We present formulas to tightly upper bound the phase-flip errors in decoy state method by using 4 intensities. Our result compressed the bound to about a quarter of known result for MDI-QKD. Based on this, we find that the key rate is improved by more than 100% given weak coherent state sources (WCS), and even more than 200% with the heralded single-photon sources (HSPS).

**PACS numbers:** 03.67.Dd, 42.81.Gs, 03.67.Hk

**I. INTRODUCTION**

One of the most fascinating properties of quantum key distribution (QKD) is its unconditional security in theory \[1, 2\]. However, most practical devices behave differently from the theoretical models assumed in the security proof. Security for real set-ups of QKD \[1, 2\] has become a major problem in this area in the recent years. The insecurity loopholes are mainly due to the imperfect single-photon source and the limited efficiency of the detectors. Fortunately, by using the decoy-state method \[3–12\], it has been shown that the unconditional security of QKD can still be assured with an imperfect single-photon source \[13, 14\].

Besides the source imperfection, the defect in the detectors is another threat to the security \[15\]. To patch up this, several approaches have been proposed. One is the device independent QKD (DI-QKD) \[16\]. This technique does not require detailed knowledge of how QKD devices work and can prove security based on the violation of a Bell inequality.

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., neither Alice and Bob performs any measurement, but they only send out quantum signals to the relay which can be controlled by the un-trusted third party (UTP). After Alice and Bob send out signals, they wait for UTP’s announcement of weather he has obtained the successful detection, and proceed to the standard postprocessing of their sifted data, such as error rate estimation, error correction, and privacy amplification. The only assumption needed in MDI-QKD is that the preparation of the quantum signal sources by Alice and Bob. In practice, in order to obtain a higher key rate or realize a longer distance key distribution, we’d better use laser sources with decoy state method. This has been discussed in Ref. \[18\], and explicit formulas for the practical decoy-state implementa-

**II. TRADITIONAL DECOY-STATE METHOD WITH ONLY 4 INTENSITIES FOR BB84 PROTOCOL**

In the four-intensity protocol, Alice has four (virtual) sources, the vacuum source \(\rho_0 = |0\rangle\langle 0|\) which prepares vacuum pulses, two decoy sources \(\rho_x, \rho_y\) which prepare decoy pulses, and the signal source \(\rho_z\) which prepares signal pulses. In photon-number space, we suppose

\[
\rho_l = \sum_k a_k^l |k\rangle \langle k|, \quad (l = x, y, z),
\]

where \(|k\rangle\) is the \(k\)-photon Fock state, \(a_k^l \geq 0\) for all \(k \geq 0\).

At each time, Alice will randomly select one of her 4 sources to emit a pulse. For post-processing, Alice and Bob evaluate the data with the same basis. With the observed total gains and error rates, the final secure key rate can be calculated by the following formula \[3\]

\[
R = a_s^1 s_1 [1 - H(e_1)] - S_z H(E_z),
\]

where \(S_z\) and \(E_z\) denote, respectively, the total gain and error rate of the signal state \(\rho_z\). \(s_1\) and \(e_1\) are, respectively, the fraction and error rate of detection events by
Bob that have originated form single-photon pulses emitted by Alice, and $H$ is the binary Shannon entropy. In this paper, we use the capital letter $S(E)$ for known total gains (error rates) and the lowercase letter $s, e$ for unknown variables.

In order to estimate the final key rate of this protocol, we need find out the lower bound of the yield $s_1$ and the upper bound of the error rate $e_1$. In the coming subsection, we devote to estimate the lower bound of $s_1$ firstly.

### A. The lower bound of the yield $s_1$

With given the different sources, Alice randomly chooses quantum channels with different photon-number states. Thus, the total gain with source $\rho_l$ can be expressed into the following convex form

$$S_l = \sum_{k \geq 0} a_k^l s_k, \quad (l = x, y, z),$$  \hspace{1cm} (3)

where $s_k$ is the yield of an $k$-photon pulse. In order to obtain an effective lower bound of $s_1$, we need eliminate the gains associated with the vacuum state from the total gain firstly. Considering this fact, we can rewrite the relations in Eq. (3) into

$$\tilde{S}_l = \sum_{k \geq 1} a_k^l s_k, \quad (l = x, y, z),$$  \hspace{1cm} (4)

where we define

$$\tilde{S}_l = S_l - a_0^l S_0, \quad (l = x, y, z),$$  \hspace{1cm} (5)

with $S_0$ being the gain of the vacuum source.

The lower bound of $s_1$ has already been studied \cite{5–8}. As presented in the previous works, if Alice has 3 different sources $\rho_0 = |0\rangle\langle 0|, \rho_x, \rho_y$, the lower bound of $s_1$ can be written into

$$\tilde{s}_1(x, y) = \frac{a_y^2 \tilde{S}_x - a_z^2 \tilde{S}_y}{a_2^2 a_y^2 - a_1^2 a_y^2},$$  \hspace{1cm} (6)

under the condition

$$\frac{a_k^y}{a_k^x} \geq \frac{a_z^2}{a_2^2} \geq \frac{a_1^y}{a_1^x},$$  \hspace{1cm} (7)

for all $k \geq 2$. It is worth pointing out that the lower bound given by Eq. (6) does not only apply to the weak coherent source, but also to any source as long as it meets the condition in Eq. (7).

