k \geqslant 2$. This proves the first part of Eq. (11). Similarly, we can also prove the second part of Eq. (11). Therefore, we have

$$\begin{aligned}\Omega_{y_A y_B} = {} & \tilde{c}'_0\tilde{\Omega}'_0 + a'_1 b'_1 \rho_1 \otimes \rho_1 + a'_1 \rho_1 \otimes \left(\frac{b'_2}{b_2} c_B\rho_{c_B} + d_B\rho_{d_B}\right) \\ & + b'_1\left(\frac{a'_2}{a_2} c_A\rho_{c_A} + d_A\rho_{d_A}\right) \otimes \rho_1 \\ & + \left(\frac{a'_2}{a_2} c_A\rho_{c_A} + d_A\rho_{d_A}\right) \otimes \left(\frac{b'_2}{b_2} c_B\rho_{c_B} + d_B\rho_{d_B}\right),\end{aligned} \tag{13}$$

which means that

$$\begin{aligned}S_{y_A y_B} = {} & \tilde{S}'_0 + a'_1 b'_1 s_{11} + \frac{b'_2}{b_2} a'_1 c_B s_{1c_B} + \frac{a'_2}{a_2} b'_1 c_A s_{c_A 1} \\ & + \frac{b'_2 a'_2}{b_2 a_2} c_A c_B s_{c_A c_B} + \xi,\end{aligned} \tag{14}$$

where

$$\tilde{S}'_0 = a'_0 S_{o_A y_B} + b'_0 S_{y_A o_B} - a'_0 b'_0 S_{o_A o_B} \tag{15}$$

and $\xi = a'_1 d_b s_{1d_B} + b'_1 s_{d_A 1} + c'_A s_{c'_A d_B} + c'_B s_{d_A c'_B} \geqslant 0$. For any sources used in the protocol, we must have either $K_a = \frac{a'_1 b'_2}{a_1 b_2} \leqslant \frac{a'_2 b'_1}{a_2 b_1} = K_b$ or $K_a \geqslant K_b$. Suppose the former one holds. Calculating [Eq. (8)]$\times K_a -$[Eq. (14)], we obtain

$$s_{11} = \frac{K_a(S_{x_A x_B} - \tilde{S}_0) - (S_{y_A y_B} - \tilde{S}'_0) + \zeta_1 + \zeta_2 + \xi}{K_a a_1 b_1 - a'_1 b'_1},$$

where $\tilde{S}_0$ and $\tilde{S}'_0$ are defined by Eqs. (9) and (15), respectively, and $\zeta_1 = (\frac{a'_2}{a_2} b'_1 - K_a b_1) c_A s_{c_A 1} = (K_b - K_a) b_1 c_A s_{c_A 1} \geqslant 0$, $\zeta_2 = (\frac{a'_2 b'_2}{a_2 b_2} - K_a) c_A c_B s_{c_A c_B} = (\frac{a_1}{a'_1}\frac{a'_2}{a_2} - 1) K_a c_A c_B s_{c_A c_B} \geqslant 0$. Note that $\frac{a_1}{a'_1}\frac{a'_2}{a_2} \geqslant 1$ according to Eq. (2). As shown already, $\xi \geqslant 0$. Thus, we have

$$s_{11} \geqslant \frac{a'_1 b'_2 (S_{x_A x_B} - \tilde{S}_0) - a_1 b_2 (S_{y_A y_B} - \tilde{S}'_0)}{a'_1 a_1 (b'_2 b_1 - b_2 b'_1)}, \tag{16}$$

where $\tilde{S}_0$ and $\tilde{S}'_0$ are defined by Eqs. (9) and (15), respectively. If $K_a \geqslant K_b$ holds, through calculating [Eq. (8)]$\times K_b -$[Eq. (14)], we obtain

$$s_{11} \geqslant \frac{a'_2 b'_1 (S_{x_A x_B} - \tilde{S}_0) - a_2 b_1 (S_{y_A y_B} - \tilde{S}'_0)}{b'_1 b_1 (a'_2 a_1 - a'_1 a_2)}.$$

This and Eq. (16) are our major formula for the decoy-state-method implementation for MDIQKD. Note that this formula always holds for whatever source satisfies the condition in Eq. (2). Physical sources such as the coherent light, the heralded source by the parametric down-conversion all meet the condition. We thus arrive at the major conclusion of this section.

