Three-intensity decoy-state method for measurement-device-independent quantum key distribution

Zong-Wen Yu,[1,2] Yi-Heng Zhou,[1] and Xiang-Bin Wang[1,3,4,*]

[1]*State Key Laboratory of Low Dimensional Quantum Physics, Tsinghua University, Beijing 100084, People's Republic of China*

[2]*Data Communication Science and Technology Research Institute, Beijing 100191, People's Republic of China*

[3]*Shandong Academy of Information and Communication Technology, Jinan 250101, People's Republic of China*

[4]*Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*

(Received 12 September 2013; published 30 December 2013)

We study the measurement-device-independent quantum key distribution (MDI-QKD) in practice with limited resources, when there are only three different states in implementing the decoy-state method. We present a tighter explicit formula to estimate the lower bound of the yield of two-single-photon pulses sent by Alice and Bob. Moreover, we show that the bounding of this yield and phase flip error of single-photon pulse pairs can be further improved by using other constraints which can be solved by a simple and explicit program. Our methods here can significantly improve the key rate and the secure distance of MDI-QKD with only three intensities.

DOI: 10.1103/PhysRevA.88.062339 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 under study in the recent years. The major problems here include the imperfection of the source 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].

Besides 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 cannot apply to the existing real setups because violation of Bell's inequality cannot be strictly demonstrated by existing setups.

Very recently, an idea of measurement-device-independent QKD (MDI-QKD) 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 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 postselect 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 other halves 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 postselected bits. However, in our existing technologies, high-quality entangled-pair-state generation cannot be done efficiently. In the most matured 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 implement the decoy-state method for security. This has been discussed in [18], and calculation formulas for the practical decoy-state implementation with only a few different states were first presented in [19] and then further studied both experimentally [20–22] and theoretically [23–27]. In particular, Tittel's group [20] did the MDI-QKD experiment with three intensities [19], in the laboratory over more than 80 km of spooled fiber, as well as across different locations within the city of Calgary. By developing up-conversion single-photon detectors with high efficiency and low noise, Liu *et al*. did it over a 50-km fiber link [22] and transmitted a 24192 image with one-time pad protocol. These pioneering experiments in Calgary [20] and in Shanghai [22] and also the proof of principle experiment [21] make a big step toward the final goal of real application because they clearly show the practical feasibility of MDI-QKD. Sun *et al*. [24] presented a variant formula of three-intensity MDI-QKD with numerical simulation. However, the earlier formula [19] actually behaves better than the Sun *et al*. result. Xu *et al*. [25] studied the more general case when each side uses three nonvacuum states. One can see that the major formula there [25] is identical with the one in [19] in the case when the weakest pulse is the vacuum. Wang and Wang [23] and Zhou *et al*. [26] studied the MDI-QKD with heralded single-photon sources. Curty *et al*. studied some finite-key effects [27]. Actually, using the idea clearly stated in Ref [12], one can straightly formulate the effects of statistical fluctuations in the decoy state MDI-QKD.

There are two directions for the future study of the MDI-QKD. One is to improve the experimental techniques, so as to improve the robustness and efficiency. The other is to upgrade the theoretical results so as to obtain a higher key rate given the same experimental data.

Here in this work, we shall first give better explicit formulas of the three-state decoy-state method for the MDI-QKD. We then estimate the infimum of yield and the supremum of error rate single-photon pulse pairs to the UTP with a simple and efficient program. In the fifth section, we present the numerical simulations. The article is ended with a concluding remark.

II. DECOY-STATE METHOD WITH ONLY THREE STATES FOR MDI-QKD

In the protocol, each time, a pulse pair (two-pulse state) is sent to the relay for detection. The relay is controlled by a UTP.

*xbwang@mail.tsinghua.edu.cn

The UTP will announce whether the pulse pair has caused a successful event. Those bits corresponding to successful events will be postselected 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

$$\rho_{x_A} = \sum_k a_k|k\rangle\langle k|, \quad \rho_{y_A} = \sum_k a'_k|k\rangle\langle k|, \tag{1}$$

$$\rho_{x_B} = \sum_k b_k|k\rangle\langle k|, \quad \rho_{y_B} = \sum_k b'_k|k\rangle\langle k|, \tag{2}$$

and we request the states satisfying the following very important condition:

$$\frac{a'_k}{a_k} \geqslant \frac{a'_2}{a_2} \geqslant \frac{a'_1}{a_1}, \quad \frac{b'_k}{b_k} \geqslant \frac{b'_2}{b_2} \geqslant \frac{b'_1}{b_1}, \tag{3}$$

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), and 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 at each time a two-pulse source is selected and 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 $\tilde{\alpha}\tilde{\beta}$ for the two-pulse source when the pulse pair is produced by source $\tilde{\alpha}$ at Alice's side and source $\tilde{\beta}$ at Bob's side; $\tilde{\alpha}$ can be one of $\{o_A,x_A,y_A\}$, and $\tilde{\beta}$ can be one of $\{o_B,x_B,y_B\}$. For example, at a certain time j when Alice uses source o_A and Bob uses source y_B, we say the pulse pair is emitted by source o_Ay_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 the 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 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 that have 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 $\tilde{\alpha}\tilde{\beta}$ as a set, the yield $S_{\tilde{\alpha}\tilde{\beta}}$ for source $\tilde{\alpha}\tilde{\beta}$ is $S_{\tilde{\alpha}\tilde{\beta}} = \frac{n_{\tilde{\alpha}\tilde{\beta}}}{N_{\tilde{\alpha}\tilde{\beta}}}$, where $n_{\tilde{\alpha}\tilde{\beta}}$ is the number of successful events that have happened corresponding to pulse pairs from source $\tilde{\alpha}\tilde{\beta}$ and $N_{\tilde{\alpha}\tilde{\beta}}$ is the number of times source $\tilde{\alpha}\tilde{\beta}$ 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 $n_{\tilde{\alpha}\tilde{\beta}}$ and $N_{\tilde{\alpha}\tilde{\beta}}$. We use capital letter $S_{\tilde{\alpha}\tilde{\beta}}$ 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 written in a convex form of different density operators. For example, two-pulse source y_Ay_B includes a subsource of pulse pairs of state $\rho_1 \otimes \rho_1$ ($\rho_1 = |1\rangle\langle 1|$) with weight $a'_1b'_1$. This is to say, after we have used source y_Ay_B for N times, we have actually used the subsource of state $\rho_1 \otimes \rho_1$ for $a'_1b'_1N$ times, asymptotically. Similarly, the source x_Ax_B also includes a subsource of state $\rho_1 \otimes \rho_1$ with weight a_1b_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, denoting 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

$$s = s' \tag{4}$$

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, and 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

$$\Omega_{\alpha\beta} = \rho_\alpha \otimes \rho_\beta \tag{5}$$

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 don't always know the value of yield of a state, because we don't know which subsource was used in each 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}, are 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. (4), if $\alpha \in \{0,x_A,y_A\}$ and $\beta \in \{0,x_B,y_B\}$, we have

$$s_{\alpha\beta} = S_{\tilde{\alpha}\tilde{\beta}} \tag{6}$$

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_Ay_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_Ay_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_Ay_B, and therefore the yield of any subsource of state $\rho_0 \otimes \rho_{y_B}$ must be just the yield of the real source o_Ay_B, which can be directly observed in the experiment. Mathematically, this is $s_{0y_B} = S_{o_Ay_B}$, 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 $y_A y_B$.

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 $\{S_{\tilde{\alpha}\tilde{\beta}}\}$. 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

$$S = \sum_{\alpha,\beta} c_{\alpha\beta} s_{\alpha\beta}. \tag{7}$$

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 subsets.

Consider the convex forms of source $x_A x_B$, $x_A y_B$, $y_A x_B$ and source $y_A y_B$. Without causing any ambiguity, we omit the subscripts A and B in the remainder of this paper. Explicitly,

$$\tilde{S}_{xx} = a_1 b_1 s_{11} + a_1 b_2 s_{12} + a_2 b_1 s_{21} + a_2 b_2 s_{22} + J_{xx}, \tag{8}$$

$$\tilde{S}_{xy} = a_1 b'_1 s_{11} + a_1 b'_2 s_{12} + a_2 b'_1 s_{21} + a_2 b'_2 s_{22} + J_{xy}, \tag{9}$$

$$\tilde{S}_{yx} = a'_1 b_1 s_{11} + a'_1 b_2 s_{12} + a'_2 b_1 s_{21} + a'_2 b_2 s_{22} + J_{yx}, \tag{10}$$

$$\tilde{S}_{yy} = a'_1 b'_1 s_{11} + a'_1 b'_2 s_{12} + a'_2 b'_1 s_{21} + a'_2 b'_2 s_{22} + J_{yy}, \tag{11}$$

where

$$\tilde{S}_{xx} = S_{xx} - a_0 S_{0x} - b_0 S_{x0} + a_0 b_0 S_{00}, \tag{12}$$

$$\tilde{S}_{xy} = S_{xy} - a_0 S_{0y} - b'_0 S_{x0} + a_0 b'_0 S_{00}, \tag{13}$$

$$\tilde{S}_{yx} = S_{yx} - a'_0 S_{0x} - b_0 S_{y0} + a'_0 b_0 S_{00}, \tag{14}$$

$$\tilde{S}_{yy} = S_{yy} - a'_0 S_{0y} - b'_0 S_{y0} + a'_0 b'_0 S_{00}, \tag{15}$$

and

$$J_{xx} = \sum_{(m,n)\in J_0} a_m b_n s_{mn}, \quad J_{xy} = \sum_{(m,n)\in J_0} a_m b'_n s_{mn},$$

$$J_{yx} = \sum_{(m,n)\in J_0} a'_m b_n s_{mn}, \quad J_{yy} = \sum_{(m,n)\in J_0} a'_m b'_n s_{mn},$$

with $J_0 = \{(m,n)|m \geqslant 1, n \geqslant 1, m+n \geqslant 4, (m,n) \neq (2,2)\}$.