In this 4-intensity protocol, there are three different no-vacuum sources. In order to get the lower bound of $s_1$ directly from Eq. (6), we also need to introduce the following condition

$$\frac{a_k^1}{a_k^x} \geq \frac{a_z^2}{a_2^2} \geq \frac{a_1^1}{a_1^x},$$  \hspace{1cm} (8)

for all $k \geq 2$. Then we can obtain some effective lower bounds of $s_1$ with Eq. (6) by choosing any two different sources from $\rho_x, \rho_y$ and $\rho_z$. After this, we can use the maximum one as the estimation of the lower bound of $s_1$ for this 4-intensity protocol

$$\tilde{s}'_1 = \max\{\tilde{s}_1(x, y), \tilde{s}_1(x, z), \tilde{s}_1(y, z)\},$$  \hspace{1cm} (9)

where $\tilde{s}_1(l, r)$ is just $s_1(x, y)$ in Eq. (6) with changing $x$ and $y$ into $l$ and $r$ respectively. In order to simplify this expression and derive other main results in this work, we need to define the following function with sources $\rho_0, \rho_y$ and $\rho_z$

$$G(i, j, k) = (g_{i}^{x} - g_{j}^{x})(g_{j}^{y} - g_{k}^{y}) - (g_{i}^{y} - g_{j}^{y})(g_{j}^{x} - g_{k}^{x}),$$  \hspace{1cm} (10)

where

$$g_{m}^{l} = \frac{a_{m}^{l}}{a_{0}^{m}}, \quad (m \geq 1; l = x, y, z).$$  \hspace{1cm} (11)

Now, we assume that the states $\rho_0, \rho_y$ and $\rho_z$ satisfy the following important condition

$$G(i, j, k) \geq 0,$$  \hspace{1cm} (12)

when $k - j \geq j - i \geq 0$. In Appendix A, we will show that the imperfect sources used in practice such as the weak coherent sources, the heralded source out of the parametric-down conversion, satisfy all the above conditions given by Eqs. (7–12). With these conditions presented in Eqs. (7–12), we can simplify the lower bound $\tilde{s}'_1$ by

$$\tilde{s}'_1 = \mathcal{S}_1(x, y).$$  \hspace{1cm} (13)

The detailed proof of this conclusion can be found in Appendix B.

### B. The upper bound of the error rate $e_1$

In order to estimate the final key rate, we also need the upper bound of the error rate $e_1$. In the previous works, the upper bound of $e_1$ is obtained by putting the errors with all multi-photon pulses on the error with the single-photon pulse. Explicitly, we can write the upper bound of $e_1$ with 3-intensity decoy state method as follows

$$\tilde{e}_1 = \frac{S_x E_x - a_0^1 S_0 E_0}{a_1^2 \tilde{s}_1},$$  \hspace{1cm} (14)

where $\tilde{s}_1$ is the lower bound of $s_1$, $S_x$ and $E_x$ are the total gain and error rate of the source $\rho_x$ respectively, $S_0$ and $E_0$ are the total gain and error rate of the vacuum source respectively. With the 3-intensity decoy state method, we can not find out a more better explicit formula to estimate the upper bound of $e_1$. In order to get a more tightened upper bound, we need to introduce one more source. This is the main reason for us to consider the 4-intensity decoy state method.
Similar to the gain, the error rate can depend on the photon number. Let us denote $e_k$ as the error of an $k$-photon pulse. The error rate $E_l$ for the source $\rho_l (l = x, y, z)$ can be given by

$$ T_l = S_l E_l = \sum_{k \geq 0} a_k s_k e_k, \quad (l = x, y, z). \quad (15) $$

If we denote $t_k = s_k e_k$, and

$$ \tilde{T}_l = T_l - a_0^l T_0, \quad (l = x, y, z), \quad (16) $$

Eq. (15) can be rewrite into the following equivalent form

$$ \tilde{T}_l = \sum_{k \geq 1} a_k^l t_k, \quad (l = x, y, z). \quad (17) $$

In this 4-intensity decoy state method, there are 3 different no-vacuum sources can be used for Alice. Then we have 3 different relations about $t_1$ which are presented in Eq. (17). With these 3 relations, by eliminating the variables $t_2$ and $t_3$, we obtain the expression of $t_1$ as follows

$$ t_1 = \tilde{T}_1 + \sum_{k \geq 4} f_{t_1}(k) t_k, \quad (18) $$

where

$$ \tilde{T}_1 = \frac{a_1^1 a_2^1 a_3^1}{G(1, 2, 3)} \left[ (a_2^2 a_3^2 - a_3^2 a_2^2) \tilde{T}_x - (a_3^1 a_2^1 - a_2^1 a_3^1) \tilde{T}_y + (a_3^1 a_2^1 - a_3^1 a_2^1) \tilde{T}_z \right], \quad (19) $$

and

$$ f_{t_1}(k) = -\frac{G(2, 3, k)}{G(1, 2, 3)}, \quad (k \geq 4), \quad (20) $$

with $G(1, 2, 3)$ being defined in Eq. (10). Under the condition presented in Eq. (12), we can easily find out that $f_{t_1}(k) \leq 0$ for all $k \geq 4$. Then we can conclude that $\tilde{T}_1$ given by Eq. (19) is actually a upper bound of $t_1$. Then the upper bound of $e_1$ can be given by

$$ \tilde{S}_1 = \frac{1}{\tilde{T}_1} \quad (21) $$

where $\tilde{S}_1$ is the lower bound of $s_1$ given by Eq. (13).

**C. Numerical Simulation for BB84 protocol**

In this subsection, we will present some numerical simulations to compare the results obtained by using the 3-intensity decoy state method with the results of 4-intensity method for the regular BB84 protocol. As discussed before, we know that the methods presented in this work does not only apply to the weak coherent sources (WCS). Actually, it can be used to estimate the final key rate for any sources that satisfy the condition given by Eq. (7) for the 3-intensity method, and the conditions given by Eqs. (7, 12) for the 4-intensity method. Below for simplicity, we consider the following two cases. In the first case, we suppose that Alice use WCS. In the second one, we suppose she use the heralded single-photon sources (HSPS) with poisson distributions [23]. The Bob’s detectors are identical, i.e., they have the same dark count rate and detection efficiency, and the detection efficiency does not depend on the incoming states.