In the protocol, there are two different bases. We denote s_{11}^Z and s_{11}^X for yields of single-photon pulse pairs in the Z and X bases, respectively. Consider those post-selected bits caused by source $y_A y_B$ in the Z basis. After an error test, we know the bit-flip error rate of this set, say $E_{y_B y_B}^Z$. We also need the phase-flip rate for the subset of bits which are caused by the two single-photon pulses, say E_{11}^{ph}, which is equal to the flip rate of post-selected bits caused by a single photon in the X basis, say E_{11}^X. We have

$$E_{11}^X \leqslant \frac{\left(E_{x_A x_B}^X - \tilde{E}_0\right)\left(S_{x_A x_B}^X - \tilde{S}_0^X\right)}{a_1 b_1 s_{11}^X}. \tag{17}$$

Here, $E_{\alpha\beta}^X$ is the error rate for those post-selected bits in the X basis, caused by pulses from source $\alpha\beta$; $S_{\alpha\beta}^X$ is the yield of source $\alpha\beta$ in the X basis; $\tilde{E}_0 = a_0 E_{o_A x_B}^X + b_0 E_{x_A o_B}^X - a_0 b_0 E_{o_A o_B}$ and $\tilde{S}_0^X = a_0 S_{o_A x_B}^X + b_0 S_{x_A o_B}^X - a_0 b_0 S_{o_A o_B}$. If $\rho_{x_A} = \rho_{x_B}$ and $\rho_{y_A} = \rho_{y_B}$, we simply replace all b_0, b_1 above by a_0, a_1. Given this, we can now calculate the key rate by the well-known formula. For example, for those post-selected bits caused by source $y_A y_B$, it is

$$R = a_1' b_1' s_{11}^Z \left[1 - H\left(E_{11}^X\right)\right] - f S_{y_A y_B} H\left(E_{y_B y_B}^Z\right), \tag{18}$$

where f is the efficiency factor of the error correction method used.

Now, we discuss the value of s_{11}^X as used in Eq. (17). If we implement the decoy-state method for different bases separately, we can calculate s_{11}^Z and s_{11}^X separately and s_{11}^X is known. We can also choose to implement the decoy-state method only in the Z basis. This is to say, in the X basis, we do not have state $\rho_{y_A y_B}$, we only have state $\rho_{x_A x_B}$. All pulses of state $\rho_{y_B y_B}$ will be only prepared in the Z basis. The advantage of this is to reduce the basis mismatch so as to raise the key rate. The value of s_{11} for X-basis pulses can be deduced from that for the Z basis. Suppose that at each side, horizontal and vertical polarizations have equal probability to be chosen. For all those single-photon pairs in the Z basis, the state in polarization space is

$$\tfrac{1}{4}\left(\Omega_{11}^{HH} + \Omega_{11}^{VV} + \Omega_{11}^{HV} + \Omega_{11}^{VH}\right) = \tfrac{1}{4} I, \tag{19}$$

where $\Omega_{11}^{PQ} = |P\rangle\langle P| \otimes |Q\rangle\langle Q|$, P, Q indicate the polarization which can be either H or V. On the other hand, for all those two single-photon pulse pairs prepared in the X basis, if the $\pi/4$ and $3\pi/4$ polarizations are chosen with equal probability, one can easily find that the density matrix for these single-photon pairs is also $I/4$. Therefore, we conclude

$$s_{11}^Z = s_{11}^X. \tag{20}$$

III. SECURITY WITH BASIS-DEPENDENT CODING ERRORS

In practice, there are many imperfections for the real setups, for example, that Eqs. (3) and (5) only hold *asymptotically*. The number of pulses is finite, hence these equations do not hold exactly due to the statistical fluctuation. Say, s and s', $s_{\alpha,\beta}$ and $S_{\tilde{\gamma},\tilde{\beta}}$ can be a bit different. Denote $s_{\alpha\beta}$ and $s_{\alpha\beta}'$ for the yields of pulses of states $\rho_\alpha \otimes \rho_\beta$ from two different sources. In general, we have

$$s_{\alpha\beta} = s_{\alpha\beta}'(1 + \delta_{\alpha\beta}), \tag{21}$$

where $\delta_{\alpha\beta}$ is the statistical fluctuation whose value is among a certain range with a probability exponentially close to 1. The range can be calculated given the number of pulses of each subsource. We can then seek the worst-case result among the range of $\delta_{\alpha\beta}$. Another imperfection is the intensity fluctuation. This can also be solved by the way given in [10].

Here, we consider the state-dependent coding errors, as studied in [19]. For clarity, we first consider the normal QKD protocol where Alice sends pulses and Bob receives and detects them. The main idea is to decompose a density operator into convex form and the concept of virtual subsources. The result is enhanced by combining additional real operation of imperfect phase randomizing.

A. Density operator decomposition, virtual subsources, and basis-dependent error for the normal QKD protocol

For simplicity, we assume a perfect single-photon source with basis-dependent coding errors. Say, at a certain time j, Alice *wants* to prepare state $|0_{jW}\rangle$ or $|1_{jW}\rangle$ in basis W (W can be Z or X) according to her bit value 0 or 1, she actually prepares $|0_{jW}^{act}\rangle = \cos\theta_{0jW}|0_{jW}\rangle + \sin\theta_{0jW} e^{i\delta_{0jW}}|1_{jW}\rangle$ or $|1_{jW}^{act}\rangle = \cos\theta_{1jW}|1_{jW}\rangle + \sin\theta_{1jW} e^{i\delta_{1jW}}|0_{jW}\rangle$. We name this subscribed θ as *error angle*. At different times of j, the subscribed values of parameters θ and δ can be different and can be correlated at different times. We set the *threshold angles* θ_Z and θ_X as