In order to get a lower bound of s_{11}, we should derive the expression of s_{11} with Eqs. (8)–(11) first. Combining Eqs. (8)–(10), we obtain the expression of s_{11} by eliminating s_{12} and s_{21} such that

$$s_{11} = s_{11}^{(123)} + \sum_{(m,n)\in J_1} f_{11}^{(123)}(m,n) s_{mn}, \tag{16}$$

where $J_1 = \{(m,n)|m \geqslant 1, n \geqslant 1, m+n \geqslant 4\}$,

$$s_{11}^{(123)} = \frac{(a_1 a'_2 b_1 b'_2 - a'_1 a_2 b'_1 b_2)\tilde{S}_{xx} - b_1 b_2 (a_1 a'_2 - a'_1 a_2)\tilde{S}_{xy} - a_1 a_2 (b_1 b'_2 - b'_1 b_2)\tilde{S}_{yx}}{a_1 b_1 (a_1 a'_2 - a'_1 a_2)(b_1 b'_2 - b'_1 b_2)}, \tag{17}$$

and

$$f_{11}^{(123)}(m,n) = \frac{a_2 b_n (a_1 a'_m - a'_1 a_m)(b_1 b'_2 - b'_1 b_2) + a_m b_1 (a_1 a'_2 - a'_1 a_2)(b_2 b'_n - b'_2 b_n)}{a_1 b_1 (a_1 a'_2 - a'_1 a_2)(b_1 b'_2 - b'_1 b_2)}. \tag{18}$$

In these expressions, we use the superscript $*^{(123)}$ to denote the result obtained with the first three equations from Eqs. (8)–(11). Under the conditions presented in Eq. (3), we can easily find out that $(a_1 a'_2 - a'_1 a_2) \geqslant 0$, $(b_1 b'_2 - b'_1 b_2) \geqslant 0$, $(a_1 a'_m - a'_1 a_m) \geqslant 0$ for all $m \geqslant 1$ and $(b_2 b'_n - b'_2 b_n) \geqslant 0$ for all $n \geqslant 2$. Then we know that $f_{11}^{(123)}(m,n) \geqslant 0$ hold for all $(m,n) \in J_1$. With this fact, we obtain a lower bound from Eq. (16) by setting $s_{mn} = 0, (m,n) \in J_1$ such that

$$\underline{s_{11}} = s_{11}^{(123)} \leqslant s_{11}, \tag{19}$$

where $s_{11}^{(123)}$ is defined by Eq. (17). This and Eq. (17) are our major formulas for the decoy-state method implementation for MDI-QKD in this section.

Similarly, we can get other expressions by choosing any other three equations from Eqs. (8)–(11). For example, we choose Eqs. (8), (9), and (11). By eliminating s_{12} and s_{21}, we get another expression of s_{11} such that

$$s_{11} = s_{11}^{(124)} + \sum_{(m,n)\in J_1} f_{11}^{(124)}(m,n) s_{mn}, \tag{20}$$

where

$$s_{11}^{(124)} = \frac{b'_1 b'_2 (a_1 a'_2 - a'_1 a_2)\tilde{S}_{xx} + (a'_1 a_2 b_1 b'_2 - a_1 a'_2 b'_1 b_2)\tilde{S}_{xy} - a_1 a_2 (b_1 b'_2 - b'_1 b_2)\tilde{S}_{yy}}{a_1 b'_1 (a_1 a'_2 - a'_1 a_2)(b_1 b'_2 - b'_1 b_2)} \tag{21}$$

and

$$f_{11}^{(124)}(m,n) = \frac{a_2 b'_n (a_1 a'_m - a'_1 a_m)(b_1 b'_2 - b'_1 b_2) + a_m b'_1 (a_1 a'_2 - a'_1 a_2)(b_2 b'_n - b'_2 b_n)}{a_1 b'_1 (a_1 a'_2 - a'_1 a_2)(b_1 b'_2 - b'_1 b_2)}. \tag{22}$$

Under the conditions presented in Eq. (3), we can also find out that $f_{11}^{(124)}(m,n) \geqslant 0$ for all $(m,n) \in J_1$. Then we know that $s_{11}^{(124)}$ is also a lower bound of s_{11}. On the other hand, by comparing $f_{11}^{(123)}(m,n)$ and $f_{11}^{(124)}(m,n)$, we have

$$f_{11}^{(123)}(m,n) - f_{11}^{(124)}(m,n) = -\frac{a_2(a_1a'_m - a'_1a_m)(b_1b'_n - b'_1b_n)}{a_1b_1b'_1(a_1a'_2 - a'_1a_2)} \leqslant 0, \quad (23)$$

for any $(m,n) \in J_1$. Then we know that

$$s_{11}^{(123)} \geqslant s_{11}^{(124)}, \quad (24)$$

with Eqs. (16) and (20). With the relation presented in Eq. (24) we know that the lower bound $s_{11}^{(123)}$ is tighter than the lower bound $s_{11}^{(124)}$. In the same way, we can get another two lower bounds $s_{11}^{(134)}$ and $s_{11}^{(234)}$ of s_{11} with Eqs. (8), (10), and (11) and Eqs. (9)–(11), respectively. Furthermore, we can also prove that

$$s_{11}^{(123)} \geqslant s_{11}^{(134)}, \quad s_{11}^{(123)} \geqslant s_{11}^{(234)}. \quad (25)$$

Now we only consider Eqs. (8) and (11). By eliminating s_{12} or s_{21}, respectively, we get two expressions of s_{11} such that

$$s_{11} = s_{11}^{(14a)} + \sum_{(m,n)\in J_2} f_{11}^{(14a)}(m,n)s_{mn}, \quad (26)$$

$$s_{11} = s_{11}^{(14b)} + \sum_{(m,n)\in J_2} f_{11}^{(14a)}(m,n)s_{mn}, \quad (27)$$

where $J_2 = \{(m,n)|m \geqslant 1, n \geqslant 1, m+n \geqslant 3\}$,

$$s_{11}^{(14a)} = \frac{a'_1b'_2\tilde{S}_{xx} - a_1b_2\tilde{S}_{yy}}{a_1a'_1(b_1b'_2 - b'_1b_2)}, \quad (28)$$

$$s_{11}^{(14b)} = \frac{a'_2b'_1\tilde{S}_{xx} - a_2b_1\tilde{S}_{yy}}{b_1b'_1(a_1a'_2 - a'_1a_2)}, \quad (29)$$

and

$$f_{11}^{(14a)}(m,n) = \frac{a_1b_2a'_mb'_n - a'_1b'_2a_mb_n}{a_1a'_1(b_1b'_2 - b'_1b_2)}, \quad (30)$$

$$f_{11}^{(14b)}(m,n) = \frac{a_2b_1a'_mb'_n - a'_2b'_1a_mb_n}{b_1b'_1(a_1a'_2 - a'_1a_2)}. \quad (31)$$

For any sources used in the protocol, we must have either $K_a = \frac{a'_1b'_2}{a_1b_2} \leqslant \frac{a'_2b'_1}{a_2b_1} = K_b$ or $K_a \geqslant K_b$. Supposing the former one holds, we can easily find out that $f_{11}^{(14a)}(m,n) \geqslant 0$ for all $(m,n) \in J_2$ and $s_{11}^{(14a)}$ is a lower bound of s_{11}. On the other hand, if $K_a \geqslant K_b$ holds, we have $f_{11}^{(14b)}(m,n) \geqslant 0$ for all $(m,n) \in J_2$ and $s_{11}^{(14b)}$ is a lower bound of s_{11}. Considering the following two relations,

$$K_a - K_b = \frac{a'_1a_2b_1b'_2 - a_1a'_2b'_1b_2}{a_1a_2b_1b_2} \quad (32)$$

and

$$f_{11}^{(14a)}(m,n) - f_{11}^{(14b)}(m,n) = \frac{(a_1a'_mb_1b'_n - a'_1a_mb'_1b_n)(a'_1a_2b_1b'_2 - a_1a'_2b'_1b_2)}{a_1a'_1b_1b'_1(a_1a'_2 - a'_1a_2)(b_1b'_2 - b'_1b_2)}, \quad (33)$$

we know that $K_a - K_b$ and $f_{11}^{(14a)} - f_{11}^{(14b)}$ have the same sign, which means that they are both positive or negative simultaneously. Then we can write the lower bound of s_{11} with Eqs. (8) and (11) into the following compact form:

$$s_{11}^{(14)} = \min\left\{s_{11}^{(14a)}, s_{11}^{(14b)}\right\}, \quad (34)$$

that is the result presented in [19]. In the following, we will prove that the lower bound $s_{11}^{(123)}$ given in Eq. (17) is more tight than $s_{11}^{(14)}$. First, if we suppose $K_a \leqslant K_b$ holds, then we know that $a'_1a_2b_1b'_2 \leqslant a_1a'_2b'_1b_2$ and $s_{11}^{(14)} = s_{11}^{(14a)}$. For any $(m,n) \in J_1$ we have

$$f_{11}^{(123)}(m,n) - f_{11}^{(14a)}(m,n) = -\frac{(a_1a'_m - a'_1a_m)D_a}{a_1a'_1b_1(a_1a'_2 - a'_1a_2)(b_1b'_2 - b'_1b_2)}, \quad (35)$$

where $D_a = (a_1a'_2b_1b_2b'_n + a'_1a_2b'_1b_2b_n - a'_1a_2b_1b'_2b_n - a'_1a_2b_1b_2b'_n) \geqslant b_2(a_1a'_2 - a'_1a_2)(b_1b'_n - b'_1b_n)$. Then we know that

$$f_{11}^{(123)}(m,n) - f_{11}^{(14a)}(m,n) \leqslant -\frac{b_2(a_1a'_m - a'_1a_m)(b_1b'_n - b'_1b_n)}{a_1a'_1b_1(b_1b'_2 - b'_1b_2)} \leqslant 0. \quad (36)$$

We can easily know that $s_{11}^{(123)} \geqslant s_{11}^{(14)}$ when $K_a \leqslant K_b$ with this equation. Second, if we suppose $K_a \geqslant K_b$ holds, we can easily prove that $f_{11}^{(123)}(m,n) - f_{11}^{(14b)}(m,n) \leqslant 0$ for all $(m,n) \in J_1$ within the same way. Then we get $s_{11}^{(123)} \geqslant s_{11}^{(14)}$ when $K_a \geqslant K_b$.