---

**TABLE I: List of experimental parameters used in numerical simulations**

| $e_0$   | $e_d$  | $p_d$     | $\eta_v$ | $p_{dc}$ |
|---------|--------|-----------|-----------|----------|
| 0.5     | 1.5%   | $3.0 \times 10^{-6}$ | 0.75      | $1.0 \times 10^{-6}$ |

---

**FIG. 1: (Color online) The ratio of the upper bound of $e_1$ between the estimations obtained by using 4-intensity and 3-intensity decoy state methods, i.e., $\tilde{S}_1/\tilde{T}_1$, versus the total channel transmission loss. We set $\mu_1 = 0.2$ for decoy state.**
The overall transmission probability of each photon is $\eta = \xi \zeta$. We assume all detectors of Bob have the same detection efficiency $\zeta$ and dark count rate $p_d$. The values of these parameters are presented in Table I. With this, the total gains $S_\mu$ and error rates $S_\mu E_\mu$ of Alice’s intensity $\mu_i$ ($i = 0, 1, 2, 3$ for 3-intensity method, $i = 0, 1, 2, 3, 4$ for 4-intensity method) can be calculated. By using these values, we can estimate the lower bounds of yield $s_1$ with Eq.(6) and Eq.(13) for 3-intensity and 4-intensity decoy state methods respectively. Also, we can estimate the upper bounds of error rate $e_1$ with Eq.(14) and Eq.(21) for 3-intensity and 4-intensity decoy state methods respectively. Furthermore, with these parameters, we can estimate the final key rate $R$ of this protocol with Eq.(2). If we fix the density(ies) of the decoy-state source(s) used by Alice, the final key rate will change with Alice taking different intensities for her signal-state pulses. Here, in order to make a rational and effective comparison, we set the intensities of the decoy source in 3-intensity method and the first decoy source in 4-intensity method are the same and $\mu_1 = 0.2$; let the intensity of the second decoy source in 4-intensity method to be the optimal intensity of signal source in 3-intensity method and assume $\mu_2 > \mu_1$.

With these preparations, we can conclude that the lower bounds of $s_1$ estimated by using the 3-intensity and 4-intensity decoy state methods are the same, i.e., $\Delta_1 = \Delta'_1$. In order to see more clearly, in Fig.1, we plot the ratio of the upper bound of $e_1$ between the estimations obtained by using 4-intensity and 3-intensity decoy state methods, i.e., $\frac{e_1}{e'_1}$. The relative value between the optimal key rate obtained with different methods and the asymptotic limit of the infinite decoy-state method are shown in Fig.2. In order to clarify the superiority of the 4-intensity decoy state method, we plot the ratio of the optimal key rate between the results obtained by using 4-intensity and 3-intensity decoy state methods in Fig.3. In Fig.1 and Fig.3, the blue dashed lines are obtained with WCS, the red solid lines are obtained with HSPS. In Fig.2, the black dotted line and green dash-dot line are the results obtained by using 3-intensity decoy state method with WCS and HSPS respectively, the blue dashed line and the red solid line are the results obtained by using 4-intensity decoy state with WCS and HSPS respectively. With these 3 figures, we can conclude that the results obtained by using the 4-intensity decoy state method are better than the results of 3-intensity method. But it only have a litter improvement.

### III. Tightened Formula for Decoy-State MDI-QKD with 4 Intensities

In the protocol, each time a pulse-pair (two-pulse state) is sent to the relay for detection. The relay is controlled by an UTP. The UTP will announce whether the pulse-pair has caused a successful event. Those bits corresponding to successful events will be post-selected and further processed for the final key. Since real set-ups only use imperfect single-photon sources, we need the decoy-state method for security.
We assume Alice (Bob) has four sources, \( o_A, x_A, y_A, z_A \) \((o_B, x_B, y_B, z_B)\) which can only emit four different states \( \rho_{A/B}(r) = a, o, x, y, z \). In the following discussion, we assume \( o_A \) and \( o_B \) are two vacuum sources. In photon number space, we have \( \rho_{oA} = |0\rangle\langle 0 |, \rho_{oB} = |0\rangle\langle 0 |. \) For the others, suppose
\[
\rho_{rA} = \sum_k a_k^r |k\rangle\langle k |, \rho_{rB} = \sum_k b_k^r |k\rangle\langle k |, r = x, y, z.
\]
In order to obtain the main results, we also need to introduce the following function
\[
\mathcal{H}(i, j, k) = (h_i^x - h_i^y)(h_j^y - h_j^z) - (h_i^y - h_i^z)(h_j^z - h_j^x),
\]
where
\[
h_{n} = \frac{b_{n}^{r}}{a_{n}^{r}}, \quad (n \geq 1, l = x, y, z).
\]
Now, we assume that the states \( \rho_{x(A/B)}, \rho_{y(A/B)}, \rho_{z(A/B)} \) satisfy the following important conditions:
\[
\frac{c_{5}}{c_{2}} \geq \frac{c_{4}}{c_{2}} \geq \frac{c_{3}}{c_{2}}, \quad \frac{c_{y}^{o}}{c_{2}} \geq \frac{c_{y}^{z}}{c_{2}} \geq \frac{c_{y}^{x}}{c_{2}}, \quad (c = a, b), \quad (23)
\]
for \( k \geq 2, \) and
\[
\mathcal{G}(i, j, k) \geq 0, \quad \mathcal{H}(i, j, k) \geq 0, \quad (24)
\]
when \( k-j \geq j-i \geq 0. \) Similar to \( \mathcal{G}, \) the imperfect sources used in practice such as the coherent state source, the heralded source out of the parametric-down conversion, satisfy the above restrictions. Given a specific type of source, the above listed different states have different average photon numbers (intensities), therefore the states can be obtained by controlling the light intensities.