$$\mathrm{Max}\{|\theta_{0jZ}|, |\theta_{1jZ}|\} \leqslant \theta_Z, \quad \mathrm{Max}\{|\theta_{0jX}|, |\theta_{1jX}|\} \leqslant \theta_X; \tag{22}$$

of course, all $\{|\theta_{0jW}|, |\sin\theta_{1jW}|\}$ must be rather small, otherwise no secure final key can be generated. Actually, as shall be shown later, our theory also applies to the case that most of these θ angles are very small, but occasionally the values can be large. In such a case, we only need to reset the threshold angles as larger than most of $\{|\theta_{0jW}|, |\theta_{1jW}|\}$ so that the threshold values can be still rather small. For this moment, we use Eq. (22). Also, we omit the subscript j if it does not cause any confusion. Our main idea is to modify the protocol by randomly producing a wrong state with a certain small probability. In this way, each single-photon state can be decomposed into a classical probabilistic mixture of two states, with one of them being ideal BB84 states. Therefore, there exists a virtual BB84 subsource in the protocol, and states generated by that subsource are perfect BB84 states. By decomposing the density operator of the BB84 source, $I/2$, one finds that the yield of such a source is at least half of any other source. Therefore, the lower bound of fraction of bits caused by the ideal BB84 source can be calculated with whatever channel loss. With this, the phase-flip error rate of the BB84 subsource can also be calculated and hence one can obtain the final key rate.

1. *Modified protocol and virtual ideal BB84 subsources*

We consider the modified protocol as the following: According to her prepared bit value ($b = 0$ or 1) in the W basis, instead of preparing state $|0_W^{act}\rangle$ (or $|1_W^{act}\rangle$), she takes a probability $1 - p_w$ to prepare a state $|0_W^{act}\rangle$ and a small

probability p_w to intentionally prepare a wrong state $|1_W^{act}\rangle$. Therefore, the density matrix of a pulse corresponding to bit values 0 or 1 in the Z basis is

$$\rho_0^Z = (1-p_z)\left|0_Z^{act}\right\rangle\left\langle 0_Z^{act}\right| + p_z\left|1_Z^{act}\right\rangle\left\langle 1_Z^{act}\right| \tag{23}$$

or

$$\rho_1^Z = (1-p_z)\left|1_Z^{act}\right\rangle\left\langle 1_Z^{act}\right| + p_z\left|0_Z^{act}\right\rangle\left\langle 0_Z^{act}\right|, \tag{24}$$

respectively. It is easy to show that, by choosing an appropriate value p_z, there exists positive value Δ_z so that the density matrices of ρ_0^Z and ρ_1^Z can be written in the convex forms of

$$\rho_0^Z = \Delta_z|0_Z\rangle\langle 0_Z| + (1-\Delta_z)\rho_{z0,res} \tag{25}$$

and

$$\rho_1^Z = \Delta_z|1_Z\rangle\langle 1_Z| + (1-\Delta_z)\rho_{z1,res}. \tag{26}$$

Here, Δ_z can be rather close to 1 if θ_z is small. For example, by setting $p_z = |\tan\theta_z|$, we can take

$$\Delta_z = \cos^2\theta_z(1-2\tan\theta_z) \tag{27}$$

for the above convex forms. Similarly, we find those states for bits 0 or 1 in the X basis can also be decomposed to convex forms of

$$\begin{aligned}\rho_0^X &= \Delta_x|0_X\rangle\langle 0_X| + (1-\Delta_x)\rho_{x0,res},\\ \rho_1^X &= \Delta_x|1_X\rangle\langle 1_X| + (1-\Delta_x)\rho_{x1,res}\end{aligned} \tag{28}$$

and we can take

$$\Delta_x = \cos^2\theta_x(1-2\tan\theta_x) \tag{29}$$

by setting

$$p_x = \tan\theta_x. \tag{30}$$

For a pulse sent at any time by Alice, the state can be one of $\{\rho_0^Z,\rho_1^Z,\rho_0^X,\rho_1^X\}$, and depends on the bit value and the basis she has chosen for that pulse. However, given the convex forms above, we can now assume different virtual sources. For state ρ_0^Z, we assume two virtual sources: source $\tilde{z}_0$ which produces state $|0_Z\rangle\langle 0_Z|$ only, and source z_0' which produces state $\rho_{z0,res}$ only. Say, whenever Alice decides to send out ρ_0^Z, we assume she uses source $\tilde{z}_0$ with probability Δ_z or uses source z_0' with probability $1-\Delta_z$. Similarly, we have virtual source $\tilde{z}_1$ which only produces state $|1_Z\rangle\langle 1_Z|$ and virtual source z_1' which only produces state $\rho_{z1,res}$. When Alice decides to send a state corresponding to bit 1 in the Z basis, we can equivalently assume that she uses source $\tilde{z}_1$ or source z_1' with probabilities of Δ_z and $1-\Delta_z$. In the same idea, we also assume virtual subsources $\tilde{x}_b,x_b'$ which only produce state $|b_X\rangle\langle b_X|$ or $\rho_{xb,res}$, with probabilities of Δ_x and $1-\Delta_x$, and $b=0,1$. *If we only use those bits caused by pulses from virtual subsources $\tilde{z}_b,\tilde{x}_b$, it is just an ideal QKD protocol without any coding error and hence the standard results apply directly*. We call these virtual subsource and the phase-flip rate for bits from the *idea subsource* as requested by standard BB84 protocol. Also, we name virtual subsources w_b' as *tagged subsource* since we assume the worst case that Eve can know bit values corresponding to a pulse from any tagged subsource. (Here, w can be x or y and b can be 0 or 1.)