In the last part of this section, we will derive another lower bound of s_{11} with Eqs. (8)–(11). The idea presented in [19,24] inspires us to do the following deduction:

$$\begin{aligned}
\tilde{S}_{yy} - \tilde{S}_{xx} &= (a'_1b'_1 - a_1b_1)s_{11} + \sum_{n\geqslant 2}(a'_1b'_n - a_1b_n)s_{1n} + \sum_{m\geqslant 2}(a'_mb'_1 - a_mb_1)s_{m1} + \sum_{m,n\geqslant 2}(a'_mb'_n - a_mb_n)s_{mn} \\
&\geqslant (a'_1b'_1 - a_1b_1)s_{11} + A\sum_{n\geqslant 2}(a'_1b_n + a_1b'_n)s_{1n} + B\sum_{m\geqslant 2}(a'_mb_1 + a_mb'_1)s_{m1} + C\sum_{m,n\geqslant 2}(a'_mb_n + a_mb'_n)s_{mn} \\
&\geqslant (a'_1b'_1 - a_1b_1)s_{11} + \alpha\left[\sum_{n\geqslant 2}(a'_1b_n + a_1b'_n)s_{1n} + \sum_{m\geqslant 2}(a'_mb_1 + a_mb'_1)s_{m1} + \sum_{m,n\geqslant 2}(a'_mb_n + a_mb'_n)s_{mn}\right]
\end{aligned}$$

$$= (a_1'b_1' - a_1b_1)s_{11} + \alpha(\tilde{S}_{xy} - a_1b_1's_{11} + \tilde{S}_{yx} - a_1'b_1s_{11})$$
$$= [a_1'b_1' - a_1b_1 - \alpha(a_1b_1' + a_1'b_1)]s_{11} + \alpha(\tilde{S}_{xy} + \tilde{S}_{yx}), \quad (37)$$

where we have used the condition presented in Eq. (3), and $\alpha = \min\{A,B,C\}$ with

$$A = \frac{a_1'b_2' - a_1b_2}{a_1'b_2 + a_1b_2'}, \quad B = \frac{a_2'b_1' - a_2b_1}{a_2'b_1 + a_2b_1'}, \quad C = \frac{a_2'b_2' - a_2b_2}{a_2'b_2 + a_2b_2'}.$$

Actually, under the condition in Eq. (3), we know that

$$A - C = -\frac{(b_2^2 + b_2'^2)(a_1a_2' - a_1'a_2)}{(a_1'b_2 + a_1b_2')(a_2'b_2 + a_2b_2')} \leqslant 0,$$
$$B - C = -\frac{(a_2^2 + a_2'^2)(b_1b_2' - b_1'b_2)}{(a_2'b_1 + a_2b_1')(a_2'b_2 + a_2b_2')} \leqslant 0.$$

Then α can be written as $\alpha = \min\{A,B\}$. According to the relation presented in Eq. (37), we obtain the other expression of s_{11}:

$$s_{11} = s_{11}^{(\alpha)} + \sum_{(m,n)\in J_2} f_{11}^{(\alpha)}(m,n)s_{mn}, \quad (38)$$

where

$$s_{11}^{(\alpha)} = \frac{\tilde{S}_{xx} - \tilde{S}_{yy} + \alpha(\tilde{S}_{xy} + \tilde{S}_{yx})}{a_1b_1 - a_1'b_1' + \alpha(a_1b_1' + a_1'b_1)}, \quad (39)$$

and

$$f_{11}^{(\alpha)}(m,n) = -\frac{a_mb_n - a_m'a_n' + \alpha(a_mb_n' + a_m'b_n)}{a_1b_1 - a_1'b_1' + \alpha(a_1b_1' + a_1'b_1)}. \quad (40)$$

With the condition presented in Eq. (3), we can easily prove that $f_{11}^{(\alpha)}(m,n) \geqslant 0$ for all $(m,n) \in J_2$. So we know that $s_{11}^{(\alpha)}$ is the other lower bound of s_{11}. In the coming, we will discuss the relation among $s_{11}^{(\alpha)}$, $s_{11}^{(14)}$, and $s_{11}^{(123)}$.

First, we consider the special case with $a_k = b_k$ and $a_k' = b_k'$ for any $k \geqslant 1$. In this case, we have $K_a = K_b = \frac{a_1'a_2'}{a_1a_2}$, $A = B = \frac{a_1'a_2' - a_1a_2}{a_1'a_2 + a_1a_2'}$, and

$$f_{11}^{(\alpha)}(m,n) - f_{11}^{(14)}(m,n) = \frac{(a_1'a_2' - a_1a_2)(a_1a_m' - a_1'a_m)(a_1a_n' - a_1'a_n)}{a_1a_1'(a_1^2 + a_1'^2)(a_1a_2' - a_1'a_2)} \geqslant 0,$$

for any $(m,n) \in J_2$. Then we know that $s_{11}^{(14)} \geqslant s_{11}^{(\alpha)}$ in this case.

Second, for the general case, we can prove that

$$s_{11}^{(123)} \geqslant s_{11}^{(\alpha)}. \quad (41)$$

In the situation with $A \leqslant B$, we have

$$A - B = \frac{D_{A_1} - D_{A_2}}{(a_1'b_2 + a_1b_2')(a_2'b_1 + a_2b_1')} \leqslant 0,$$

where $D_{A_1} = a_1'a_2b_1b_2 - a_1a_2'b_1b_2 - a_1a_2b_1'b_2 + a_1a_2b_1b_2' + a_1'a_2'b_1b_2'$, and $D_{A_2} = a_1'a_2'b_1'b_2 - a_1'a_2b_1'b_2' + a_1a_2'b_1'b_2'$. With this condition, we can do the following calculation:

$$f_{11}^{(\alpha=A)}(m,n) - f_{11}^{(123)}(m,n)$$
$$= -\frac{(a_1a_m' - a_1'a_m)(a_1b_nD_{A_1} + D_{A_3})}{a_1b_1(a_1^2 + a_1'^2)(a_1a_2' - a_1'a_2)(b_1b_2' - b_1'b_2)}$$
$$\geqslant -\frac{(a_1a_m' - a_1'a_m)(a_1b_nD_{A_2} + D_{A_3})}{a_1b_1(a_1^2 + a_1'^2)(a_1a_2' - a_1'a_2)(b_1b_2' - b_1'b_2)}$$
$$= \frac{(a_1b_2' + a_1'b_2)(a_1a_m' - a_1'a_m)(b_1b_n' - b_1'b_n)}{a_1b_1(a_1^2 + a_1'^2)(b_1b_2' - b_1'b_2)}$$
$$\geqslant 0. \quad (42)$$

On the other hand, in the situation with $A \geqslant B$, we have

$$A - B = \frac{D_{B_1} - D_{B_2}}{(a_1'b_2 + a_1b_2')(a_2'b_1 + a_2b_1')} \geqslant 0,$$

where $D_{B_1} = a_1'a_2b_1b_2 - a_1a_2'b_1b_2 - a_1a_2b_1'b_2 + a_1a_2b_1b_2' - a_1a_2'b_1'b_2'$, and $D_{A_2} = a_1'a_2'b_1'b_2 - a_1'a_2'b_1b_2' - a_1'a_2b_1'b_2'$. With this condition, we can do the following calculation:

$$f_{11}^{(\alpha=B)}(m,n) - f_{11}^{(123)}(m,n)$$
$$= \frac{(b_1b_n' - b_1'b_n)(b_1a_mD_{B_1} + D_{B_3})}{a_1b_1(b_1^2 + b_1'^2)(a_1a_2' - a_1'a_2)(b_1b_2' - b_1'b_2)}$$
$$\geqslant \frac{(b_1b_n' - b_1'b_n)(b_1a_mD_{B_2} + D_{B_3})}{a_1b_1(b_1^2 + b_1'^2)(a_1a_2' - a_1'a_2)(b_1b_2' - b_1'b_2)}$$
$$= \frac{(a_2b_1' + a_2'b_1)(a_1a_m' - a_1'a_m)(b_1b_n' - b_1'b_n)}{a_1b_1(b_1^2 + b_1'^2)(a_1a_2' - a_1'a_2)}$$
$$\geqslant 0. \quad (43)$$

Summing up the results presented in Eqs. (42) and (43), we complete the proof of Eq. (41).

In order to estimate the final key rate, we also need the upper bound of error rate caused by the two single-photon pulses, say e_{11}. Similar to the total gain, the total error rate with source $\alpha\beta$ chosen by Alice and Bob can be written as [18]

$$\tilde{T}_{xx} = a_1b_1t_{11} + a_1b_2t_{12} + a_2b_1t_{21} + a_2b_2t_{22} + K_{xx}, \quad (44)$$

$$\tilde{T}_{xy} = a_1b_1't_{11} + a_1b_2't_{12} + a_2b_1't_{21} + a_2b_2't_{22} + K_{xy}, \quad (45)$$

$$\tilde{T}_{yx} = a_1'b_1t_{11} + a_1'b_2t_{12} + a_2'b_1t_{21} + a_2'b_2t_{22} + K_{yx}, \quad (46)$$

$$\tilde{T}_{yy} = a_1'b_1't_{11} + a_1'b_2't_{12} + a_2'b_1't_{21} + a_2'b_2't_{22} + K_{yy}, \quad (47)$$

where $T_{\alpha\beta} = E_{\alpha\beta}S_{\alpha\beta}$, $t_{mn} = s_{mn}e_{mn}$,

$$\tilde{T}_{xx} = T_{xx} - a_0T_{0x} - b_0T_{x0} + a_0b_0T_{00}, \quad (48)$$

$$\tilde{T}_{xy} = T_{xy} - a_0T_{0y} - b_0'T_{x0} + a_0b_0'T_{00}, \quad (49)$$

$$\tilde{T}_{yx} = T_{yx} - a_0' T_{0x} - b_0 T_{y0} + a_0' b_0 T_{00}, \quad (50)$$

$$\tilde{T}_{yy} = T_{yy} - a_0' T_{0y} - b_0' T_{y0} + a_0' b_0' T_{00}, \quad (51)$$

and

$$K_{xx} = \sum_{(m,n)\in J_0} a_m b_n t_{mn}, \quad K_{xy} = \sum_{(m,n)\in J_0} a_m b_n' t_{mn},$$

$$K_{yx} = \sum_{(m,n)\in J_0} a_m' b_n t_{mn}, \quad K_{yy} = \sum_{(m,n)\in J_0} a_m' b_n' t_{mn},$$

with $J_0 = \{(m,n)|m \geqslant 1, n \geqslant 1, m+n \geqslant 4, (m,n) \neq (2,2)\}$. According to Eq. (44), we can find out the upper bound of e_{11} such that

$$e_{11} \leqslant e_{11}^{(1)} = \frac{\tilde{T}_{xx}}{a_1 b_1 s_{11}} = \overline{e_{11}}. \quad (52)$$