At each time, Alice will randomly select one of her 3 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 un-trusted relay. We regard equivalently that each time a two-pulse source is selected and a pulse pair (one pulse from Alice, one pulse from Bob) is emitted. For post-processing, Alice and Bob evaluate the data sent in two bases separately. The Z-basis is used for key generation, while the X-basis is used for testing against tampering and the purpose of quantifying the amount of privacy amplification needed. With the observed total gains and error rates, we can calculate the final secure key rate with the following formula
\[
R = a_{1}^{l}b_{1}^{l}s_{11}\left[1 - H(e_{11}^{l})\right] - S_{zA2B}^{Z} + H(E_{zA2B}^{Z}), \quad (25)
\]
where \( S_{zA2B}^{Z} \) and \( E_{zA2B}^{Z} \) denote, respectively, the gain and error rate in the Z-basis when both Alice and Bob use z-source \( \rho_{zA} \) and \( \rho_{zB}; \) \( f \) is the efficiency factor of the error correction method used; \( s_{11}^{l} \) and \( e_{11}^{l} \) are the gain and error rate when both Alice and Bob send single-photon states. In this paper, we use capital letter \( Z(X) \) for the bases and the lowercase letter \( x, y, z \) for the different sources.

In order to estimate the final key rate of this protocol, we need find out the lower bound of the yield \( s_{11} \) and the upper bound of the error rate \( e_{11}. \)

### A. The lower bound of the yield \( s_{11} \)

With given the different sources, Alice and Bob randomly choose quantum channels with different photon-number states. Thus, the total gain can be expressed into the following convex form
\[
S_{lr} = \sum_{j, k \geq 0} a_{j}^{l}b_{k}^{l}s_{jk}, \quad (r = x, y, z), \quad (26)
\]
when Alice and Bob send pulses with \( \rho_{oA} \) and \( \rho_{oB} \) respectively. Here and after, we omit the subscripts \( A \) and \( B \) without causing any ambiguity. It is well-known that, in order to obtain an effective lower bound of \( s_{11} \), we need eliminate the gains associated with the vacuum state from the total gain firstly. Considering this fact, we can rewrite the relation in Eq. \((27)\) into
\[
\tilde{S}_{lr} = \sum_{j, k \geq 1} a_{j}^{l}b_{k}^{r}s_{jk}, \quad (r = x, y, z), \quad (28)
\]
with
\[
\tilde{S}_{lr} = S_{lr} - a_{0}^{l}s_{0r} - b_{0}^{l}s_{0l} + a_{0}^{l}b_{0}^{r}s_{00}, \quad (r = x, y, z). \quad (29)
\]

The lower bound of \( s_{11} \) has already been exhaustive studied for 3-intensity decoy state MDI-QKD protocol \[11, 23, 26–28\]. Until now, the most tightly explicit formula to calculate the lower bound of \( s_{11} \) is given in Ref. 26. As presented in Ref. 26, the lower bound of \( s_{11} \) with 3 different sources \((o_A, l_A, r_A \) and \( o_B, l_B, r_B)\) used in each side of Alice and Bob can be expressed as
\[
\Sigma_{11}(l, r) = \frac{(a_{1}^{l}a_{2}^{l}b_{1}^{l}b_{2}^{l} - a_{1}^{l}a_{2}^{l}b_{1}^{l}b_{2}^{l})S_{lr} - b_{1}^{l}b_{2}^{l}(a_{1}^{l}a_{2}^{l} - a_{1}^{l}a_{2}^{l})S_{lr} - a_{1}^{l}a_{2}^{l}(b_{1}^{l}b_{2}^{l} - b_{1}^{l}b_{2}^{l})S_{lr}}{a_{1}^{l}b_{1}^{l}(a_{1}^{l}a_{2}^{l} - a_{1}^{l}a_{2}^{l})(b_{1}^{l}b_{2}^{l} - b_{1}^{l}b_{2}^{l})}, \quad (30)
\]
under the condition
\[ \frac{a_{k}^{l}}{a_{k}^{r}} \geq \frac{a_{l}^{z}}{a_{k}^{r}} \geq \frac{a_{l}^{x}}{a_{l}^{r}} a_{l}^{x} \frac{b_{k}^{r}}{b_{l}^{r}} \geq \frac{b_{l}^{r}}{b_{l}^{r}} \geq \frac{b_{l}^{r}}{b_{l}^{r}} \]

for all \( k \geq 2 \), where \( S_{1l}, S_{lr}, S_{r} \) are the amended gains defined by Eq. (25). In this 4-intensity protocol, there are 3 no-vacuum sources. We can estimate the effective lower bounds of \( s_{11} \) with Eq. (30) by choosing \( l \) and \( r \) as any two different sources from \( x, y, z \). Then we can use the maximum one as the lower bound of \( s_{11} \) for this 4-intensity protocol

\[ \tilde{s}_{11} = \max \{ s_{11}(x, y), s_{11}(x, z), s_{11}(y, z) \} \]. (31)

Actually, under the assumptions given by Eqs. (24, 25), we can simplify the lower bound of \( s_{11} \) in Eq. (31) by choosing the lowest two sources at each side of Alice and Bob, such that

\[ \tilde{s}_{11} = s_{11}(x, y). \] (32)

The detailed proof of this conclusion can be found in appendix B.

