Measurement-device-independent quantum key distribution with source state errors in photon number space

Cong Jiang\textsuperscript{1,2}, Zong-Wen Yu\textsuperscript{1,3}, and Xiang-Bin Wang\textsuperscript{1,2,4*†}

\textsuperscript{1}State Key Laboratory of Low Dimensional Quantum Physics, Department of Physics, Tsinghua University, Beijing 100084, Peoples Republic of China
\textsuperscript{2}Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China
\textsuperscript{3}Data Communication Science and Technology Research Institute, Beijing 100191, China
\textsuperscript{4}Jinan Institute of Quantum technology, SAICT, Jinan 250101, Peoples Republic of China

The existing decoy-state MDI-QKD theory assumes the perfect control of the source states which is an impossible task for any real setup. In this paper, we study the decoy-state MDI-QKD method with source errors without any presumed conditions and we get the final security key rate only with the range of a few parameters in the source state.

I. INTRODUCTION

Quantum key distribution (QKD) is one of the most successful applications of quantum information processing. QKD can provide unconditional security based on the laws of quantum physics\textsuperscript{1,2}. Almost all of the existing setups of QKD use an imperfect single-photon source which, in principle, suffers from the photon-number-splitting (PNS) attack\textsuperscript{3,4}. Fortunately, the decoy-state-method\textsuperscript{5,14} can help to make a setup with an imperfect single-photon source be as secure as that with a perfect single-photon source\textsuperscript{3,4}. Aside from the source imperfection, the limited detection efficiency is another threat to the security\textsuperscript{15}. The device independent QKD (DI-QKD)\textsuperscript{16} and the measurement-device-independent QKD (MDI-QKD)\textsuperscript{17,18} have been proposed to overcome the problem.

The key idea of MDI-QKD is that both Alice and Bob send out quantum signals to the untrust third party (UTP) but neither of them perform any measurement. The UTP would perform a Bell state measurement to each received pulse pair and announce whether it’s a successful event as well his measurement outcome in the public channel. Those bits corresponding to successful events will be post selected and further processed for the final key. By using the decoy-state method, Alice and Bob can use imperfect single-photon sources\textsuperscript{17,19} securely in the MDI-QKD. Hence, the decoy-state MDI-QKD can remove all detector side-channel attacks and PNS attacks with imperfect single-photon sources. The combination of the decoy-state method and MDI-QKD has been studied both experimentally\textsuperscript{20}\textsuperscript{25} and theoretically\textsuperscript{19,26,37}.

The existing decoy-state MDI-QKD theory assumes the perfect control of the source states. This is an impossible task for any real setup in practice. As shown in Ref.\textsuperscript{12,14}, in BB84 decoy-state QKD protocol, the intensity fluctuation, or more generally, the source errors in Fock space may break the equality

\[ s_k = s'_{k'}, \]  

where \( s_k \) is the yield of \( k \)-photon decoy pulse and \( s'_{k'} \) is the yield of \( k \)-photon signal pulse. Similarly to the traditional decoy-state QKD protocol, the source used in the decoy-state MDI-QKD protocol can not be perfectly stable. One important problem is the effect of source errors. In this paper, we would study the decoy-state MDI-QKD method with source errors without any presumed conditions (In most of the case, we have no idea about the details of source error, we can’t make any assumptions to the source error model). Only with the range of a few parameters in the source state, we could get the final security key rate in the cost of little decrease. In our method, we have assumed the worst case that Eve knows exactly the error of each pulse. Our result immediately applies to all existing experimental results. Before going further, we emphasize that our results here are unconditionally correct because we have not assumed any unproven conditions. Although there is another approach reported for the issue of intensity error by using the model of attenuation to pulses from an untrusted source, however, there exists counter examples to the elementary equation in that approach, as was shown in the appendix of Ref.\textsuperscript{14}.

This paper is arranged as follows. After the Introduction above, we present our method with the virtual protocol and some definitions in Sec. II A and Sec. II B. We then show the details in Sec. II C and Sec. II D about how we formulate the final security key rate with only the bound values of a few parameters in the states involved. And in Sec. II E we will show some numerical simulation results. The article is ended with a concluding remark.
II. OUR METHOD