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 postselected bits caused by source $x_A x_B$ in the Z basis. After an error test, we know the bit-flip error rate of this set, say $T_{x_A x_B}^Z = E_{x_A x_B}^Z S_{x_A x_B}^Z$. We also need the phase-flip rate for the subset of bits which are caused by the two single-photon pulse, say e_{11}^{ph}, which is equal to the flip rate of postselected bits caused by a single photon in the X basis, say e_{11}^X. Given this, we can now calculate the key rate by the well-known formula. For example, for those postselected bits caused by source $y_A y_B$, it is

$$R = a_1' b_1' s_{11}^Z \left[1 - H\left(e_{11}^X\right)\right] - S_{y_A y_B}^Z f H\left(E_{y_A y_B}^Z\right), \quad (53)$$

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

III. EXACT MINIMUM OF YIELD WITH ONLY THREE STATES FOR MDI-QKD

In the previous section, we show the lower bound of yield s_{11} and the upper bound of error rate e_{11} with explicit formulas. The lower bound $s_{11}^{(123)}$ is obtained with Eqs. (8)–(10) by setting $s_{mn} = 0$, where $(m,n) \in J_1$. The upper bound of $e_{11}^{(1)}$ is obtained with Eq. (44) by setting $e_{mn} = 0$, where $(m,n) \in J_2$. Obviously, the relation with source $y_A y_B$ is not used in deriving $s_{11}^{(123)}$ and $e_{11}^{(1)}$. Keeping sight of this fact, we suspect that a tighter bound can be found out considering all relations given by Eqs. (8)–(11) [or Eqs. (44)–(47)]. In the rest of this section, we will present an explicit algorithm within a finite number of steps to get an exact minimum of yield s_{11}. An exact maximum of error rate e_{11} will be given in the next section.

According to Eqs. (8)–(11), we can find out the expression of s_{11}, s_{12}, s_{21}, and s_{22} uniquely:

$$s_{11} = s_{11}^{(1234)} + \sum_{(m,n)\in J_0} f_{11}^{(1234)}(m,n) s_{mn}, \quad (54)$$

$$s_{12} = s_{12}^{(1234)} + \sum_{(m,n)\in J_0} f_{12}^{(1234)}(m,n) s_{mn}, \quad (55)$$

$$s_{21} = s_{21}^{(1234)} + \sum_{(m,n)\in J_0} f_{21}^{(1234)}(m,n) s_{mn}, \quad (56)$$

$$s_{22} = s_{22}^{(1234)} + \sum_{(m,n)\in J_0} f_{22}^{(1234)}(m,n) s_{mn}, \quad (57)$$

where

$$s_{11}^{(1234)} = \frac{a_2' b_2' \tilde{S}_{xx} - a_2' b_2 \tilde{S}_{xy} - a_2 b_2' \tilde{S}_{yx} + a_2 b_2 \tilde{S}_{yy}}{(a_1 a_2' - a_1' a_2)(b_1 b_2' - b_1' b_2)},$$

$$s_{12}^{(1234)} = \frac{-a_2' b_1' \tilde{S}_{xx} + a_2' b_1 \tilde{S}_{xy} + a_2 b_1' \tilde{S}_{yx} - a_2 b_1 \tilde{S}_{yy}}{(a_1 a_2' - a_1' a_2)(b_1 b_2' - b_1' b_2)},$$

$$s_{21}^{(1234)} = \frac{-a_1' b_2' \tilde{S}_{xx} + a_1' b_2 \tilde{S}_{xy} + a_1 b_2' \tilde{S}_{yx} - a_1 b_2 \tilde{S}_{yy}}{(a_1 a_2' - a_1' a_2)(b_1 b_2' - b_1' b_2)},$$

$$s_{22}^{(1234)} = \frac{a_1' b_1' \tilde{S}_{xx} - a_1' b_1 \tilde{S}_{xy} - a_1 b_1' \tilde{S}_{yx} + a_1 b_1 \tilde{S}_{yy}}{(a_1 a_2' - a_1' a_2)(b_1 b_2' - b_1' b_2)},$$

and

$$f_{11}^{(1234)}(m,n) = -\frac{(a_2 a_m' - a_2' a_m)(b_2 b_n' - b_2' b_n)}{(a_1 a_2' - a_1' a_2)(b_1 b_2' - b_1' b_2)}, \quad (58)$$

$$f_{12}^{(1234)}(m,n) = -\frac{(a_2 a_m' - a_2' a_m)(b_1 b_n' - b_1' b_n)}{(a_1 a_2' - a_1' a_2)(b_1 b_2' - b_1' b_2)}, \quad (59)$$

$$f_{21}^{(1234)}(m,n) = -\frac{(a_1 a_m' - a_1' a_m)(b_2 b_n' - b_2' b_n)}{(a_1 a_2' - a_1' a_2)(b_1 b_2' - b_1' b_2)}, \quad (60)$$

$$f_{22}^{(1234)}(m,n) = -\frac{(a_1 a_m' - a_1' a_m)(b_1 b_n' - b_1' b_n)}{(a_1 a_2' - a_1' a_2)(b_1 b_2' - b_1' b_2)}. \quad (61)$$

In the following, we denote the superscript (1234) by $(*)$ for short.

In order to estimate the lower bound of s_{11}, we need to present some properties about the functions $f_{11}^{(*)}(m,n), f_{12}^{(*)}(m,n), f_{21}^{(*)}(m,n), f_{22}^{(*)}(m,n)$. With the condition given by Eq. (3), we know that $f_{11}^{(*)}(2,k) = f_{11}^{(*)}(k,2) = 0$ for all $k \geqslant 3$, $f_{11}^{(*)}(1,k) \geqslant 0, f_{11}^{(*)}(k,1) \geqslant 0$ for all $k \geqslant 3$, and $f_{11}^{(*)}(m,n) \leqslant 0$ for all $m,n \geqslant 3$. Similarly, we know that $f_{12}^{(*)}(1,k) \leqslant 0$, $f_{12}^{(*)}(k,1) = f_{12}^{(*)}(2,k) = 0$, $f_{12}^{(*)}(k,2) \geqslant 0$, $f_{12}^{(*)}(m,n) \geqslant 0$, $f_{21}^{(*)}(k,1) \leqslant 0$, $f_{21}^{(*)}(1,k) = f_{21}^{(*)}(k,2) = 0$, $f_{21}^{(*)}(2,k) \geqslant 0$, $f_{21}^{(*)}(m,n) \geqslant 0$, $f_{22}^{(*)}(1,k) = f_{22}^{(*)}(k,1) = 0$ for all $k,m,n \geqslant 3$, and $f_{22}^{(*)}(m,n) \leqslant 0$ for all $m,n \geqslant 2$. With these facts, we can find out a lower bound of s_{11} by setting $s_{1k} = s_{k1} = 0, (k \geqslant 3)$ and $s_{mn} = 1, (m,n \geqslant 3)$ crudely. Actually, all $s_{mn}(m,n \geqslant 3)$ do not have to equal to 1 at the same time as the constraint conditions such that $s_{12}, s_{21}, s_{22} \in [0,1]$. Thus, the problem of estimating the lower bound of s_{11} can be written into the following constrained optimization problem (COP):

$$\begin{aligned} \min: s_{11} &= s_{11}^{(*)} + \sum_{(m,n)\in J_3} f_{11}^{(*)}(m,n) s_{mn} \\ \mathrm{st}: s_{22} &= s_{22}^{(*)} + \sum_{(m,n)\in J_3} f_{22}^{(*)}(m,n) s_{mn} \geqslant 0, \end{aligned} \quad (62)$$

where $J_3 = \{(m,n)|m \geqslant 2, n \geqslant 2, (m,n) \neq (2,2)\}$. In this COP, there is an infinite number of variables. If $s_{22}^{(*)} + \sum_{(m,n)\in J_3} f_{22}^{(*)} \geqslant 0$, the problem can be solved by taking $s_{mn} = 1$ for all $(m,n) \in J_3$, but in practice this trivial situation never or almost never occurs.

Generally, we cannot solve this COP analytically. In what follows we will show that the problem can be solved by an explicit algorithm. Still, as shown below, it can always be determined within a finite number of steps.

A. Definition of the lower bound

In order to solve this COP presented in Eq. (62), we need to analyze the ratio

$$h_{11}^{(22)}(m,n) = \frac{f_{11}^{(*)}(m,n)}{f_{22}^{(*)}(m,n)} = h_a(m)h_b(n), \tag{63}$$

where

$$h_a(m) = \frac{a_2 a'_m - a'_2 a_m}{a_1 a'_m - a'_1 a_m}, \quad h_b(n) = \frac{b_2 b'_n - b'_2 b_n}{b_1 b'_n - b'_1 b_n}. \tag{64}$$

Under the condition in Eq. (3), we can easily prove that $h_a(k),h_b(k)$ are two non-negative monotone increasing functions of variable $k \geqslant 3$. This fact tells us that $s_{m+1,n}$ and $s_{m,n+1}$ have priority to be equal to 1 over s_{mn} in order to minimize s_{11} in Eq. (62). Back to the COP, we can solve it by introducing the three subsets $J_L, J_s = \{(m_s,n_s)\}, J_U$ of J_3, and one positive real number $s_L \in (0,1]$ such that

$$\begin{aligned} h_{11}^{(22)}((m,n) \in J_L) &\leqslant h_{11}^{(22)}(m_s,n_s) \\ &\leqslant h_{11}^{(22)}((m,n) \in J_U), \end{aligned} \tag{65}$$

with $J_3 = J_L \cup J_s \cup J_U$ and

$$s_{22}^{(*)} + \sum_{(m,n)\in J_U} f_{22}^{(*)}(m,n) > 0, \tag{66}$$

$$s_{22}^{(*)} + \sum_{(m,n)\in J_U \cup J_s} f_{22}^{(*)}(m,n) \leqslant 0, \tag{67}$$

$$s_{22}^{(*)} + \sum_{(m,n)\in J_U} f_{22}^{(*)}(m,n) + s_L f_{22}^{(*)}(m_s,n_s) = 0. \tag{68}$$