### B. The upper bound of the error rate \( e_{11} \)

In order to estimate the final key rate, we also need the upper bound of the error rate \( e_{11} \). In previous works, the upper bound of \( e_{11} \) is obtained by putting the errors with all multi-photon pairs on the error with the single-photon pair. Explicitly, we can write the upper bound of \( e_{11} \) with 3-intensity decoy state method as follows

\[ \tilde{\tau}_{11} = \frac{S_{xx}E_{xx} - a_{0}^{6}S_{00}E_{00} - b_{0}^{6}S_{00}E_{00} + a_{0}^{6}b_{0}^{6}S_{00}E_{00}}{a_{1}^{l}a_{l}^{r}b_{l}^{r} \tilde{s}_{11}} \] (33)

where \( \tilde{s}_{11} \) is the lower bound of \( s_{11}, S_{lr} \) and \( E_{lr} \) are the total gain and error rate when Alice use the source \( \rho_{x} \) and Bob use the source \( \rho_{y} \) respectively. With the numerical results presented in the third subsection of this part, we know that the upper bound obtained with this method is too rough to get an tight estimation of the final key rate comparing with the results obtained by using the infinite-decoy state method. In order to find out a more tightened upper bound of \( e_{11} \), we need introduce one more source in each side of Alice and Bob. This is the main reason for us to consider the 4-intensity decoy state method for MDI-QKD. As expected, we can find out a more tightened upper bound of \( e_{11} \) for this protocol.

Similar to the total gain, the error rate can be write into the following convex expressions

\[ \tilde{T}_{lr} = \sum_{j,k \geq 1} a_{j}^{l}b_{k}^{l}t_{jk}, \quad (l, r = x, y, z), \] (34)

where \( T_{lr} = E_{lr}S_{lr}, t_{jk} = s_{jk}e_{jk} \), and

\[ \tilde{T}_{lr} = T_{lr} - a_{0}^{l}T_{0r} - b_{0}^{l}T_{0l} + a_{0}^{l}b_{0}^{l}T_{00}, \quad (l, r = x, y, z). \] (35)

In this 4-intensity protocol, there are 3 different no-vacuum sources in each side of Alice and Bob. Then we have 9 different relations about \( e_{11} \) which are given by Eq. (34). With these 9 relations, by eliminating the variables \( t_{12}, t_{21}, t_{22}, t_{31}, t_{32}, t_{33}, t_{33}, t_{32}, t_{31}, \) we obtain the expression of \( t_{11} \)

\[ t_{11} = \tilde{t}_{11} + \sum_{(m,n) \in J_{0}} f_{t_{11}}(m,n)t_{mn}, \] (36)

with

\[ f_{t_{11}}(m,n) = - \frac{a_{m}^{l}G(m)b_{n}^{l}H'(n)}{a_{1}^{2}a_{3}^{2}G(1, 2, 3)b_{1}^{2}b_{2}^{2}b_{3}H(1, 2, 3)}, \] (37)

and

\[ G'(m) = \begin{cases} G(m, 2, 3), & m = 1, 2; \\ G(2, 3, m), & m \geq 3, \end{cases} \]

\[ H'(n) = \begin{cases} H(n, 2, 3), & n = 1, 2; \\ H(2, 3, n), & n \geq 3. \end{cases} \]

Here, \( h_{l}^{k} \) is defined by Eq. (23), \( G(i, j, k) \) and \( H(i, j, k) \) are defined in Eq. (10) and Eq. (22) respectively. With the
The upper bound of $e_{11}$ versus the total channel transmission loss for MDI-QKD with WCS and HSPS. We set $\mu_1 = \nu_1 = 0.1$ for decoy state, and $\mu_2 = \nu_2$.

**TABLE II:** List of experimental parameters used in numerical simulations: $e_0$ is the error rate of background, $e_d$ is the misalignment-error probability; $p_d$ is the dark count rate of UTP’s per detector; $f$ is the error correction inefficiency; $\eta_v$ is the detection efficiency of Alice and Bob’s detector; $p_{dv}$ is the dark count rate of Alice and Bob’s detector.

| Parameter | Value         |
|-----------|---------------|
| $e_0$     | 0.5           |
| $e_d$     | 1.5%          |
| $p_d$     | $3 \times 10^{-6}$ |
| $f$       | 1.16          |
| $\eta_v$  | 0.75          |
| $p_{dv}$  | $1 \times 10^{-6}$ |

conditions presented in Eqs. (24-25), we can prove that

$$f_{t_{11}}(m, n) \leq 0,$$

for all $(m, n) \in J_0$. Then we conclude that the expression given by Eq. (37) is actually an upper bound of $f_{t_{11}}$. With this, we can estimate the upper bound of $e_{11}$ by the following explicit formula

$$e_{11}' = \frac{s_{11}'}{s_{11}},$$

(40)

where $s_{11}'$ is the lower bound of $s_{11}$ given in Eq. (32).

**C. Numerical Simulation for MDI-QKD**

In this section, we will present some numerical simulations to comparing our results with the results obtained by using 3-intensity decoy state method for MDI-QKD [26]. As discussed before, we know that the methods presented in this paper does not only apply to the weak coherent sources (WCS). Actually, it can be used to estimate the final key rate for any sources that satisfy the condition given by Eqs. (24-25). Below for simplicity, we consider the following two cases. In the first case, we suppose that Alice and Bob use the WCS. In the second one, we suppose they use the heralded single-photon sources (HSPS) with poisson distributions [23]. The UTP locates 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 the linear models as in [5, 18, 29]:

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

where $\xi^k$ is the transmittance for a distance from Alice to the UTP. For fair comparison, we use the same...
and error rates $\xi$ of UTP have the same detection efficiency $\eta$. Assume all detectors of Alice and Bob have the same detection efficiency $\eta$. We assume all detectors of Alice and Bob have the same detection efficiency $\eta_i$ 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 $\eta_i$ and dark count rate $p_d$. The values of these parameters are presented in Table II. With this, taking the photon-number-cutoff approximation up to 6 photon-number state, the total gains $S_{\mu_1, \nu_1}^\omega (\omega = X, Z)$ and error rates $S_{\mu_1, \nu_1}^{\omega, E_{\mu_1, \nu_1}} (\omega = X, Z)$ of Alice’s intensity $\mu_1 (i = 0, 1, 2$ for 3-intensity method, $i = 0, 1, 2, 3$ for 4-intensity method) and Bob’s intensity $\nu_1 (j = 0, 1, 2$ for 3-intensity method, $j = 0, 1, 2, 3$ for 4-intensity method) can be calculated. By using these values, we can estimate the lower bounds of yield $s_{11}^\omega$ with Eq.(30) and Eq.(32) for 3-intensity and 4-intensity decoy state methods respectively. Also, we can estimate the upper bounds of error rate $e_{11}^\omega$ with Eq.(33) and Eq.(34) for these two decoy state methods respectively. Furthermore, with these parameters, we can estimate the final key rate $R$ of this protocol with Eq.(20). If we fix the densities of the decoy-state sources used by Alice and Bob, the final key rate will change with they taking different intensities for their signal-state pulses. Here, in order to make a rational and effective comparison, we set the intensities of the decoy source in 3-intensity method and the first decoy source in 4-intensity method are the same and $\mu_1 = \nu_1 = 0.1$; let the intensity of the second decoy source in 4-intensity method to be the optimal intensity of signal source in 3-intensity method and assume $\mu_2 = \nu_2 > \mu_1$.

With these preparations, we can conclude that the lower bounds of $s_{11}$ estimated by using the 3-intensity and 4-intensity decoy state methods are the same, i.e., $s_{11}^{\omega} = s_{11}^{\omega}$. In Fig.7, we plot the upper bound of $e_{11}$ with different methods. The optimal key rates with different methods for WCS and HSPS are shown in the up and down subfigures respectively in Fig.7. To see more clearly, in Fig.8 we plot the relative value between the optimal key rate obtained with different methods and the asymptotic limit of the infinite decoy-state method. In order to clarify the superiority of the 4-intensity decoy state method, we plot the ratio of the optimal key rate between the results obtained by using 4-intensity and 3-intensity decoy state methods in Fig.7. These figures clearly show that our results are better than the pre-existed results. The optimal densities with the optimal key rate versus the total channel transmission loss is given in Fig.7. In Fig.7 and Fig.6, the black dotted line and green dash-dot line are the results obtained by using 3-intensity decoy state method with WCS and HSPS respectively, the blue dashed line and the red solid line are the results obtained by using 4-intensity decoy state method with HSPS and HSPS respectively, the thick cyan line are the results obtained by using infinite decoy state method. In Fig.7 and Fig.8, the green dotted, the red dashed and the cyan solid lines are the results obtained by using 4-intensity and 3-intensity decoy state methods in Fig.7. These figures clearly show that our results are better than the pre-existed results. The optimal densities with the optimal key rate versus the total channel transmission loss is given in Fig.8. In Fig.8 and Fig.6, the black dotted line and green dash-dot line are the results obtained by using 3-intensity decoy state method with WCS and HSPS respectively, the blue dashed line and the red solid line are the results obtained by using 4-intensity decoy state method with HSPS and HSPS respectively, the thick cyan line are the results obtained by using infinite decoy state method. In Fig.7 and Fig.8, the green dotted, the red dashed and the cyan solid lines are the results obtained by using 3-intensity, 4-intensity and the infinite decoy state methods respectively. In Fig.7, the blue dashed lines are obtained with WCS, the red solid lines are obtained with HSPS.

**IV. CONCLUDING REMARK**

In conclusion, we show how to tightly formulate the upper bound of the phase-flip errors in decoy state method for the regular BB84 protocol and MDI-QKD. Our result compressed the bound to about a quarter of known result for MDI-QKD with WCS, and even about one fifth with...
HSPS. To achieve the result, we only need 4-intensity decoy state method. These methods can be applied to the recently proposed protocols with imperfect single-photon source such as the coherent states or the heralded states recently proposed protocols with imperfect single-photon in the domain $m > n \geq 1$.

Acknowledgement: We acknowledge the 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.

Appendix A. Eqs. (78122425) with the imperfect sources used in practice

We know that the state emits from a parametric downconversion (PDC) source is [17,18]
\[
\rho_{v} = \sum_{k} |a_{k}^{v}|^{2} |k\rangle\langle k|,
\]
with $a_{k}^{v} = e^{-|k|/l} / k!$ or $a_{k}^{v} = \sqrt{l/(l+1)} / k!$ where $|k\rangle$ represents a $k$-photon state, $l$ is the intensity (average photon number) of $\rho_{v}$. Firstly, in this appendix, we will prove that the assumptions given by Eqs. (7812) are satisfied by the PDC source. In the 4-intensity protocol, Alice has 3 different no-vacuum sources which are denoted by $\rho_{x}, \rho_{y}, \rho_{z}$ with $0 < x < y < z$.

In the case with $a_{k} = e^{-|k|/l} / k!$, we have
\[
a_{k}^{x} = e^{-x} x^{k} / k!, \quad a_{k}^{y} = e^{y-x} y^{k} / k!, \quad (k \geq 0).
\]

Then we can easily prove the conclusions in Eqs. (78) with $x < y < z$. In order to prove the result presented in Eq. (12), we need the following lemma.

Lemma 1. For any two natural number $m, n$ with $m > n \geq 1$, $F(v) = \frac{v^{m}}{1-v^{n}}$ is a monotone increasing function in the domain $v \in (0,1)$.

The function $F(v) = \frac{v^{m}}{1-v^{n}}$ can be rewritten into
\[
F(v) = \frac{\sum_{k=0}^{m-1} v^{k}}{\sum_{k=0}^{m-1} v^{k}} = 1 + v^{m-1} \sum_{k=0}^{m-n-1} v^{k} = 1 + \frac{\sum_{k=0}^{m-n-1} v^{k}}{1/1^{k}}.
\]

This predicts that the function $F(v)$ is monotone increasing with $m > n \geq 1$ in the domain $v \in (0,1)$.