2. *Fraction of bits from ideal BB84 source and final key rate*

Since these subsources are virtual, we do not know which pulses are from them. Given a lossy channel, we need to estimate faithfully how many bits are generated by the ideal subsource the phase-flip rate for bits from the ideal sources. Define virtual source $\tilde{w} = \tilde{w}_0 + \tilde{w}_1$, where w can be either z or x. This means that virtual source $\tilde{z}$ (or $\tilde{x}$) includes all pulses from ideal BB84 subsources in the Z (or X) basis. Obviously, the density operator of a pulse from such an ideal source is simply $\tilde{\rho}_w = I/2$. We also regard the two tagged subsources subscribed by 0 or 1 as one composite tagged source w', say, $w' = w_0' + w_1'$. The density operator of a pulse from such a source in the W basis at a certain time j is $\rho_w'(j) = \frac{\rho_{w0,res}+\rho_{w1,res}}{2}$. For example, in the X basis, the density operator of a pulse from such a source (source x') at time j is $\rho_x'(j) = \frac{\rho_{x0,res}+\rho_{x1,res}}{2}$. The state of a pulse in the X basis at time j is

$$\rho_X(j) = \Delta_x I/2 + (1-\Delta_x)\rho_x'(j). \tag{31}$$

Here, Δ_x is independent of time j, although ρ_x' is dependent on time j. This means that whenever there is a pulse in the X basis sent out, it has a probability Δ_x that the ideal source $\tilde{w}$ is used, and a probability $1-\Delta_x$ that the tagged source x' is used. To estimate the upper bound of error rate of post-selected bits caused by pulses from source $\tilde{x}$, we need the lower bound of the fraction of bits caused by virtual source $\tilde{x}$ among all post-selected bits in basis X. Note that the density matrix for source $\tilde{x}$ is simply $I/2$, and there always exists a density operator $\bar{\rho}$ so that source $\tilde{x}$ can have the convex form of

$$I/2 = \tfrac{1}{2}[\bar{\rho}(j) + \rho_x'(j)]. \tag{32}$$

Here, $\bar{\rho}(j)$ is defined as $\bar{\rho}(j) = \left(\begin{smallmatrix} c & -d \\ -b & a\end{smallmatrix}\right)$ if $\rho_x'(j) = \left(\begin{smallmatrix} a & d \\ b & c\end{smallmatrix}\right)$. This means that we can regard source $\tilde{x}$ as a mixed source consisting of two parts: source $\tilde{\tilde{x}}$ that can only emit $\bar{\rho}(j)$ at time j and source $\tilde{x}'$ that can only emit $\rho_x'(j)$ at time j. Whenever a pulse is sent out of source $\tilde{x}$, with half a probability that source $\tilde{x}'$ is used, which generates the same state $[\rho_x'(j)]$ as the tagged source x' does, at any time j. Asymptotically, if the total number of X-basis pulses sent out is N_x, there are $\tilde{N}_x = N_x\Delta_x$ from ideal source $\tilde{x}$ and $N_x(1-\Delta_x)$ from tagged source x'. Denote $\tilde{s}_x$, $\tilde{\tilde{s}}_x$, $\tilde{s}_x'$, and s_x' as the yield of sources $\tilde{x}$, $\tilde{\tilde{x}}$, $\tilde{x}'$, and x', respectively. We have

$$\tilde{s}_x = \tfrac{1}{2}\tilde{\tilde{s}}_x + \tfrac{1}{2}\tilde{s}_x' \geqslant \tfrac{1}{2}s_x'. \tag{33}$$

Here, we have used the following two facts: (1) The yield of any source must be non-negative, therefore, $\tilde{\tilde{s}}_x \geqslant 0$. (2) The sources $\tilde{x}'$ and x' can only produce the same state $[\rho_x'(j)]$ at any time j, and they must have the same yield in the whole protocol. Therefore, among all bits caused by source X, the fraction of bits caused by ideal source $\tilde{x}$ is

$$\tilde{\Delta}_x = \frac{N_x\Delta_x\tilde{s}_x}{N_x\Delta_x\tilde{s}_x + N_x(1-\Delta_x)s_x'} \geqslant \frac{\Delta_x/2}{1-\Delta_x/2} = \tilde{\Delta}_x^l. \tag{34}$$