Then we can define the lower bound of s_{11} by

$$\underline{s_{11}^*} = s_{11}^{(*)} + \sum_{(m,n)\in J_U} f_{11}^{(*)}(m,n) + s_L f_{11}^{(*)}(m_s,n_s). \tag{69}$$

With the definitions of J_L, J_s, J_U given by Eqs. (65)–(68), we know that the set J_3 is decomposed into three subsets J_L, J_s, J_U. It is important to point out that the subsets J_L, J_s, J_U need not be unique but the lower bound $\underline{s_{11}^*}$ given by Eq. (69) is always uniquely determined. If the subsets J_L, J_s, J_U have two different choices which are denoted by $J_{L_1}, J_{s_1}, J_{U_1}$ and $J_{L_1}, J_{s_1}, J_{U_1}$, then we must have

$$\begin{aligned} h_{11}^{(22)}\big((m,n) \in J_{L_{12}}\big) &= h_{11}^{(22)}\big(m_{s_1},n_{s_1}\big) \\ &= h_{11}^{(22)}\big(m_{s_2},n_{s_2}\big) = h_{11}^{(22)}\big((m,n) \in J_{U_{12}}\big), \end{aligned} \tag{70}$$

and the numbers of elements in the two sets J_{L_1}, J_{L_2} are the same, and the number of elements in the two sets J_{U_1}, J_{U_2} are also the same. In Eq. (70), $J_{L_{12}} = (J_{L_1} - J_{L_2}) \cup (J_{L_2} - J_{L_1})$ contains the elements that are only included in J_{L_1} or only in J_{L_2}, and $J_{U_{12}} = (J_{U_1} - J_{U_2}) \cup (J_{U_2} - J_{U_1})$ contains the elements that are only included in J_{U_1} or only in J_{U_2}. Here and after in this article, we use $A - B$ to denote the set which contains the elements in A but not in B. Thus, we get $s_{L_1} = s_{L_2}$ and

$$\begin{aligned} &\sum_{(m,n)\in J_{U_1}} f_{11}^{(*)}(m,n) + s_{L_1} f_{11}^{(*)}\big(m_{s_1},n_{s_1}\big) \\ &= \sum_{(m,n)\in J_{U_2}} f_{11}^{(*)}(m,n) + s_{L_2} f_{11}^{(*)}\big(m_{s_1},n_{s_1}\big). \end{aligned} \tag{71}$$

With this fact, we can conclude that the lower bound $\underline{s_{11}^*}$ given by Eq. (69) is unique.

B. An algorithm for finding J_L, J_s, J_U, and s_L

In order to confirm the value of $\underline{s_{11}^*}$, we need to determine the elements in sets J_L, J_s, J_U and the proper value of s_L. In the following, we will present an algorithm for finding it within finite steps.

We know that $h_{11}^{(22)}(m+1,n) \geqslant h_{11}^{(22)}(m,n)$ and $h_{11}^{(22)}(m,n+1) \geqslant h_{11}^{(22)}(m,n)$ for any $(m,n) \in J_3$. But we cannot pick the larger one between $h_{11}^{(22)}(m+1,n)$ and $h_{11}^{(22)}(m,n+1)$ unless we preset the sources used by Alice and Bob. Fortunately, this defect does not affect our derivation of the algorithm within finite steps.

In order to describe the algorithm clearly, we need to do the following preparations. First, we define two limits:

$$\hat{h}_a = \lim_{m\to\infty} h_a(m), \quad \hat{h}_b = \lim_{n\to\infty} h_b(n), \tag{72}$$

where $h_a(m)$ and $h_b(n)$ are defined in Eq. (64). As discussed before, we know that $h_a(k),h_b(k)$ are two non-negative monotone increasing functions of $k \geqslant 3$. Furthermore, under the condition in Eq. (3), we can also prove that $h_a(a'_m,a_m)$ is monotone increasing about $a'_m \in [0,1]$ and monotone decreasing about $a_m \in [0,1]$. Then we can find out a upper bound of the function h_a such that $h_a(a'_m,a_m) \leqslant a_2/a_1$. By the same method, we also have $h_b(b'_n,b_n) \leqslant b_2/b_1$. The function $h_a(k)$ is a non-negative monotone increasing function with finite upper bound, which means that limitations of it must exist. The same is true for $h_b(k)$. This completes the proof of Eq. (72). Explicitly, if Alice and Bob send out coherent pulses, we have $\hat{h}_a = (a'_2 - a_2)/(a'_1 - a_1), \hat{h}_b = (b'_2 - b_2)/(b'_1 - b_1)$. Second, we also need the notations

$$F_c(m_0,n_0) = \sum_{m\geqslant m_0} f_{22}^{(*)}(m,n_0), \tag{73}$$

$$F_r(m_0,n_0) = \sum_{n\geqslant n_0} f_{22}^{(*)}(m_0,n). \tag{74}$$

Considering the normalizing conditions

$$\sum_{k\geqslant 0} x_k = 1, \quad (x = a,b,a',b'), \tag{75}$$

we can calculate $F_c(m_0,n_0), F_r(m_0,n_0)$ by the following explicit formulas:

$$F_c(m_0,n_0) = -\frac{\big(a_1 \bar{a}'_{m_0} - a'_1 \bar{a}_{m_0}\big)\big(b_1 b'_{n_0} - b'_1 b_{n_0}\big)}{(a_1 a'_2 - a'_1 a_2)(b_1 b'_2 - b'_1 b_2)}, \tag{76}$$

$$F_r(m_0,n_0) = -\frac{\big(a_1 a'_{m_0} - a'_1 a_{m_0}\big)\big(b_1 \bar{b}'_{n_0} - b'_1 \bar{b}_{n_0}\big)}{(a_1 a'_2 - a'_1 a_2)(b_1 b'_2 - b'_1 b_2)}, \tag{77}$$

where $\bar{x}_{k_0} = 1 - \sum_{k=0}^{k_0-1} x_k, (x = a,b,a',b')$.

Furthermore, for given J_L, J_s, and J_U we introduce a vector V_s with l_s elements and two natural number m_J, n_J such that

$$m_J = \min_{(m,n)\in J_U} m, \quad n_J = \min_{(m,n)\in J_U} n. \tag{78}$$

The number l_s is defined by

$$l_s = \max_{(m\geqslant m_J, n\geqslant n_J)\in J_L} n. \tag{79}$$

The kth element of V_s can be defined by

$$V_s(k) = \begin{cases} \min_{(m,k)\in J_U} m, & 2 \leqslant k < l_s \\ m_J, & k = l_s \end{cases}. \tag{80}$$

Actually, given the vector V_s, we know that $J_s = \{(m_s,n_s)\}$ can only be one element chosen from the following set:

$$\hat{J}_s = \{(m,n) = (V_s(k),k) | n_J \leqslant k \leqslant l_s\}. \tag{81}$$

With $\hat{J}_s$, we define three sets, which contain only one element in each as follows:

$$K_s = \left\{(k,l) | h_{11}^{(22)}(k,l) = \min_{(m,n)\in\hat{J}_s} h_{11}^{(22)}(m,n)\right\}, \tag{82}$$

$$K_c = \left\{(k,l) | h_{11}^{(22)}(k,l) = \min_{(m,n)\in\hat{J}_s^{(c)}} h_{11}^{(22)}(m,n)\right\}, \tag{83}$$

$$K_r = \left\{(k,l) | h_{11}^{(22)}(k,l) = \min_{(m,n)\in\hat{J}_s^{(r)}} h_{11}^{(22)}(m,n)\right\}, \tag{84}$$

where $\hat{J}_s$ is defined in Eq. (81), and $\hat{J}_s^{(c)} = \hat{J}_s - \{(V_s(n_J),n_J)\}$, $\hat{J}_s^{(r)} = \hat{J}_s - \{(V_s(l_s),l_s)\}$.

Finally, for given J_s and J_U, we define

$$G(J_U) = s_{22}^{(*)} + \sum_{(m,n)\in J_U} f_{22}^{(*)}(m,n), \tag{85}$$

$$G_s(J_s,J_U) = s_{22}^{(*)} + \sum_{(m,n)\in J_s\cup J_U} f_{22}^{(*)}(m,n). \tag{86}$$

With these preparations, we are ready to present the algorithm as follows:

Step 1. Initially, we have $J_L = \emptyset$, $J_s = \{(m,n) | h_{11}^{(*)}(m,n) = \min[h_{11}^{(*)}(2,3),h_{11}^{(*)}(3,2)]\}$, $J_U = J_3 - J_s$, and $l_s = 2$, if $J_s = \{(2,3)\}, V_s = (3,3)$, else if $J_s = \{(3,2)\}, V_s = (4,2)$ and $m_J = n_J = 2$. Calculate G_s using Eq. (86). Actually, with $J_L = \emptyset$, G_s can be calculated by the following explicit formula:

$$G_s = s_{22}^{(*)} - \frac{(a_1\bar{a}_2' - a_1'\bar{a}_2)(b_1\bar{b}_2' - b_1'\bar{b}_2)}{(a_1a_2' - a_1'a_2)(b_1b_2' - b_1'b_2)} + 1. \tag{87}$$

As discussed before, we suppose $G' = G(L_3) < 0$ initially. After these preparations, we initialize G_f with $G_f = G(J_U)$ according to Eq. (85). If $G_f < 0$ we go to step 2, else we go to step 3.

Step 2. Find out $J_s' = \{(m_s',n_s')\}$ such that $f_{22}^{(*)}(m_s',n_s') = \min_{(m,n)\in J_U} f_{22}^{(*)}(m,n) = \min_{(m,n)\in\hat{J}_s} f_{22}^{(*)}(m,n)$, where $\hat{J}_s$ is defined in Eq. (81). So we need to find out the set $\hat{F}_s$. First, we check whether the following two inequalities are fulfilled or not:

$$h_{11}^{(22)}((m,n)\in K_r) \geqslant h_a[V_s(n_J)]\hat{h}_b, \tag{88}$$

$$h_{11}^{(22)}((m,n)\in K_c) \geqslant \hat{h}_a h_b(l_s), \tag{89}$$

where $h_a(k),h_b(k)$ are defined in Eq. (64) and $\hat{h}_a,\hat{h}_b$ are defined in Eq. (72). If Eq. (88) holds, we go to step 2.1, else if Eq. (89) holds we go to step 2.2, else we go to step 2.3.