In the five-intensity decoy-state MDI-QKD protocol, we assume that Alice (Bob) has two sources $v_A$, $x_A$ ($v_B$, $x_B$) in $X$ basis and three sources $w_A$, $y_A$, $z_A$ ($w_B$, $y_B$, $z_B$) in $Z$ basis, and they send pulse pairs (one pulse from Alice, one pulse from Bob) to UTP one by one. Each pulse sent out by Alice (Bob) is randomly chosen from one of the five sources $l_A$ ($r_B$) with constant probability $p_{l_A}$ ($p_{r_B}$) respectively for $l, r = v, x, w, y, z$. Sources $v_A, w_A$ ($v_B, w_B$) are the unstable vacuum sources in $X$ and $Z$ basis respectively. Generally, these unstable vacuum sources are not exact zeros photon-number state. $x_A, y_A$ ($x_B, y_B$) are the decoy sources which are used to estimate the lower bounds of yield and the upper bound of phase-flip error of single-photon pulse pairs. $z_A$ ($z_B$) is the signal source which is used to extract the final key.

We shall use notation $lr$ to indicate the two-pulse source when Alice use source $l_A$ and Bob use source $r_B$ to generate a pulse pair. For simplicity, we omit the subscripts of any $l$ and $r$ for a two-pulse source, eg., source $y_2$ is the source that Alice uses source $y_A$ and Bob uses source $z_B$. We also denote the number of counts caused by the two-pulse source $lr$ as $N_{lr}$. $N_{lr}$ are observed values and will be regarded as known values.

A. Virtual protocol

For clarity, we first consider a virtual protocol. Suppose Alice and Bob send $N_l$ pulse pairs to UTP in the whole protocol. In photon-number space, the states of the $l_{th}$ pulse pair from source $l_A$ ($r_B$) is

$$
\rho_{l_A} = \sum_k a_k^{l, i}|k\rangle\langle k| \quad (\rho_{r_B} = \sum_k b_k^{r, i}|k\rangle\langle k|),
$$

(2)

for $l, r = v, x, w, y, z$. At any time $i (i \in [1, N_l])$, Alice (Bob) choose only one source from $l_A$ ($r_B$) with constant probability $p_{l_A}$ ($p_{r_B}$) respectively. The unselected pulses will be discarded. After UTP has completed all measurements to the incident pulse pairs, Alice (Bob) checks the record about which pulse is selected at each time, i.e., which time has used which source. Obviously, Alice (Bob) can decide which source is to be used at each time in the very beginning. This is just then the real protocol of the decoy-state method. Videlicet, the formulas we get under such a virtual protocol will hold for the real protocol.

B. Some definitions

Definition 1. In the protocol, Alice and Bob send $N_l$ pulse pairs to UTP, one by one. If UTP announces that it’s a successful event, then we say that the $l_{th}$ pulse pair has caused a count.

Given the source state in Eq. (2), any $l_{th}$ pulse sent out by Alice (Bob) must be in a photon number state. We shall make use of this fact that any individual pulse is in one Fock state.

Definition 2. Set $C$ and $c_{jk}$: Set $C$ contains any pulse pair that has caused a count; set $c_{jk}$ contains any $|jk\rangle$-photon pulse pair (Alice’s $j$-photon pulse and Bob’s $k$-photon pulse) that has caused a count. Mathematically speaking, the sufficient and necessary condition for $i \in C$ is that the $l_{th}$ pulse pair has caused a count. The sufficient and necessary condition for $i \in c_{jk}$ is that the $l_{th}$ pulse pair is a $|jk\rangle$-photon pulse pair and it has caused a count. For instance, if the photon number states of the first 10 pulse pairs sent to UTP are $|00\rangle, |01\rangle, |10\rangle, |12\rangle, |11\rangle, |10\rangle, |10\rangle, |00\rangle, |11\rangle, |11\rangle$, and the pulse pairs of $i = 2, 3, 4, 7, 8, 9, \ldots$, $c_{00} = \{i|i = 2, 3, 4, 7, 8, 9, \ldots\}$, $c_{01} = \{i|i = 3, 7, \ldots\}$, $c_{10} = \{i|i = 8, \ldots\}$.

Clearly, $C = \cup_{j,k \geq 0} c_{jk}$.

Definition 3. We use superscripts $U, L$ for the upper bound and lower bound of a certain parameter. In particular, given any $k \geq 0$ in Eq. (2), we denote $a_k^{l, U}$, $b_k^{r, L}$ ($b_k^{U}$, $b_k^{L}$) for the maximum value and minimum value of $\{a_k^{l, i}|i \in C\}$, and $l, r = v, x, w, y, z$. We assume these bound values are known in the protocol.