In the Z basis, there is also a similar formula. Asymptotically, among all those post-selected bits of basis W, the fraction of bits caused by source $\tilde{w}$ is

$$\tilde{\Delta}_w \geqslant \frac{\Delta_w}{2-\Delta_w} = \frac{\cos^2\theta_w(1-2\tan\theta_w)}{\sin^2\theta_w + (\sin\theta_w+\cos\theta_w)^2}. \tag{35}$$

Suppose the error rate for all X-basis bits is E^X. Then, the error rate for bits caused by pulses from source $\tilde{x}$ and the phase-flip rate of Z-basis bits caused by pulses from source $\tilde{z}$ is

$$E^Z_{z,ph} = E^X_x = \frac{E^X}{\tilde{\Delta}_x}. \tag{36}$$

We have assumed a perfect single-photon source in the above. If we use an imperfect single-photon source, we need to implement the decoy-state method. We have the key rate formula

$$R = \tilde{\Delta}_z \Delta_1 \left[1 - H\left(\frac{E^X}{\tilde{\Delta}_x \Delta_1}\right)\right] - fH(E) \tag{37}$$

and $\tilde{\Delta}_x$, $\tilde{\Delta}_z$ are given by Eq. (35), E is the detected error rate of Z-basis bits, and Δ_1 is the fraction of single-photon pulse bits in the Z basis as post selected.

In the protocol, we request Alice take random flip of her qubits with a small probability. However, these flipping operations are actually not necessary physically. Instead of flipping the qubits physically, she can choose to randomly flip her classical bit values with the same small probability. Similar to the case of flipping her qubits physically, this will cause a rise in the error rate. The rise of the bit-flip part does not decrease the final key rate because Alice knows which bits have been flipped. The rise of the phase-flip part is the major factor that causes the final key dropping. Aside from this, there are also factors such as $\tilde{\Delta}_z$ in the key rate formula and $1/\tilde{\Delta}_x$ in estimating the phase error. These also decrease the key rate, but the amount decreased is almost negligible compared with the factor of phase-flip rise. However, all these do not require a *very* accurate source coding. Obviously, one can obtain final key given the largest source error (i.e., $\sin^2\theta_z$) in the order of magnitude of 10^{-4}. This has already loosened the demand in the source accuracy, compared with the existing result which requires an order of magnitude of 10^{-7}–10^{-6}. However, as shall be shown later in our work, we can further loosen the accuracy to 10^{-2}–10^{-1} for the order of magnitude of the largest error by adding a phase-randomizing operation.

In the study above, we have set $\theta_w \geqslant \{|\theta_{0jW}|, |\theta_{1jW}|\}$ for *all* j, i.e., error angles at *all* individual times must by smaller than the threshold angle. We can also treat the case in which most of $|\theta_{0jW}|, |\theta_{1jW}|$ are not larger than θ_w, but a small fraction g_w of them are larger than it. In this case, we only need to reset $\tilde{\Delta}_z, \tilde{\Delta}_x$ in the key rate formula (37) by

$$\tilde{\Delta}_w \longrightarrow \frac{1 - g_w}{1 + g_w}\tilde{\Delta}_w. \tag{38}$$

B. Enhanced results with phase randomizing

We can add real physical operations to the protocol in order to further increase the efficiency. Instead of random flipping to bit values, we can choose to take a phase-randomizing operation to decompose the states into convex form. Suppose we use the photon polarization space. To each qubit in the Z basis, with half a probability we take an additional unitary operation of ($|H\rangle \longrightarrow |H\rangle$, $|V\rangle \longrightarrow -|V\rangle$); to each qubit in the X basis, with half a probability we take an additional unitary operation of ($|+\rangle \longrightarrow |+\rangle$, $|-\rangle \longrightarrow -|-\rangle$). If we can realize such an operation perfectly, we can obtain convex forms for density operators corresponding to each bit value in each basis and we can directly use the ideal of virtual subsources to solve the problem. For example, for those pulses corresponding to bit values 0 and 1 in the Z basis, we have

$$\begin{aligned}\rho^Z_0 &= \cos^2\theta_{z0}|0_Z\rangle\langle 0_Z| + \sin^2\theta_{z0}|1_Z\rangle\langle 1_Z| \\ &= \cos^2\theta_z|0_Z\rangle\langle 0_Z| + \sin^2\theta_z\rho_{z0,res}\end{aligned} \tag{39}$$

and

$$\begin{aligned}\rho^Z_1 &= \cos^2\theta_{z1}|1_Z\rangle\langle 1_Z| + \sin^2\theta_{z1}|1_Z\rangle\langle 1_Z| \\ &= \cos^2\theta_z|1_Z\rangle\langle 1_Z| + \sin^2\theta_z\rho_{z1,res}.\end{aligned} \tag{40}$$