Step 2.1. In this situation, we know that $h_{11}^{(22)}((m,n)\in K_r)$ is greater than all the values $h_{11}^{(22)}(V_s(l_s),k)$ for all $k \geqslant 2$. We need to calculate the value

$$G'(J_U) = G_f - \sum_{(m,n)\in J_r} f_{22}^{(*)}(m,n), \tag{90}$$

where $J_r = \{(m,n) | m = V_s(l_s), n \geqslant l_s\}$. If $G'(J_U) \leqslant 0$ we need to remove all the elements in J_r from the set of J_U. Then we can renew the values with $m_J = m_J + 1, n_J = n_J, l_s = l_s - 1, J_L = J_L \cup J_r, J_s = K_r, J_U = J_3 - J_L - J_s$ and $G_f = G_f - f_{22}^{(*)}((m,n)\in J_s)$. If $G_f < 0$, we go back to step 2, else we go to step 3. On the other hand, if $G'(J_U) > 0$, then we know that the element in the final set of J_s must be included in J_r. In this case we need to renew $J_L = J_L \cup J_s, J_s = \{(V_s(l_s),l_s)\}, J_U = J_U - J_s, V_s(l_s) = V_s(l_s) + 1, l_s = l_s + 1, V_s(l_s) = V_s(l_s - 1) - 1$, and $G_f = G_f - f_{22}^{(*)}((m,n)\in J_s)$. If $G_f < 0$, we go back to step 2, else we go to step 3.

Step 2.2. In this situation, we know that $h_{11}^{(22)}((m,n)\in K_c)$ is greater than all the values $h_{11}^{(22)}(k,n_J)$ for all $k \geqslant 2$. We need to calculate the value

$$G'(J_U) = G_f - \sum_{(m,n)\in J_c} f_{22}^{(*)}(m,n), \tag{91}$$

where $J_c = \{(m,n) | m \geqslant V_s(n_J), n = n_J\}$. If $G'(J_U) \leqslant 0$ we need to remove all the elements in J_c from the set of J_U. Then we can renew the values with $m_J = m_J, n_J = n_J + 1, l_s = l_s, J_L = J_L \cup J_c, J_s = K_c, J_U = J_3 - J_L - J_s$ and $G_f = G_f - f_{22}^{(*)}((m,n)\in J_s)$. If $G_f < 0$, we go back to step 2, else we go to step 3. On the other hand, if $G'(J_U) > 0$, then we know that the element in the final set of J_s must be included in J_c. In this case we need to renew $J_L = J_L \cup J_s, J_s = \{(V_s(n_J),n_J)\}, J_U = J_U - J_s, V_s(n_J) = V_s(n_J) + 1, l_s = l_s$, and $G_f = G_f - f_{22}^{(*)}((m,n)\in J_s)$. If $G_f < 0$, we go back to step 2, else we go to step 3.

Step 2.3. In this situation, we should renew $J_L = J_L \cup J_s, J_s = K_s, J_U = J_U - J_s$. Denoting $K_s = \{(k_m,k_n)\}$, we can renew l_s and V_s by the following method. If $k_n = l_s$, we have $V_s(l_s) = V_s(l_s) + 1, l_s = l_s + 1, V_s(l_s) = V_s(l_s - 1) - 1$. If $k_n < l_s$, we have $V_s(k_n) = V_s(k_n) + 1, l_s = l_s$. Finally, we renew $G_f = G_f - f_{22}^{(*)}((m,n)\in J_s)$. If $G_f < 0$, we go back to step 2, else we go to step 3.

Step 3. Now we have already found out the final sets J_L, J_s, J_U with step 2. In this step, we will calculate the value of s_L. According to the relation presented in Eq. (68), we should define

$$s_L = -\frac{G_f}{f_{22}^{(*)}((m,n)\in J_s)}. \tag{92}$$

Then we can calculate the lower bound $\underline{s_{11}^*}$ of s_{11} by using Eq. (69).

IV. EXACT MAXIMUM ERROR RATE WITH ONLY THREE STATES FOR MDI-QKD

In Sec. II, we showed the upper bound of error rate e_{11} with an explicit formula. The upper bound of $e_{11}^{(1)}$ is obtained with Eq. (44) by setting $e_{mn} = 0$, where $(m,n)\in J_2$. Obviously, the

condition with source y_A and y_B is not used in deriving $e_{11}^{(1)}$. Keeping sight of this fact, we suspect that a tighter bound can be found out considering all relations given by Eqs. (44)–(47). In the rest of this section, we will show that we can find out an exact maximum of error rate e_{11} within a finite number steps.

According to Eqs. (44)–(47), we can find out the expression of t_{11},t_{12},t_{21}, and t_{22} uniquely:

$$t_{11} = t_{11}^{(*)} + \sum_{(m,n)\in J_0} f_{11}^{(*)}(m,n)t_{mn}, \tag{93}$$

$$t_{12} = t_{12}^{(*)} + \sum_{(m,n)\in J_0} f_{12}^{(*)}(m,n)t_{mn}, \tag{94}$$

$$t_{21} = t_{21}^{(*)} + \sum_{(m,n)\in J_0} f_{21}^{(*)}(m,n)t_{mn}, \tag{95}$$

$$t_{22} = t_{22}^{(*)} + \sum_{(m,n)\in J_0} f_{22}^{(*)}(m,n)t_{mn}, \tag{96}$$

where

$$t_{11}^{(*)} = \frac{a_2'b_2'\tilde{T}_{xx} - a_2'b_2\tilde{T}_{xy} - a_2b_2'\tilde{T}_{yx} + a_2b_2\tilde{T}_{yy}}{(a_1a_2' - a_1'a_2)(b_1b_2' - b_1'b_2)},$$

$$t_{12}^{(*)} = \frac{-a_2'b_1'\tilde{T}_{xx} + a_2'b_1\tilde{T}_{xy} + a_2b_1'\tilde{T}_{yx} - a_2b_1\tilde{T}_{yy}}{(a_1a_2' - a_1'a_2)(b_1b_2' - b_1'b_2)},$$

$$t_{21}^{(*)} = \frac{-a_1'b_2'\tilde{T}_{xx} + a_1'b_2\tilde{T}_{xy} + a_1b_2'\tilde{T}_{yx} - a_1b_2\tilde{T}_{yy}}{(a_1a_2' - a_1'a_2)(b_1b_2' - b_1'b_2)},$$

$$t_{22}^{(*)} = \frac{a_1'b_1'\tilde{T}_{xx} - a_1'b_1\tilde{T}_{xy} - a_1b_1'\tilde{T}_{yx} + a_1b_1\tilde{T}_{yy}}{(a_1a_2' - a_1'a_2)(b_1b_2' - b_1'b_2)},$$

and $f_{11}^{(*)}(m,n), f_{12}^{(*)}(m,n), f_{21}^{(*)}(m,n), f_{22}^{(*)}(m,n)$ are defined by Eqs. (58)–(61).

With the properties of the functions $f_{11}^{(*)}(m,n), f_{12}^{(*)}(m,n), f_{21}^{(*)}(m,n), f_{22}^{(*)}(m,n)$ discussed in the previous section, we can find out an upper bound of t_{11} by setting $t_{1k} = t_{k1} = 1,(k \geqslant 3)$ and $t_{mn} = 0,(m,n \geqslant 3)$ crudely. As discussed in the previous section, all $t_{1k},t_{k1},(k \geqslant 3)$ do not have to equal to 1 at the same time as the constraint conditions such that $t_{12},t_{21},t_{22} \in [0,1]$. Thus, the problem of estimating the upper bound of t_{11} can be written into the following constrained optimization problem:

$$\begin{aligned} \max: t_{11} &= t_{11}^{(*)} + \sum_{k\geqslant 3} f_{11}^{(*)}(1,k)t_{1k} + f_{11}^{(*)}(k,1)t_{k1} \\ \text{st: } t_{12} &= t_{12}^{(*)} + \sum_{k\geqslant 3} f_{12}^{(*)}(1,k)t_{1k} \geqslant 0, \\ t_{12} &= t_{12}^{(*)} + \sum_{k\geqslant 3} f_{21}^{(*)}(k,1)t_{k1} \geqslant 0. \end{aligned} \tag{97}$$

In this COP, there is an infinite number of variables. Considering the independence between variables t_{1k} and t_{k1}, the COP in Eq. (97) can be decomposed into the following two COPs:

$$\begin{aligned} \max: t_1 &= \sum_{k\geqslant 3} f_{11}^{(*)}(1,k)t_{1k} \\ \text{st: } t_{12} &= t_{12}^{(*)} + \sum_{k\geqslant 3} f_{12}^{(*)}(1,k)t_{1k} \geqslant 0 \end{aligned} \tag{98}$$

and

$$\begin{aligned} \max: t_2 &= \sum_{k\geqslant 3} f_{11}^{(*)}(k,1)t_{k1} \\ \text{st: } t_{12} &= t_{12}^{(*)} + \sum_{k\geqslant 3} f_{21}^{(*)}(k,1)t_{k1} \geqslant 0. \end{aligned} \tag{99}$$