With the definition of $G(i,j,k)$ in Eq. (13), we have
\[
e^{x+y-2z} G(i, j, k)
= [x^{i} - x^{j}] [y^{i} - y^{j}] - [y^{i} - y^{j}] [x^{i} - x^{j}]
= x^{i} y^{j} [1 - x^{i}] [1 - y^{j}] - y^{i} x^{j} [1 - y^{j}] [1 - x^{i}]
\]

with $x_{r} = x / z$ and $y_{r} = y / z$. If $x < y < z$, and $k > j - i > 0$, we get
\[
x^{i} y^{j} = \frac{x^{i} y^{j}}{z^{i} z^{j}} = \frac{y^{i} z^{j}}{x^{j}} \geq 1,
\]

and
\[
(1 - x^{i}) (1 - y^{j}) - (1 - y^{j}) (1 - x^{i})
= (1 - x^{i}) (1 - y^{j}) \left(\frac{1 - y^{j}}{1 - y^{j}} - \frac{1 - x^{i}}{1 - x^{i}}\right) \geq 0.
\]

In the last step, we have used Lemma 1. With these relations, we can finish the proof of Eq. (12).

In the case with $a_{k} = \sqrt{l/(l+1)} / k!$, we have
\[
a_{k}^{y} = \frac{x + 1}{y + 1} \left(\frac{xy + x}{xy + y}\right)^{k}, \quad a_{k}^{z} = \frac{y + 1}{z + 1} \left(\frac{yz + z}{yz + y}\right)^{k},
\]

for all $k \geq 1$. Then we can easily prove the conclusions in Eqs. (78) with $x < y < z$. By introducing
\[
\tilde{x}_{r} = \frac{x + x}{z + z}, \quad \tilde{y}_{r} = \frac{y + y}{z + z},
\]

we find out
\[
\frac{(1 + x)(1 + y)}{(1 + z)^{2}} \sum_{i} \sum_{j} \sum_{k} a_{i}^{x} a_{j}^{y} a_{k}^{z} x^{i} y^{j} z^{k} G(i, j, k)
= \frac{[x^{i} - y^{j}] [y^{i} - y^{k}] - [y^{i} - y^{j}] [x^{i} - x^{k}]}{[1 - y^{j}] [1 - y^{k}] - [1 - x^{j}] [1 - x^{k}]},
\]

If $x < y < z$, with Lemma 1, we can prove that $G(i, j, k) \geq 0$ when $k - j \geq j - i \geq 0$. This complete the proof of Eq. (12).

Similarly, we can prove that those assumptions in Eqs. (7812) can be fulfilled by the heralded single-photon sources (HSPS) with possion or thermal distributions [23]. When we consider the 4-intensity decay state method for MDI-QKD, the assumptions presented in Eqs. (2425) can be fulfilled if Alice and Bob choose PDC sources or HSPS.

Appendix B. The derivation of the simplified forms of $s_{1}$ and $s_{11}$

As discussed in section III the lower bound of $s_{1}$ can be estimated by Eq. (10) when Alice use three different sources $\rho_{o}, \rho_{x}, \rho_{y}$ and $\rho_{z}$. Furthermore, in this case, we can write $s_{1}$ into the following form with $s_{1}(x, y)$
\[
s_{1} = s_{1}(x, y) + \sum_{m \geq 3} f_{s_{1}}(x, y)(m)s_{1},
\]

where
\[
f_{s_{1}}(m) = \frac{a_{x}^{y} a_{y}^{x} - a_{x}^{y} a_{x}^{y}}{a_{x}^{x} a_{y}^{y} - a_{x}^{x} a_{x}^{y}}, \quad (m \geq 3).
\]

Similarly, if Alice choose sources $\rho_{o}, \rho_{x}, \rho_{z}$ and $\rho_{o}, \rho_{y}, \rho_{z}$, then $s_{1}$ can also be expressed into
\[
s_{1} = s_{1}(x, z) + \sum_{m \geq 3} f_{s_{1}}(x, z)(m)s_{1},
\]

and
\[
s_{1} = s_{1}(y, z) + \sum_{m \geq 3} f_{s_{1}}(y, z)(m)s_{1},
\]
respectively. By calculation, we have
\[
f_{x,z}(m) = \frac{a_x^2 a_m^2 - a_y^2 a_m^2}{a_y^2 a_m^2 - a_z^2 a_m^2}, \quad f_{y,z}(m) = \frac{a_y^2 a_m^2 - a_z^2 a_m^2}{a_y^2 a_m^2 - a_z^2 a_m^2},
\]
for all \( m \geq 3 \). So we have
\[
s_1(x, y) \geq s_4(x, z) \geq s_3(y, z).
\]
This completes the proof of Eq. (13).

Now we commit to prove Eq. (32) for MDI-QKD. By choosing any two different no-vacuum sources \( \rho_{x_A(y_B)} \) form \( \rho_{x_A(y_B)} \), \( \rho_{y_A(x_B)} \), \( \rho_{z_A(x_B)} \), we have
\[
s_{11} = s_{11}(l, r) + \sum_{(m, n) \in J_1} f_{s_{11}}^{(l, r)}(m, n) s_{mn},
\]
with \( s_{11}(l, r) \) being defined in Eq. (30) by replacing \( x, y \) with \( l, r \) respectively, and
\[
f_{s_{11}}^{(l, r)}(m, n) = \frac{a_x^2 b_l^2 a_y^2 a_m^2 - a_y^2 b_l^2 a_z^2 a_m^2}{a_y^2 b_l^2 a_z^2 a_m^2 - a_z^2 b_l^2 a_y^2 a_m^2} G(1, 2, m) + \frac{a_y^2 b_l^2 a_z^2 a_m^2 - a_z^2 b_l^2 a_y^2 a_m^2}{a_z^2 b_l^2 a_y^2 a_m^2 - a_y^2 b_l^2 a_z^2 a_m^2} G(1, 2, m),
\]
for all \( m \geq 3 \). Secondly, we obtain
\[
f_{s_{11}}^{(x,y)}(m, n) = \frac{-a_x^2 a_y^2 a_m^2 G(1, 2, n)}{a_y^2 a_m^2 - a_z^2 a_m^2},
\]
for all \( m \geq 3 \). In the last case, we get
\[
f_{s_{11}}^{(x,y)}(m, n) = \frac{-a_y^2 a_z^2 a_m^2 G(1, 2, n)}{a_z^2 a_m^2 - a_y^2 a_m^2},
\]
for all \( m, n \geq 2 \). In the last inequality, we have used the assumption presented in Eq. (24). With these relations, we can conclude that
\[
f_{s_{11}}^{(x,y)}(m, n) \leq f_{s_{11}}^{(x,z)}(m, n) \leq f_{s_{11}}^{(y,z)}(m, n),
\]
for any \( (m, n) \in J_1 \) under the conditions in Eqs. (24)-(26). This completes the proof of Eq. (32).