C. The lower bound of counts of single-photon pulse pairs

Here in this subsection, we only need to consider the pulse pairs in $Z$ basis. According to our definitions, if the $l_{th}$ pulse pair is an element of $c_{jk}$, the probability that it is from source $lr$ is

$$
P_{l_{ijk}} = p_{l_B} p_{r_B} a_j^{l, U} b_k^{r, L} d_{jk}, \quad (l, r = w, y, z),
$$

(3)

where

$$
d_{jk} = \frac{1}{\sum_{l, r = w, y, z} p_{l_B} p_{r_B} a_j^{l, U} b_k^{r, L}}.
$$

(4)

We want to formulate the numbers of $|jk\rangle$-photon pulse pair counts caused by each two-pulse source. Given the definition of the set $c_{jk}$, this is equivalent to asking how many pulse pairs in set $c_{jk}$ come from each two-pulse source. The probability that the $l_{th}$ pulse pair $(i \in c_{jk})$ comes from source $lr$ is $P_{l_{ijk}}$, and equivalently,

$$
n_{l_{jk}}^{lr} = \sum_{i \in c_{jk}} P_{l_{ijk}},
$$

(5)

where $n_{l_{jk}}^{lr}$ is the numbers of $|jk\rangle$-photon pulse pair counts caused by source $lr$. Since every pulse pair in $c_{jk}$ has caused a count, therefore we can formulate the total pulse pair counts caused by source $lr$ by

$$
N_{lr} = \sum_{j,k \geq 0} n_{l_{jk}}^{lr} = \sum_{j,k \geq 0} \sum_{1 \leq i \leq c_{jk}} p_{l_B} p_{r_B} a_j^{l, U} b_k^{r, L} d_{jk}.
$$

(6)
We also need to introduce the following notation
\[ \tilde{N}_{lr} = \sum_{j,k \geq 1} \sum_{i \in c_{jk}} p_i p_{r_i} a_1^{j,l} b_{k}^{i} d_{jk}, \] (7)

If we define
\[ D_{jk} = \sum_{i \in c_{jk}} d_{ij}^{k}, \] (8)
our goal as stated in the very beginning of Sec. I is simple to find out the lower bound of \( D_{11} \). For, with this and Def. 3, the lower bound of the number of counts caused by those single-photon pulse pairs from the source \( lr \), i.e., \( n_{11}^{lr} \) is
\[ n_{11}^{lr} = p_i p_{r_i} a_1^{l} b_{k}^{i} D_{11} \leq n_{11}^{lr}. \] (9)

In what follows, we shall first find the formula of \( D_{11} \) in terms of \( \tilde{N}_{yy}, \tilde{N}_{zz} \) based on Eq. (7).
\[ \tilde{N}_{yy} = p_2 a_1^{y,y} b_1^{l} D_{11} + p_2 a_1^{y,y} - \xi_1, \] (10)
\[ \tilde{N}_{zz} = p_2 a_1^{z,z} b_1^{l} D_{11} + p_2 a_1^{z,z} + \xi_2, \] (11)
where
\[ \Lambda = \sum_{j} a_j^{y,y} b_k^{l} D_{jk}, \quad \Lambda' = \sum_{j} a_j^{z,z} b_k^{l} D_{jk}, \] (12)
\[ \xi_1 = p_2 \sum_{j,k \geq 1} \sum_{i \in c_{jk}} (a_j^{y,y} b_k^{l} - a_j^{y,y} b_k^{l}) d_{jk} \geq 0, \] (13)
\[ \xi_2 = p_2 \sum_{j,k \geq 1} \sum_{i \in c_{jk}} (a_j^{z,z} b_k^{l} - a_j^{z,z} b_k^{l}) d_{jk} \geq 0, \] (14)
with
\[ J = \{ j, k | j \geq 1, k \geq 1, j > k \}. \] (15)

Without losing the generality, we assume \( K_a = a_j^{z,z} b_k^{l} - a_j^{z,z} b_k^{l} \leq a_j^{z,z} b_k^{l} = K_b \) (in the case of \( K_a > K_b \), the results can be obtained similarly). According to the definitions of \( \Lambda \) and \( \Lambda' \), we have
\[ \Lambda' = K_a \Lambda + \frac{\xi_3}{p_2^2}, \] (16)
where
\[ \frac{\xi_3}{p_2} = \sum_{j} (a_j^{z,z} b_k^{l} - K_a a_j^{y,y} b_k^{l}) D_{jk}. \] (17)

Further, we assume the important conditions
\[ \frac{a_k^{z,l}}{a_k^{y,y}} \geq \frac{a_k^{z,l}}{a_k^{y,y}} \geq \frac{a_k^{z,l}}{a_k^{y,y}}, \quad \frac{b_k^{z,l}}{b_k^{y,y}} \geq \frac{b_k^{z,l}}{b_k^{y,y}}, \] (18)
for all \( k \geq 2 \). The imperfect sources with small error used in practice such as the coherent state source, the heralded source out of the parametric down-conversion, could satisfy the above restriction.