In order to solve the two COPs, we need to analyze the ratios $f_{11}^{(*)}(1,k)/f_{12}^{(*)}(1,k)$ and $f_{11}^{(*)}(k,1)/f_{21}^{(*)}(k,1)$. Actually, we have

$$\frac{f_{11}^{(*)}(1,k)}{f_{12}^{(*)}(1,k)} = -h_b(b_k',b_k), \quad \frac{f_{11}^{(*)}(k,1)}{f_{21}^{(*)}(k,1)} = -h_a(a_k',a_k),$$

where h_a,h_b are defined in Eq. (64). As discussed before, under the condition in Eq. (3), $h_a(k),h_b(k)$ are two non-negative monotone increasing functions of variable $k \geqslant 3$. This fact predicts that $t_{1,k+1}$ $(t_{k+1,1})$ has priority to be equal to 1 over $t_{1,k}$ $(t_{k,1})$ in order to maximize t_1 (t_2). Back to the COPs, we can solve them by introducing two neutral numbers k_a,k_b and two positive real numbers $s_a,s_b \in (0,1]$ such that

$$\begin{aligned} t_{12}^{(*)} + \sum_{k>k_b} f_{12}^{(*)}(1,k) &> 0 \\ t_{12}^{(*)} + \sum_{k\geqslant k_b} f_{12}^{(*)}(1,k) &\leqslant 0 \\ t_{12}^{(*)} + \sum_{k\geqslant k_b} f_{12}^{(*)}(1,k) + s_b f_{12}^{(*)}(1,k_b) &= 0 \end{aligned} \tag{100}$$

and

$$\begin{aligned} t_{21}^{(*)} + \sum_{k>k_a} f_{21}^{(*)}(k,1) &> 0 \\ t_{21}^{(*)} + \sum_{k\geqslant k_a} f_{21}^{(*)}(k,1) &\leqslant 0 \\ t_{21}^{(*)} + \sum_{k\geqslant k_a} f_{21}^{(*)}(k,1) + s_a f_{21}^{(*)}(k_a,1) &= 0. \end{aligned} \tag{101}$$

Then we can define the upper bound of t_{11} by

$$\begin{aligned} \overline{t_{11}^*} = t_{11}^{(*)} &+ \sum_{k\geqslant k_b} f_{11}^{(*)}(1,k) + s_b f_{11}^{(*)}(1,k_b) \\ &+ \sum_{k\geqslant k_a} f_{11}^{(*)}(k,1) + s_a f_{11}^{(*)}(k_a,1), \end{aligned} \tag{102}$$

where k_a,k_b and s_a,s_b are defined in Eqs. (100) and (101), which can be easily found out by using the algorithm presented in the previous section.

After getting the lower bound of s_{11} and the upper bound of t_{11}, we can easily obtain the upper bound of the error rate e_{11} such that

$$\overline{e_{11}^{(*)}} = \overline{t_{11}^{(*)}} / \underline{s_{11}^{(*)}}, \tag{103}$$

where $\underline{s_{11}^{(*)}}$ is defined in Eq. (69) and $\overline{t_{11}^{(*)}}$ is defined in Eq. (102).

V. NUMERICAL SIMULATION

In this section, we will present some numerical simulations to compare our results with the pre-existing results [19,23,24]. As discussed before, we know that the methods presented in

TABLE I. List of experimental parameters used in numerical simulations: e_0 is the error rate of the background; e_d is the misalignment-error probability; p_d is the dark count rate of UTPs per detector; f is the error correction inefficiency; η_v is the detection efficiency of Alice and Bob's detector; p_{dv} is the dark count rate of Alice and Bob's detector.

e_0	e_d	p_d	f	η_v	p_{dv}
0.5	1.5%	3.0×10^{-6}	1.16	0.75	1.0×10^{-6}

this paper apply to any sources that satisfy the condition given by Eq. (3). Below, for simplicity, we consider the following two cases. In the first case, we suppose that Alice and Bob use weak coherent states (WCS). In the second one, we suppose they use heralded single-photon sources (HSPS) with Poissonian distributions [23]. The UTP is located in the middle of Alice and Bob, and the UTP's detectors are identical, i.e., they have the same dark count rate and detection efficiency, and their detection efficiency does not depend on the incoming signals. We shall estimate what values would be probably observed for the gains and error rates in the normal cases by a linear lossy channel model as used elsewhere, e.g., [18,29]:

$$|n\rangle\langle n| = \sum_{k=0}^{n} C_n^k \xi^k (1-\xi)^{n-k} |k\rangle\langle k|$$

where ξ^k is the transmittance for a distance from Alice to the UTP. For fair comparison, we use the same parameter values used in [18,24] for our numerical evaluation, which follow the experiment reported in [28]. For simplicity, we shall put the detection efficiency to the overall transmittance $\eta = \xi^2\zeta$. We assume all detectors of UTP have the same detection efficiency ζ and dark count rate p_d. In the second case with HPSP, we assume all detectors of Alice and Bob have the same detection efficiency η_v and dark count rate p_{dv}.

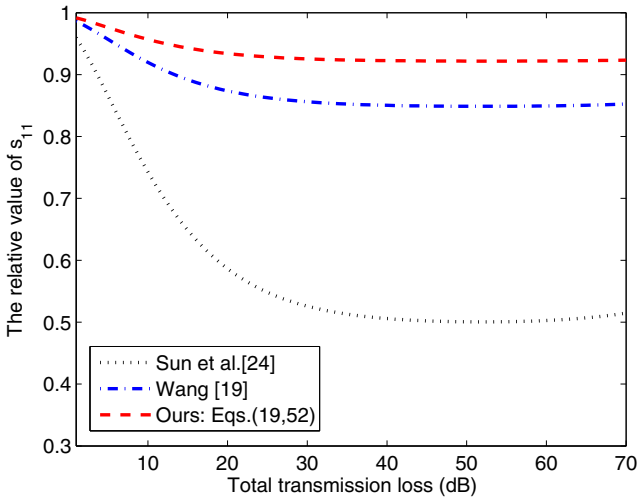

FIG. 1. (Color online) The relative value between the estimated parameter of s_{11} and the asymptotic limit of the infinite decoy-state method vs the total channel transmission loss using three-intensity decoy-state MDI-QKD with WCS. We set $\mu_1 = \nu_1 = 0.1$, $\mu_2 = \nu_2 = 0.5$ for decoy state and signal states, respectively.

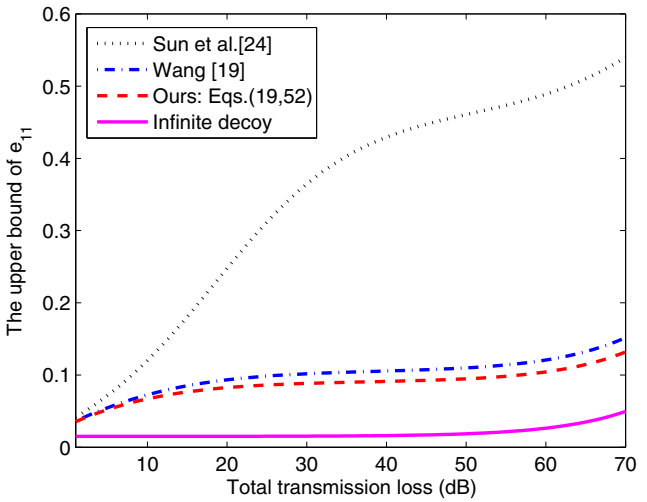

FIG. 2. (Color online) The estimated parameter of e_{11} vs the total channel transmission loss using three-intensity decoy-state MDI-QKD with WCS. We set $\mu_1 = \nu_1 = 0.1$, $\mu_2 = \nu_2 = 0.5$ for decoy state and signal states, respectively.

The values of these parameters are presented in Table I. With this, by taking the photon number cutoff approximation up to six photon number states, the total gains $S^{\omega}_{\mu_i,\nu_j}, (\omega = X, Z)$ and error rates $S^{\omega}_{\mu_i,\nu_j} E^{\omega}_{\mu_i,\nu_j}, (\omega = X, Z)$ of Alice's intensity $\mu_i (i = 0,1,2)$ and Bob's intensity $\nu_j (j = 0,1,2)$ can be calculated. By using these values, we can estimate the lower bounds of yield s^Z_{11} with Eq. (19). Also, we can estimate the upper bounds of error rate e^X_{11} with Eq. (52). In order to see more clearly, in Fig. 1, we plot the relative value of s_{11} to the result obtained with the infinite decoy-state method. The simulation of the upper bound of e_{11} is shown in Fig. 2. These figures clearly show that our results are tighter than the pre-existing ones. Furthermore, with these parameters, we can estimate the final key rate R of this protocol with Eq. (53), which is shown

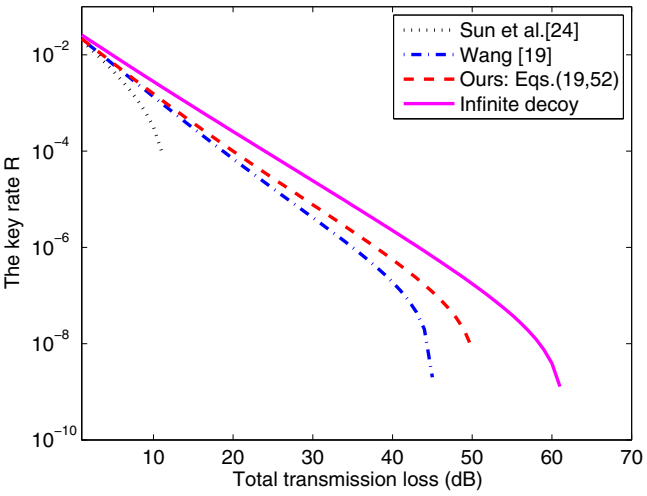

FIG. 3. (Color online) The estimated key rate R vs channel transmission using three-intensity decoy-state MDI-QKD with WCS. We set $\mu_1 = \nu_1 = 0.1$, $\mu_2 = \nu_2 = 0.5$ for decoy state and signal states, respectively.

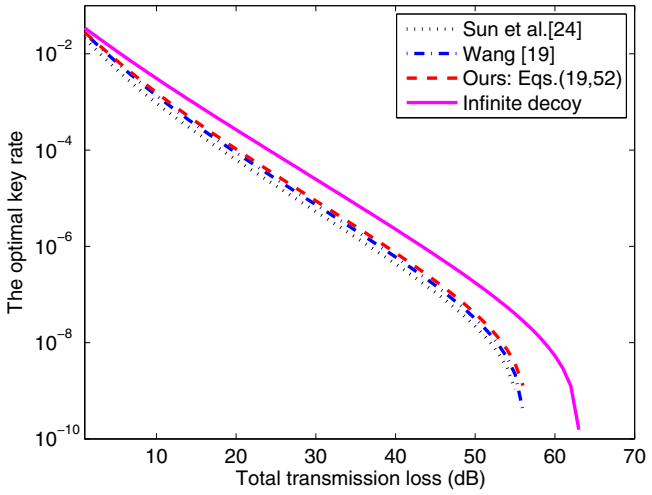

FIG. 4. (Color online) The optimal key rate vs the total channel transmission loss using three-intensity decoy-state MDI-QKD. We set $\mu_1 = \nu_1 = 0.1$ for decoy states.