We can imagine that there are subsources of z_0 which only emit state $|0_Z\rangle$ and subsource z_1 which only emits state $|1_Z\rangle$. Each subsource will be used with a constant probability $\cos^2\theta_z/2$. Density operators for those qubits in the X basis can also be decomposed in

$$\rho^X_0 = \cos^2\theta_x|0_x\rangle\langle +| + \sin^2\theta_x\rho_{x0,res} \tag{41}$$

and

$$\rho^X_1 = \cos^2\theta_x|1_Z\rangle\langle 1_Z| + \sin^2\theta_x\rho_{x1,res}. \tag{42}$$

We can regard that there are subsources of x_0 which only emit state $|0_X\rangle$ and subsource x_1 which only emits state $|1_x\rangle$. Each subsource will be used with a constant probability $\cos^2\theta_x/2$. Therefore, pulses from the four subsources above form the ideal BB84 states. We can use Eq. (37) for the key rate, but the value E^X_1 is not overestimated at all, and factors of $\tilde{\Delta}_W = \cos^2\theta_W$, which are almost 1 if θ_W is small. In this way, the tolerable largest coding error is in the order of magnitude of $\frac{1}{10}$ if the phase randomization can be realized. What is most interesting is that we can obtain almost the same good result even though the phase randomization is a little bit imperfect, through applying results in an earlier section.

In an imperfect phase randomization, to each qubit in the X basis, with half a probability we take an additional unitary operation of ($|0_X\rangle \longrightarrow |0_X\rangle$, $|1_X\rangle \longrightarrow |1_X\rangle - e^{-i\delta_2}|+\rangle$). Here, δ_2 are errors in the operations, can be different from time to time, and can be correlated at different times. We assume the largest value for $|\delta_2|$ is δ_x. We can also choose to do phase randomization for qubits in the Z basis, but this is not necessary since the major factor in efficiency is in the tightness of phase-flip rate estimation. Technically, if the phase operation is done in only in one basis, the rotation between the two basis states is negligible. Therefore, we can use the above diagonal form above in the X basis for an imperfect phase operation. By the current mature technology, the value δ_x can be controlled below $\frac{1}{20}$. With these, we obtain the density matrices of qubits in the X basis. For a qubit of bit value 0 in the X basis,

$$\rho^X_0 = \begin{pmatrix} \cos^2\theta_{x0} & \sin 2\theta_{x0}(2\sin^2\delta_1 - i\sin\delta)/4 \\ \sin 2\theta_{x0}(2\sin^2\delta_1 + i\sin\delta)/4 & \sin^2\theta \end{pmatrix}. \tag{43}$$

This can be directly decomposed in

$$\rho_0^X = \Delta_x|0_X\rangle\langle 0_X| + (1-\Delta_x)\rho_{x0,res} \tag{44}$$

and $\Delta_x = \cos^2\theta_x - \sin\theta_x \sin\delta_x/2$. Similarly, we can also decompose the density matrix for bit value 1 in the X basis. Explicitly,

$$\rho_1^X = \Delta_x|1_X\rangle\langle 1_X| + (1-\Delta_x)\rho_{x1,res}. \tag{45}$$

Therefore, there exist two virtual ideal subsources which emit states $|+\rangle$ or $|-\rangle$ only. The fraction of bits caused by pulses form these two ideal subsources among all post-selected X bits is

$$\tilde{\Delta}_x = \frac{\Delta_x}{2-\Delta_x} = \frac{2\cos^2\theta_x - \sin\theta_x\sin\delta_x}{4 - 2\cos^2\theta_x + \sin\theta_x\sin\delta_x}. \tag{46}$$

We do not need to take phase operation to qubits in the Z basis. We just take random flipping to the bit values of the Z basis with a small probability as discussed in an earlier section. We shall still use the key rate formula of Eq. (37), but the key rate is greatly improved now because here the phase-flip rate is overestimated only by a negligible amount, i.e., a factor of $1/\tilde{\Delta}_{AX}$ given by Eq. (46).

C. MDIQKD with source coding errors

Here, we need to convert our results to the case of two-pulse sources. In this case, both Alice and Bob will send their pulses to the untrusted third party (UTP), as has been shown. Neither Alice nor Bob can prepare the coding state exactly. When either one of them *wants* to prepare a state $|b_W\rangle$, she (he) can only prepare a state $|b_W^{act}\rangle = \cos\theta_{bW}|b_W\rangle + e^{i\delta_{bW}}\sin\theta_{bW}|\bar{b}_W\rangle$ and $b = 0,1$, $\bar{b}_W = 1 \oplus b_W$. Most generally, Alice and Bob have different threshold angles, noted as θ_{Az},θ_{Ax} for Alice in the Z or X basis and θ_{Bz},θ_{Bx} for Bob in the Z or X basis.