With the assumption \( K_a \leq K_b \), one may easily prove that \( \xi_3 \geq 0 \). Thus Eq. (11) can be rewritten into
\[ \tilde{N}_{zz} = p_2 a_1^{z,z} b_1^{l} D_{11} + p_2 K_a \Lambda + \xi_2 + \xi_3. \] (19)

Combining Eqs. (10, 11), we get the lower bound of \( D_{11} \)
\[ D_{11} \geq D_{11}^{L} = \frac{b_k^{z,l}\tilde{N}_{yy} - b_k^{z,l}\tilde{N}_{zz}}{a_1^{y,y} (b_1^{l} b_2^{z,l} - b_2^{z,l} b_1^{l})}, \] (20)
where \( \tilde{N}_{yy} \) and \( \tilde{N}_{zz} \) are the lower and upper bounds of \( \tilde{N}_{yy} \) and \( \tilde{N}_{zz} \) respectively that will be evaluated in the coming. In obtaining Eq. (20), we have used the facts that \( \xi_1, \xi_2 \) and \( \xi_3 \) are all nonnegative values.

In what follows, we shall formulate the lower bound of \( \tilde{N}_{yy} \) and the upper bound of \( \tilde{N}_{zz} \). These bounds can be easily obtained if we assume that Alice and Bob can prepare the vacuum source. However, in practice, the different intensities are usually generated with an intensity modulator, which has a finite extinction ratio. So it is usually difficult to create a perfect vacuum state in decoy-state QKD experiments. In the following of this paper, we will show that these bounds can also be formulated without using the perfect vacuum source.

Similarly to the conditions in Eq. (13), we also assume
\[ \frac{a_k^{i,l}}{a_k^{i,l}} \geq \frac{b_k^{i,l}}{b_k^{i,l}} \geq \frac{b_k^{i,l}}{b_k^{i,l}}, \] (21)
for all \( i \in C \). The lower bound of \( \tilde{N}_{yy} \) and the upper bound of \( \tilde{N}_{zz} \) can be expressed by
\[ \tilde{N}_{yy}^{L} = \frac{N_{yy} - n_{yy}^{w,L}}{1 - \sigma_C^{y}}, \quad \tilde{N}_{zz}^{U} = \frac{N_{zz} - n_{zz}^{w,L}}{1 - \sigma_A^{z} - \sigma_B^{z}}, \] (22)
where
\[ \sigma_C^{y} = \frac{a_k^{y,y} b_k^{l} a_k^{y,y} b_k^{l}}{a_k^{y,y} b_k^{l} a_k^{y,y} b_k^{l}}, \quad \sigma_A^{z} = \frac{a_k^{z,z} b_k^{l} a_k^{z,z} b_k^{l}}{a_k^{z,z} b_k^{l} a_k^{z,z} b_k^{l}}, \quad \sigma_B^{z} = \frac{b_k^{z,l} b_k^{l} b_k^{z,l}}{b_k^{z,l} b_k^{l} b_k^{z,l}}, \] and
\[ \tilde{n}_{yy}^{w,L} = \frac{p_y a_0^{y,y} N_{wy} + p_y b_0^{y,y} N_{wy} - p_2 a_0^{y,y} b_0^{y,y} b_0^{y,y}}{p_2 a_0^{w,L} b_0^{y,y} b_0^{y,y} N_{wy}}, \] (23)
\[ \tilde{n}_{zz}^{u,L} = \frac{p_z a_0^{z,z} N_{wz} + p_z b_0^{z,z} N_{wz} - p_2 a_0^{w,z} b_0^{z,z} b_0^{z,z}}{p_2 a_0^{w,L} b_0^{z,z} b_0^{z,z} N_{wz}}. \] (24)

The detailed proof of Eq. (22) can be found in Appendix A. With Eqs. (20, 22), we could formulate \( D_{11}^{L} \) with only known parameters. Eq. (22) is the most important conclusion in this paper.