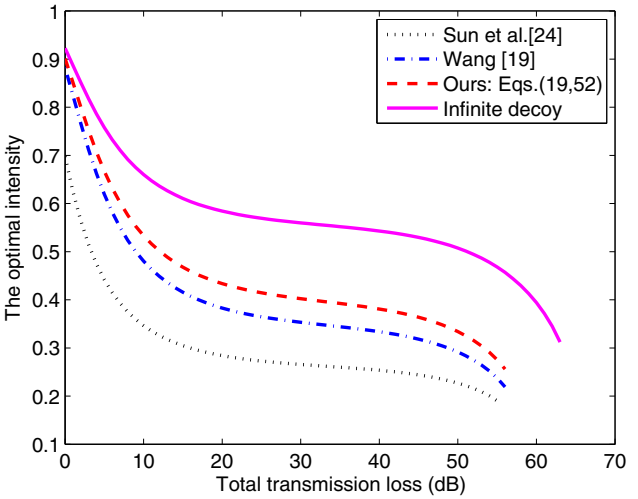

FIG. 6. (Color online) The optimal intensity vs the total channel transmission loss using three-intensity decoy-state MDI-QKD with WCS. We set $\mu_1 = \nu_1 = 0.1$ for decoy states.

in Fig. 3. In these three figures, the dotted lines are obtained by the method presented in [24], the dash-dotted lines are obtained by the method presented in [19], the dashed lines are obtained by the analytical method presented in Sec. II with Eqs. (19) and (52), and the solid lines are obtained by the infinite decoy-state method. In the simulation, the intensities used by Alice and Bob are assigned to $\mu_1 = \nu_1 = 0.1$, $\mu_2 = \nu_2 = 0.5$.

Furthermore, if we fix the densities of the decoy-state pulses used by Alice and Bob, the final key rate will change with Alice and Bob taking different intensities for their single-state pulses. Here, we also take $\mu_1 = \nu_1 = 0.1$ and assume that $\mu_2 = \nu_2 > \mu_1$. In Fig. 4, we present the optimal key rates with different methods. In order to see more clearly, in Fig. 5, we plot the relative value of the optimal key rate to the result obtained with the infinite decoy-state method. We can observe that our results are better than the pre-existing results. The optimal densities with the optimal key rate vs the total channel transmission loss are given in Fig. 6.

If we use a source of HSPS, we can obtain a similar conclusion, as illustrated by Fig. 7.

In Fig. 8, we plot the relative value of the optimal final key rate R to the result obtained with the infinite decoy-state method. We find that the results are further improved if we use a program based on Eqs. (69) and (103). In the simulation, we also take $\mu_1 = \nu_1 = 0.1$ and assume that $\mu_2 = \nu_2 > \mu_1$.

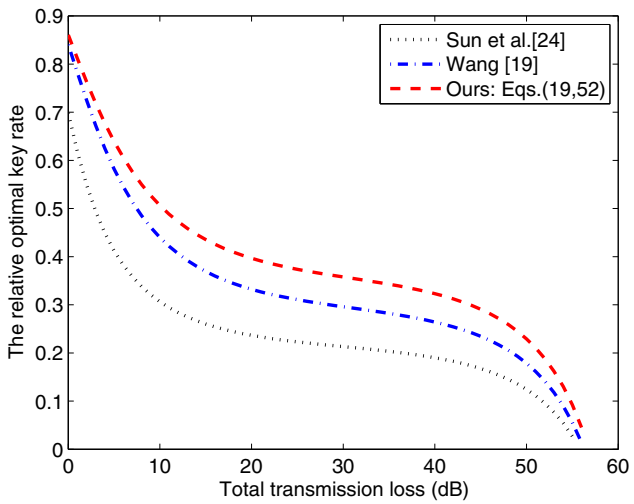

FIG. 5. (Color online) The relative value between the optimal key rate obtained with different methods and the asymptotic limit of the infinite decoy-state method vs the total channel transmission loss using three-intensity decoy-state MDI-QKD. We set $\mu_1 = \nu_1 = 0.1$ for decoy states.

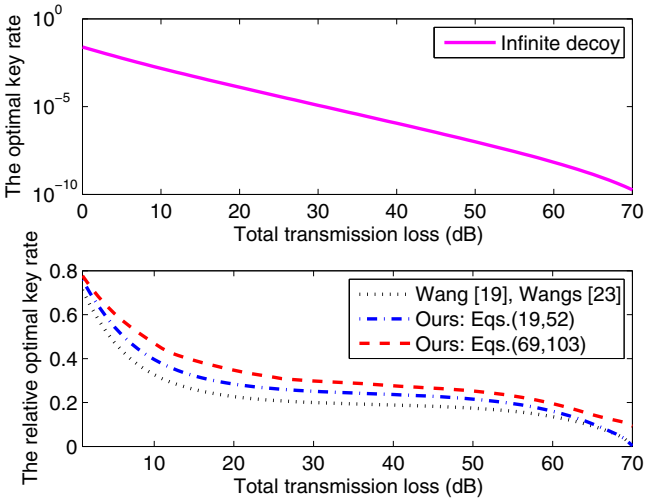

FIG. 7. (Color online) Key rates with HSPS. Top: Optimal key rate with infinite decoy states. Bottom: Relative value between the optimal key rate obtained with different methods and the asymptotic limit of the infinite decoy-state method vs the total channel transmission loss using three-intensity decoy-state MDI-QKD with HSPS. We set $\mu_1 = \nu_1 = 0.1$ for decoy states.

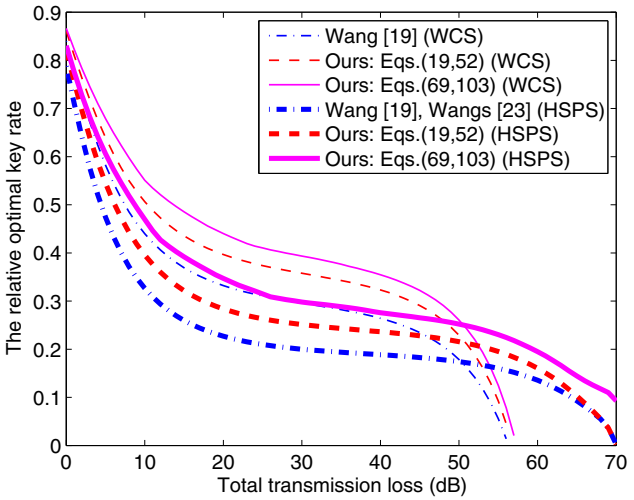

FIG. 8. (Color online) The relative value between the optimal key rate obtained with different methods and the asymptotic limit of the infinite decoy-state method vs the total channel transmission loss using three-intensity decoy-state MDI-QKD. We set $\mu_1 = \nu_1 = 0.1$ decoy states.

VI. CONCLUSION

We study the MDI-QKD in practice with only three different states in implementing the decoy-state method. First, we present tighter analytical formulas for the decoy-state method for two-pulse sources with three different states. Then we show an exact maximum of the yield s_{11} and an exact minimum of the error rate e_{11} with an efficient algorithm. These methods can be applied to the recently proposed MDI-QKD with an imperfect single-photon source such as the coherent states or the heralded states from the parametric down conversion. Our methods here can significantly improve the key rate and secure the distance of MDI-QKD with only three intensities.

ACKNOWLEDGMENTS

We acknowledge support from the 10000-Plan of Shandong province, the National High-Tech Program of China Grants No. 2011AA010800 and No. 2011AA010803, and NSFC Grants No. 11174177 and No. 60725416.

[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 *et al.*, Rev. Mod. Phys. **74**, 145 (2002); N. Gisin and R. Thew, Nature Photonics **1**, 165 (2006); M. Dusek, N. Lütkenhaus, and M. Hendrych, *in Progress in Optics VVVX*, edited by E. Wolf (Elsevier, New York, 2006); V. Scarani *et al.*, Rev. Mod. Phys. **81**, 1301 (2009).

[3] H. Inamori, N. Lütkenhaus, and D. Mayers, Eur. Phys. J. D **41**, 599 (2007); D. Gottesman *et al.*, 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).

[8] M. Hayashi, Phys. Rev. A **74**, 022307 (2006); **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); C. Z. 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); Y. Zhao *et al.*, in *Proceedings of IEEE International Symposium on Information Theory, Seattle* (IEEE, New York, 2006), pp. 2094–2098.

[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 *et al.*, Phys. Rep. **448**, 1 (2007).

[12] X.-B. Wang *et al.*, New J. Phys. **11**, 075006 (2009).

[13] G. Brassard, N. Lutkenhaus, 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 Semiclassic. Opt. **8**, 939 (1996).

[15] L. Lyderson, V. Makarov, and J. Skaar, Nature Photonics **4**, 686 (2010); I. Gerhardt *et al.*, Nature Commu. **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, D.C., 1998), p. 503; A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007); V. Scarani and R. Renner, *ibid.* **100**, 302008 (2008); in *3rd Workshop on Theory of Quantum Computation, Communication and Cryptography (TQC 2008)*, arXiv:0806.0120.

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

[18] K. Tamaki, H. K. Lo, C.-H. F. Fung, and B. Qi, Phys. Rev. A **85**, 042307 (2012).

[19] X.-B. Wang, Phys. Rev. A **87**, 012320 (2013).

[20] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Phys. Rev. Lett. **111**, 130501 (2013); P. Chan *et al.*, arXiv:1204.0738v1.

[21] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid, Phys. Rev. A **88**, 052303 (2013).

[22] Y. Liu *et al.*, Phys. Rev. Lett. **111**, 130502 (2013).
[23] Q. Wang and X.-B. Wang, Phys. Rev. A **88**, 052332 (2013).
[24] S. H. Sun, M. Gao, C. Y. Li, and L. M. Liang, Phys. Rev. A **87**, 052329 (2013).
[25] F. Xu, B. Qi, Z. Liao, and H.-K. Lo, Appl. Phys. Lett. **103**, 061101 (2013).
[26] C. Zhou *et al.*, arXiv:1308.3347v1.
[27] M. Curty *et al.*, arXiv:1307.1081v1.
[28] R. Ursin *et al.*, Nat. Phys. **3**, 481 (2007).
[29] Q. Wang and X.-B. Wang, arXiv:1311.1739.