In our protocol, we require Bob (Alice) to take a probability $1-p_{Bw}$ (or $1-p_{Aw}$) to prepare a state $|b_W^{act}\rangle$ and probability p_{Bw} (p_{Aw}) to prepare $|\bar{b}_W^{act}\rangle$, if the data of bit value indicate that he (she) should prepare a state $|b_W\rangle$, in basis W (i.e., Z or X). By analysis similar to the section above, we can also present the appropriate convex forms and find the ideal subsources for Alice and Bob separately in both bases. Suppose θ_{Aw}, θ_{Bw} are threshold angles in basis W for Alice and Bob, respectively. We can set $p_{\gamma w} = \tan\theta_{\gamma w}$ ($\gamma = A, B$). Then, the density operators at Alice's side and the one at Bob's side can be decomposed in convex forms similar to Eqs. (23) and (24). We have the decomposition form

$$\rho_b^{\alpha W} = \Delta_{\alpha w}|b_W\rangle\langle b_W| + (1-\Delta_{\alpha w})\rho_{\alpha bw,res} \tag{47}$$

for a state corresponding to bit value b in basis at side $\alpha = A$ or B. In our notation, as a subscript of Δ, the lower case w can be x or z if the basis W takes X or Z. Here, $\Delta_{\alpha w} = \cos^2\theta_{\alpha w}(1 - 2\tan\theta_{\alpha w})$. Both Alice and Bob have virtual ideal subsources which emit standard BB84 states. Therefore, a single-photon pair corresponding to bit values a and b at Alice's side and Bob's side in basis W correspond to a two-pulse state

$$\rho_a^{AW} \otimes \rho_b^{BW} = \Delta_w^{(2)}|a\rangle\langle a| \otimes |b\rangle\langle b| + \left(1-\Delta_w^{(2)}\right)\rho_{abw,res} \tag{48}$$

and

$$\Delta_w^{(2)} = \Delta_{Aw}\Delta_{Bw}, \tag{49}$$

where $\Delta_{\gamma w}$ is given by Eqs. (27) and (29) with z or x replaced by γw there. We define virtual two-pulse ideal subsources $\{W_{ab}\}$, a,b can be 0 or 1. If at a certain time states of both single-photon pulses are from ideal virtual subsources and are corresponding to bit values a,b in the basis W, we say the pulse pair is from source W_{ab}, which is a two-pulse ideal virtual subsource. If at a certain time the pulses from two sides are in the same basis W but not from any of the above virtual ideal subsources, we regard them as tagged states from the tagged source which produces states $\rho'_{W,res}$ only. Therefore, we can regard all single-photon pairs in the Z basis as coming from five different virtual sources: Z_{00}, Z_{11}, Z_{01}, Z_{10}, and Z'_{res}, which only emits two-pulse states $|0_Z0_Z\rangle$, $|1_Z1_Z\rangle$, $|0_Z1_Z\rangle$, $|1_Z0_Z\rangle$ and state $\rho'_{Z,res} = \frac{1}{4}\Sigma_{a,b}\rho_{abW,res}$. We can also regard the first four sources as one composite source $\tilde{Z}$, which emits single-photon pair state of density matrix $I/2$ in the 4×4 space only. We can then require that any single-photon pair in the Z basis comes out from source $\tilde{Z}$ with a probability $\Delta_z^{(2)}$, or from source Z'_{res} with a probability $1-\Delta_z^{(2)}$. We can find that the fraction of bits caused by source $\tilde{W}$ among all those post-selected bits in the W basis caused by single-photon pairs as

$$\tilde{\Delta}_w = \frac{\Delta_w^{(2)}}{2-\Delta_w^{(2)}}. \tag{50}$$

Observing the error rate of the X-basis pairs from the decoy source $E^X_{x_Ax_B}$, we can find the upper bound E_{11}^X, the error rate of those post-selected bits corresponding to single-photon pairs in the X basis by Eq. (17), and then the upper bound error rate of post-selected bits corresponding to single-photon pairs in X-basis bits caused by virtual source $\tilde{X}$ is

$$E_{11,\tilde{X}} \leqslant E_{11}^X/\tilde{\Delta}_x, \tag{51}$$

where E_{11}^X is the error rate for post-selected bits in the X basis caused by single-photon pairs, as given by Eq. (17). This is also the asymptotic phase-flip rate of bits corresponding to two single-photon pulses from source $\tilde{Z}$. We can then use the key rate formula of Eq. (37), with $\tilde{\Delta}_x$ and phase-flip rate given above. Finally, we have the following key rate formula for decoy-state MDIQKD with basis-dependent errors:

$$R = \tilde{\Delta}_z\Delta_{11}^Z[1 - H(E_{11,\tilde{X}})] - fH\left(E_{11}^Z\right) \tag{52}$$

and $\Delta_{11}^Z = \frac{a'_1b'_1s_{11}^Z}{S_{y_Ay_B}}$, a'_1,b'_1 are parameters appearing in the signal states ρ_{y_A},ρ_{y_B} as given by Eq. (1), s_{11}^Z is given by Eq. (16), E_{11}^Z is the observed error rate for all post-selected bits in the Z basis, and $S_{y_Ay_B}$ is the observed yield of two-pulse source y_Ay_B as defined in Sec. 1.