With these preparation, we can now bound the fraction of counts of single-photon pulse pair among all counts caused by the signal source \( zz \)
\[ \Delta_{11}^{zz} = \frac{n_{zz}^{zz}}{N_{zz}} \geq \frac{p_2 a_1^{z,z} b_1^{l} D_{11}^{t}}{N_{zz}} = \Delta_{11}^{t} \Delta_{11}. \] (25)
Define \( S_{lr} = \frac{N_m}{p_{lr}p_rN_o} \) as the yield of source \( lr \). Then, we have
\[
\Delta_1^{L} = \frac{a_1^L b_1^L}{a_1^L b_1^L} \left( \frac{a_1^L b_1^L}{a_1^L b_1^L} \right) = \frac{a_1^L b_1^L}{a_1^L b_1^L},
\]
where
\[
\tilde{S}_{yy} = S_{yy} - \frac{a_0^U b_0^U S_{wU}}{a_0^U b_0^U} - \frac{b_0^L S_{wL}}{b_0^L},
\]
\[
\tilde{S}_{zz} = S_{zz} - \frac{a_0^L S_{wL}}{a_0^L} - \frac{b_0^L S_{wL}}{b_0^L} - \frac{a_0^U b_0^U S_{wU}}{a_0^U b_0^U}.
\]

D. The upper bound of the phase-flip error rate of single-photon pulse pairs

In order to estimate the final key rate, we also need the upper bound of phase-flip error rate of single-photon pulse pair, i.e., \( e_{11} \), which means we need to formulate the upper bound of phase-flip error counts of single-photon pulse pairs first. Here in this subsection, we only need consider the pulse pairs in basis \( X \). Similarly to Def. 2 in Sec. II A, we define set \( H \) which contains all pulse pairs that has caused an error count and \( h_{jj} \) which contains all \((j,k)\)-photon pulse pair that has caused an error count. The probability that the \( i \)th pulse pair \((i \in h_{jj})\) is from each two-pulse source \( lr \) \((l, r = v, x)\) is
\[
Q^l_{i,jk} = p_{lr} a_j^l b_k^i g_{jk}, \quad (l, r = v, x).
\]
where
\[
g_{jk} = \frac{1}{\sum_{l,v=x,v} p_{lr} a_j^l b_k^i}.
\]

If we denote the number of error counts caused by the source \( lr \) as \( M_{xx} \), we have
\[
M_{xx} = m_{xx}^v + \sum_{i \in h_{11}} p_2 a_1^i b_1^i T_{11} \geq \sum_{i \in h_{11}} p_2 a_1^i b_1^i \tilde{g}_{11},
\]
where
\[
m_{xx}^v = \sum_{k \geq 0} p_2 a_0^k b_0^i g_{00} + \sum_{j \geq 0} p_2 a_j^i b_0^j g_{00} - \sum_{i \in h_{00}} p_2 a_0^i b_0^i g_{00}.
\]

If we define
\[
\tilde{M}_{xx} = M_{xx} - m_{xx}^v,
\]
Eq. (31) can be written into
\[
\tilde{M}_{xx} = \sum_{i \in h_{11}} p_2 a_1^i b_1^i \tilde{g}_{11} + \sum_{j \in h_{11}} p_2 a_j^i b_0^j \tilde{g}_{11} \geq p_2 a_1^L b_1^L \tilde{g}_{11},
\]
\[
G_{11} = \sum_{i \in h_{11}} \tilde{g}_{11}.
\]

Our goal now is to formulate the upper bound of \( G_{11} \). For, we have
\[
m_{xx}^v \geq \sum_{i \in h_{11}} 2 p_2 a_1^i b_1^i G_{11} = m_{xx}^v G_{11},
\]
where \( m_{xx}^v \) is the number of error counts of single-photon pulse pairs for source \( xx \), and \( m_{xx}^v G_{11} \) is the upper bound of \( m_{xx}^v \).

With the same method to upper bound \( \tilde{N}_{yy} \), the upper bound of \( G_{11} \) can be formulated by
\[
G_{11}^U = \frac{1}{a_1^L b_1^L (1 - \sigma_A^v - \sigma_B^v)} \left[ M_{xx} - \frac{1}{p_2} a_0^U b_0^U M_{xx} \right],
\]
where
\[
\sigma_A^v = \frac{a_0^U a_0^V b_0^U b_0^V \sigma_{\tilde{T}_{xx}^v}}{a_0^U b_0^U}, \quad \sigma_B^v = \frac{b_0^U b_0^V a_0^V a_0^U \sigma_{\tilde{T}_{xx}^v}}{b_0^U b_0^V}.
\]