[1] C.H. Bennett and G. Brassard, in Proc. of IEEE Int. Conf. on Computers, Systems, and Signal Processing (IEEE, New York, 1984), pp. 175-179.
[2] N. Gisin, G. Ribordy, W. Tittel, et al., Rev. Mod. Phys. 74, 145 (2002); N. Gisin and R. Thew, Nature Photonics, 1, 165 (2006); M. Dusek, N. Lütkenhaus, M. Hendrych, in Progress in Optics VVIX, edited by E. Wolf (Elsevier, 2006); V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, et al., Rev. Mod. Phys. 81, 1301 (2009).

[3] H. Inamori, N. Lütkenhaus, and D. Mayers, European Physical Journal D, 41, 599 (2007), which appeared in the arXiv as quant-ph/0107017. D. Gottesman, H.K. Lo, N. Lütkenhaus, 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); X.-B. Wang, 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, et al., Phys. Rev. A 72, 012326 (2005).

[7] Y. Adachi, T. Yamamoto, M. Koashi, et al., Phys. Rev. Lett. 99, 180503 (2007).

[8] M. Hayashi, Phys. Rev. A 74, 022307 (2006); ibid 76, 012329 (2007).

[9] D. Rosenberg, J.W. Harrington, P.R. Rice, et al., Phys. Rev. Lett. 98, 010503 (2007); T. Schmitt-Manderbach, H. Weier, M. Rüst, et al., Phys. Rev. Lett. 98, 010504 (2007); C.-Z. Peng, J. Zhang, D. Yang, et al. Phys. Rev. Lett. 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, et al., Phys. Rev. Lett. 96, 070502 (2006); Y. Zhao, B. Qi, X. Ma, 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, et al., Phys. Rev. A 77, 042311 (2008); J.-Z. Hu and X.-B. Wang, Phys. Rev. A, 82, 012331(2010).

[11] X.-B. Wang, T. Hiroshima, A. Tomita, et al., Physics Reports 448, 1(2007).

[12] X.-B. Wang, L. Yang, C.-Z. Peng, et al., New J. Phys. 11, 075006 (2009).

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

[14] B. Huttner, N. Imoto, N. Gisin, et al., 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, L. Mai, A. Lamas-Linares, et al., Nature Commun. 2, 349 (2011).

[16] D. Mayers and A. C.-C. Yao, in Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS98) (IEEE Computer Society, Washington, DC, 1998), p. 503; A. Acin, N. Brunner, N. Gisin, et al., Phys. Rev. Lett. 98, 230501 (2007); V. Scarani, and R. Renner, Phys. Rev. Lett. 100, 302008 (2008); V. Scarani, and R. Renner, in 3rd Workshop on Theory of Quantum Computation, Communication and Cryptography (TQC 2008), (University of Tokyo, Tokyo 30 JanC1 Feb 2008) See also arXiv:0806.0120

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

[18] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett., 108,130503(2012), K. Tamaki, H.-K. Lo, C.-H. F. Fung, et al., Phys. Rev. A, 85, 042307 (2012).

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

[20] A. Rubenok, J. A. Slater, P. Chan, et al., 1304.2463v1.

[21] P. Chan, J. A. Slater, I. LUCIO-MARTINEZ, et al., arXiv:1204.0738v1.

[22] Y. Liu, T.-Y. Chen, L.-J. Wang, et al., arXiv:1209.0178v1.

[23] Q. Wang and X.-B. Wang, Phys. Rev. A, 88, 052332 (2013).

[24] F. Xu, M. Curty, B. Qi, et al., arXiv:1306.5814v1.

[25] M. Curty et al, arXiv:1307.1081v1.

[26] Z.-W. Yu, Y.-H. Zhou, and X.-B. Wang, arXiv:1308.5677v1.

[27] Z.-W. Yu, Y.-H. Zhou, and X.-B. Wang, arXiv:1309.0471v1.

[28] Z.-W. Yu, Y.-H. Zhou, and X.-B. Wang, arXiv:1309.5886v1.

[29] Q. Wang, and X.-B. Wang, arXiv:1311.1739v1.

[30] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, et al., Nat. Phys. 3, 481 (2007).

[31] In the simulations, we set the intensity of the second decoy source in 4-intensity method to be the optimal intensity of signal source in 3-intensity method. In such setting, the key rate of 3-intensity protocol is optimized given the intensity of the weak coherent state to be 0.1 but the key rate of 4-intensity protocol is not optimized. We make such an unfair comparison only in order to clearly demonstrate the advantage of our tightened estimation in the 4-intensity protocol. It is worth to note that, we can actually further improve the key rate of the 4-intensity protocol by taking some weaker intensities for the decoy sources. For example, if we take $\mu_1 = 0.1, \mu_2 = 0.15$ the key rate can be further improved about 10 percent.