We must change the formula if we only implement the decoy-state method in the Z basis; in preparing X-basis bits, we only use source x_Ax_B. We need to derive the upper bound of $E_{11,\tilde{Z}}^{ph}$, the phase-flip rate of bits corresponding to single-photon pairs from source $\tilde{Z}$, which is equal to $E_{11,\tilde{X}}$. Note that now in general, $s_{11}^X \neq s_{11}^Z$, since the polarization states for the Z and X bases are *different*. But, the yields from the ideal sources $\tilde{X}$ and $\tilde{Z}$ must be equal. We have

$$s_{11,\tilde{X}} = s_{11,\tilde{Z}} \geqslant \tilde{\Delta}_z^{(2)}s_{11}^Z, \tag{53}$$

which immediately leads to

$$E_{11,\tilde{X}} \leqslant \frac{E_{11}^{X}}{\tilde{\Delta}_z^{(2)}\tilde{\Delta}_x^{(2)}}, \tag{54}$$

and $\tilde{E}_{11}^{X}$ is given by Eq. (17). With this, the key rate can be calculated by Eq. (52).

ACKNOWLEDGMENTS

We thank Professor J. W. Pan, Professor C. Z. Peng, and Professor Q. Zhang in USTC for useful discussions. This work was supported in part by the National High-Tech Program of China through Grants No. 2011AA010800 and No. 2011AA010803, NSFC through Grants No. 11174177 and No. 60725416, and 10000-Plan of Shandong province.

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

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002); N. Gisin and R. Thew, Nat. Photonics **1**, 165 (2006); M. Dusek, N. Lütkenhaus, and M. Hendrych, in *Progress in Optics VVVX*, edited by E. Wolf (Elsevier, Amsterdam, 2006); V. Scarani, H. Bechmann-Pasqunucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[3] H. Inamori, N. Lütkenhaus, and D. Mayers, Eur. Phys. J. D **41**, 599 (2007); D. Gottesman, H. K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).

[4] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[5] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005); Phys. Rev. A **72**, 012322 (2005).

[6] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005); X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).

[7] Y. Adachi, T. Yamamoto, M. Koashi, and N. Imoto, Phys. Rev. Lett. **99**, 180503 (2007); Q. Wang, X.-B. Wang, and G.-C. Guo, Phys. Rev. A **75**, 012312 (2007); Q. Wang, X.-B. Wang, G. Björk, and A. Karlsson, Euro. Phys. Lett. **79**, 40001 (2007).

[8] H. Jirari and W. Pötz, Phys. Rev. A **74**, 022306 (2006); M. Hayashi, *ibid.* **76**, 012329 (2007).

[9] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, Phys. Rev. Lett. **98**, 010503 (2007); T. Schmitt-Manderbach *et al.*, *ibid.* **98**, 010504 (2007); Cheng-Zhi Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, *ibid.* **98**, 010505 (2007); Z.-L. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **90**, 011118 (2007); Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, Phys. Rev. Lett. **96**, 070502 (2006); in *Proceedings of IEEE International Symposium on Information Theory, Seattle* (IEEE, New York, 2006), pp. 2094–2098; Q. Wang, W. Chen, G. Xavier, M. Swillo, T. Zhang, S. Sauge, M. Tengner, Z.-F. Han, G.-C. Guo, and A. Karlsson, Phys. Rev. Lett. **100**, 090501 (2008).

[10] X.-B. Wang, C.-Z. Peng, J. Zhang, L. Yang, and J.-W. Pan, Phys. Rev. A **77**, 042311 (2008); J.-Z. Hu and X.-B. Wang, *ibid.* **82**, 012331 (2010).

[11] X.-B. Wang, T. Hiroshima, A. Tomita, and M. Hayashi, Phys. Rep. **448**, 1 (2007).

[12] X.-B. Wang, L. Yang, C.-Z. Peng, and J.-W. Pan, New J. Phys. **11**, 075006 (2009).

[13] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000); N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000); N. Lütkenhaus and M. Jahma, New J. Phys. **4**, 44 (2002).

[14] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995); H. P. Yuen, Quantum Semiclassical Opt. **8**, 939 (1996).

[15] L. Lyderson *et al.*, Nat. Photonics **4**, 686 (2010); I. Gerhardt *et al.*, Nat. Commun. **2**, 349 (2011).

[16] D. Mayers and A. C.-C. Yao, in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS98)* (IEEE Computer Society, Washington, DC, 1998), p. 503; A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarini, Phys. Rev. Lett. **98**, 230501 (2007); V. Scarani and R. Renner, *ibid.* **100**, 200501 (2008); in *3rd Workshop on Theory of Quantum Computation, Communication and Cryptography (TQC 2008)* (University of Tokyo, Tokyo, 2008).

[17] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).

[18] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[19] K. Tamaki, H.-K. Lo, Chi-Hang Fred Fung, and B. Qi, Phys. Rev. A **85**, 042307 (2012); see also recent erratum *ibid.* **86**, 059903(E) (2012).