Thus, we can get the upper bound of the error rate of single-photon pulse pairs
\[
e_{11} = \frac{m_{xx}^v}{n_{xx}^v} \leq \frac{a_1^L b_1^L x_{xx}^v}{a_1^L b_1^L D_{11}^v} \tilde{G}_{11}^U = e_{11}^U.
\]

Define \( T_{\alpha\beta} = \frac{M_{xx}}{p_{lr} p_r N_s} \) as the error yield of source \( lr \). We have
\[
e_{11}^U = \frac{e_{11}^U}{(a_1^U b_1^U) (1 - \sigma_A^v - \sigma_B^v) \tilde{T}_{xx}^v},
\]
where
\[
\tilde{T}_{xx} = T_{xx} - \frac{a_0^U a_0^V T_{xx}}{a_0^U a_0^U} - \frac{b_0^U b_0^V T_{xx}}{b_0^U b_0^V} + \frac{a_0^V b_0^V T_{xx}}{a_0^V b_0^V},
\]
and \( x_{11}^v = D_{11}^v/N_s \) is the yield of single-photon pulse pair. Here we have used the fact that the lower bound of yield of single-photon pulse pair in basis \( X \) can be estimated by the lower bound of it in \( Z \) basis.

III. THE FINAL KEY RATE AND NUMERICAL SIMULATION

In this section, we present some numerical simulations. Firstly, we shall estimate what values would be probably observed for the yields and error yields in the normal cases by the linear models [24]. With these known values, we can calculate the lower bound of counting rate and the upper bound of phase-flip error rate of single-photon pulse pair with Eq. (29) and Eq. (39) respectively. Then the final key rate can be calculated by
\[
R = S_{zz} \{ \Delta_1^{L} [1 - H(e_{11}^U)] - f H(E_{zz}) \},
\]


| $e_0$ | $e_d$ | $p_d$ | $\eta_d$ | $f$ | $\alpha_f$ |
|-------|-------|-------|----------|-----|------------|
| 0.5   | 1.5%  | $6.02 \times 10^{-6}$ | 14.5%    | 1.16| 0.2        |

TABLE I: List of experimental parameters used in numerical simulations. $e_0$: error rate of the vacuum count. $e_d$: the misalignment-error probability. $p_d$: the dark count rate of UTP’s detectors. $\eta_d$: the detection efficiency of UTP’s detectors. $f$: the error correction inefficiency. $\alpha_f$: the fiber loss coefficient (dB/km).

where $f$ is the error correction inefficiency and $H(x) = -x \log_2 x - (1-x) \log_2 (1-x)$ is the binary Shannon entropy function.

We focus on the symmetric case where the two channel transmissions from Alice to UTP and from Bob to UTP are equal. We also assume that the UTP’s detectors are identical, i.e., they have the same dark count rates and detection efficiencies, and their detection efficiencies do not depend on the incoming signals. The density matrix of the coherent state with intensity $\mu$ can be written into

$$\rho = \sum_k \frac{\mu^k}{k!} |k\rangle \langle k|.$$  

The actual intensity of the $i$th pulse for source $l$ out of Alice’s (or Bob’s) laboratory is

$$\mu_i^l = \mu_i (1 + \delta_l), \quad (l = v, x, w, y, z),$$ 

(42)

with the boundary conditions $|\delta_l| \leq \delta_1$ for $l = v, w$ and $|\delta_l| \leq \delta_2$ for $l = x, y, z$.

Experimental conditions and the detectors properties are listed in Table I and Fig. 1 and Fig. 2 show the key rates versus transmission distance. The red solid curve is the result of the protocol with infinite number of decoy states, and other curves are the results for the protocol discussed in this work with different intensity fluctuation.

FIG. 1: (color online) The optimal key rates versus transmission distance (the distance between Alice and Bob). Here we set $\mu_v = 0.03, \mu_w = 0.03$. The intensity of the signal sources are optimized. The red solid curve is the result of the protocol with infinite number of decoy states, and other curves are the results for the protocol discussed in this work with different intensity fluctuation.

FIG. 2: (color online) The optimal key rates versus transmission distance (the distance between Alice and Bob). Here we set $\mu_v = 0.03, \mu_w = 0.03$. The intensity of the signal sources are optimized. The red solid curve is the result of the protocol with infinite number of decoy states, and other curves are the results for the protocol discussed in this work with different intensity fluctuation.

IV. CONCLUSION

In summary, we have shown how to calculate the lower bound of the fraction of single-photon pulse pair counts and the upper bound of the phase-flip error rate of the single-photon pulse pair in the decoy state MDI-QKD with source errors, provided that the parameters in the diagonal state of the source satisfy equation (15) and (21) and bound values of each parameters in the state is known. Our result here can be extended to the nonasymptotic case by taking statistical fluctuations into consideration in Eq. (26) and Eq. (39). This will be reported elsewhere.

Acknowledgement: We thank Xiao-Long Hu and Yi-Heng Zhou for discussions. We acknowledge the financial support in part by the 10000-Plan of Shandong province (Taishan Scholars); National High-Tech Program of China Grants No. 2011AA010800 and No. 2011AA010803; National Natural Science Foundation of China Grants No. 11474182, No. 11174177, and No. 60725416; Open Research Fund Program of the State Key Laboratory of Low-Dimensional Quantum Physics.

Grant No. KF2015153; and Key Research and Development Plan Project of Shandong Province Grant No. 2015GGX101035.
Appendix A: The proof of the lower and upper bounds of $\tilde{N}_{yy}$, $\tilde{N}_{zz}$ and $\tilde{M}_{xx}$

Firstly, we formulate the lower and upper bounds of $\tilde{N}_{yy}$. The lower and upper bounds of $\tilde{M}_{xx}$ and $\tilde{N}_{zz}$ can be obtained similarly.

We could write $N_{wy}, N_{yw}, N_{ww}$ and $N_{yy}$ in the form of Eq. (6)

$$N_{wy} = \sum_{j,k \geq 0} \sum_{i \in c_{jk}} p_w p_y q_{0}^{y,i} d_{m,i}^{p} b_{m,i}^{0} d_{k,i}^{j}, \quad (A.1)$$

$$N_{yw} = \sum_{j,k \geq 0} \sum_{i \in c_{jk}} p_w p_y q_{0}^{y,i} d_{m,i}^{p} b_{m,i}^{0} d_{k,i}^{j}, \quad (A.2)$$

$$N_{ww} = \sum_{j,k \geq 0} \sum_{i \in c_{jk}} p_w p_y q_{0}^{y,i} d_{m,i}^{p} b_{m,i}^{0} d_{k,i}^{j}, \quad (A.3)$$

$$N_{yy} = \sum_{j,k \geq 0} \sum_{i \in c_{jk}} p_y q_{0}^{y,i} d_{m,i}^{p} b_{m,i}^{0} d_{k,i}^{j}, \quad (A.4)$$

After a series of calculation, Eq. (A.4) can be rewritten in the following equivalent form

$$N_{yy} = \sum_{j,k \geq 0} p_y q_{0}^{y,i} d_{m,i}^{p} b_{m,i}^{0} d_{k,i}^{j}, \quad (A.5)$$

where

$$\tilde{N}_{yy} = p_y^2 \left[ \sum_{j,k \geq 0} \sum_{i \in c_{jk}} \frac{a_{0}^{y,i}}{a_{0}^{y,i}} d_{m,i}^{p} b_{m,i}^{0} d_{k,i}^{j} \right]$$

$$+ \sum_{j,k \geq 0} \sum_{i \in c_{jk}} \frac{a_{0}^{y,i}}{a_{0}^{y,i}} d_{m,i}^{p} b_{m,i}^{0} d_{k,i}^{j}$$

$$- \sum_{j,k \geq 0} \sum_{i \in c_{jk}} \frac{a_{0}^{y,i}}{a_{0}^{y,i}} d_{m,i}^{p} b_{m,i}^{0} d_{k,i}^{j}$$

$$A = p_y^2 \sum_{j \geq 1} \sum_{i \in c_{jk}} \frac{a_{0}^{y,i}}{a_{0}^{y,i}} d_{m,i}^{p} b_{m,i}^{0} d_{k,i}^{j},$$

$$B = p_y^2 \sum_{j \geq 1} \sum_{i \in c_{jk}} \frac{a_{0}^{y,i}}{a_{0}^{y,i}} d_{m,i}^{p} b_{m,i}^{0} d_{k,i}^{j},$$

$$C = p_y^2 \sum_{j \geq 1} \sum_{i \in c_{jk}} \frac{a_{0}^{y,i}}{a_{0}^{y,i}} d_{m,i}^{p} b_{m,i}^{0} d_{k,i}^{j}. $$

One may easily prove that

$$n_{yy}^{w} = \tilde{N}_{yy} - A - B + C,$$

where

$$n_{yy}^{w} = \sum_{k \geq 0} \sum_{i \in c_{ko}} p_{0}^{y,i} q_{0}^{y,i} d_{m,i}^{p} b_{m,i}^{0} d_{k,i}^{j}$$

$$+ \sum_{j \geq 0} \sum_{i \in c_{ko}} p_{0}^{y,i} q_{0}^{y,i} d_{m,i}^{p} b_{m,i}^{0} d_{k,i}^{j}$$

$$- \sum_{i \in c_{ko}} p_{0}^{y,i} q_{0}^{y,i} d_{m,i}^{p} b_{m,i}^{0} d_{k,i}^{j}.$$
Combining Eq. (A.7) with Eq. (A.10), we can formulate upper bounds of $\tilde{\sigma}_{yy}$ as follows:

$$\tilde{\sigma}_{yy}^L = \frac{N_{yy} - \tilde{n}_{yy}^U}{1 + \sigma_C^U},$$  \hspace{1cm} (A.12)

where $\sigma_C^U = \sigma_C^\dagger \sigma_C^\dagger$. Combining Eq. (A.8) with Eq. (A.11), we can formulate upper bounds of $\tilde{\sigma}_{yy}$ as:

$$\tilde{\sigma}_{yy}^U = \frac{N_{yy} - \tilde{n}_{yy}^L}{1 - \sigma_A^U - \sigma_B^U},$$  \hspace{1cm} (A.13)

where $\sigma_A^U$ and $\sigma_B^U$ have been defined in Eq. (A.9).

By using the same way, we can formulate the lower and upper bounds of $\tilde{N}_{zz}$ and $\tilde{M}_{xx}$. Actually, we only need the upper bounds of $\tilde{N}_{zz}$ and $\tilde{M}_{xx}$. Explicitly, we have:

$$\tilde{N}_{zz} = \frac{N_{zz} - \tilde{n}_{zz}^L}{1 - \sigma_A^U - \sigma_B^U}, \quad \tilde{M}_{xx} = \frac{M_{xx} - \tilde{m}_{xx}^U}{1 - \sigma_A^U - \sigma_B^U},$$  \hspace{1cm} (A.14)

where

$$\tilde{n}_{zz}^L = \frac{p_w}{p_w w_0 b_0} N_{wz} + \frac{p_z}{p_w b_0} N_{zw} - \frac{p_w}{p_v} \tilde{n}_{zz}^U b_w^L N_{ww},$$

$$\tilde{m}_{xx}^U = \frac{p_w}{p_v a_0} a_0 M_{xx} + \frac{p_z}{p_v} b_0^L M_{xv} - \frac{p_w}{p_v} \tilde{m}_{xx}^U a_0^L b_w^L M_{wv},$$

and

$$\sigma_A^U = \frac{a_0^U a_1^U}{a_0^L a_1^L}, \quad \sigma_B^U = \frac{b_0^U b_1^U}{b_0^L b_1^L},$$

\[ \sigma_A^\dagger = \frac{a_0^\dagger a_1^\dagger}{a_0^\dagger a_1^\dagger}, \quad \sigma_B^\dagger = \frac{b_0^\dagger b_1^\dagger}{b_0^\dagger b_1^\dagger}. \]
[26] K. Tamaki, H.-K. Lo, C.-H. F. Fung, et al., Phys. Rev. A, 85, 042307 (2012).
[27] X. Ma, C.-H. F. Fung, and M. Razavi, Phys. Rev. A 86, 052305 (2012).
[28] Q. Wang and X.-B. Wang, Phys. Rev. A 88, 052332 (2013).
[29] F. Xu, M. Curty, B. Qi et al., Appl. Phys. Lett. 103, 061101 (2013).
[30] M. Curty, F. Xu, W. Cui et al., Nat. Commun. 5, 3732 (2014).
[31] Z.-W. Yu, Y.-H. Zhou, and X.-B. Wang, Phys. Rev. A 88, 062339 (2013).
[32] R. Valivarthi, I. Lucio-Martinez, P. Chan, A. Rubenok et al., J. Mod. Opt. 62, 1141 (2015).
[33] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, Phys. Rev. A 89, 052325 (2014).
[34] Q. Wang and X.-B. Wang, Sci. Rep. 4, 4612 (2014).
[35] F. Xu, H. Xu, and H.-K. Lo, Phys. Rev. A 89, 052333 (2014).
[36] Z.-W. Yu, Y.-H. Zhou, and X.-B. Wang, Phys. Rev. A 91, 032318 (2015).
[37] Y.-H. Zhou, Z.-W. Yu, X.-B. Wang. Phy. Rev. A 93, 042324 (2016).