Practical decoy-state measurement-device-independent quantum key distribution

Shi-Hai Sun,[1,*] Ming Gao,[2] Chun-Yan Li,[1] and Lin-Mei Liang[1,3,†]

[1]*Department of Physics, National University of Defense Technology, Changsha 410073, People's Republic of China*

[2]*State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450002, People's Republic of China*

[3]*State Key Laboratory of High Performance Computing, National University of Defense Technology, Changsha 410073, People's Republic of China*

(Received 18 March 2013; published 29 May 2013)

Measurement-device-independent quantum key distribution (MDI-QKD) is immune to all the detection attacks; thus when it is combined with the decoy-state method, the final key is unconditionally secure, even if a practical weak coherent source is used by Alice and Bob. However, until now, the analysis of decoy-state MDI-QKD with a weak coherent source is incomplete. In this paper, we derive, with only vacuum + weak decoy state, some tight formulas to estimate the lower bound of yield and the upper bound of error rate for the fraction of signals in which both Alice and Bob send a single-photon pulse to the untrusted third party Charlie. The numerical simulations show that our method with only vacuum + weak decoy state can asymptotically approach the theoretical limit of the infinite number of decoy states. Furthermore, the statistical fluctuation due to the finite length of date is also considered based on the standard statistical analysis.

DOI: 10.1103/PhysRevA.87.052329 PACS number(s): 03.67.Hk, 03.67.Dd

I. INTRODUCTION

Quantum key distribution (QKD), such as the BB84 protocol [1], admits two remote parties, known as Alice and Bob, to share an unconditional security key, which is guaranteed by the quantum mechanics and has been proved in theory [2–4]. However, the setups used in the practical system are imperfect, which will leave some loopholes for Eve to spy the secret key. In fact, some potential quantum hacking strategies have been discovered by exploiting the imperfection of practical setups, such as the passive Faraday mirror attack [5], blinding attack [6], time-shift attack [7], and so on [8–10]. Therefore, the legitimate parties must carefully reexamine their practical system to close all the loopholes, when they use this system in practical situations.

In order to close the gap between the theory and practice, some approaches have been proposed. The first one is trying to characterize the practical system fully and considered all the side channels existing in the practical system. Although some potential loopholes have been discovered and then closed by using this approach, it cannot find all the loopholes existing in the practical system, since, theoretically speaking, the number of loopholes is infinite. The second approach is trying to establish the full device-independent (DI-) QKD system [11,12]. The DI-QKD can guarantee the unconditional security of the practical system without knowing the detailed information of the practical setups of Alice and Bob. However, this approach is impractical within current technology, since it requires that the legitimate parties have single-photon detectors with near unit detection efficiency.

Instead of full DI-QKD, recently Lo *et al.* proposed a scheme called measurement-device-independent (MDI-) QKD [13], in which both Alice and Bob send a pulse to an untrusted third party, called Charlie. Charlie performs the Bell state measurement (BSM) and tells her results to Alice and Bob; then Alice and Bob can use this information to distill a secret key. Since the detection party can be fully controlled by the eavesdropper (Eve), this scheme is immune to all the detector attacks. Thus the legitimate parties just need to ensure that the source is secret; then the total QKD system is secret. In fact, this condition can be satisfied in practical situations, since the source is relatively simple and can be fully characterized.

Although the MDI-QKD has been demonstrated in experiments [14,15], and some modified schemes for a fiber-based system have been proposed [16,17], it is not completely device independent. It requires that the source of Alice and Bob is perfect; for example, the pulse sent by Alice and Bob should be a single-photon state. However, within current technology, the weak coherent state is often used due to the lack of a feasible single-photon source, which will send multiphoton pulses with nonzero probability and suffer from the photon-number-splitting attack [18,19]. Luckily, the same problem is also faced for the regular BB84 protocol with the weak coherent state, and the decoy-state method [20–23] has been proposed to efficiently estimate the contribution of a single-photon pulse. Thus the decoy-state method can also be introduced to the MDI-QKD to close the loophole of the multiphoton pulses.

However, the analysis for the decoy-state MDI-QKD is different from the regular decoy-state QKD for the regular BB84 protocol [20–23]. Recently, the security of the decoy-state MDI-QKD has been considered by many researchers [13,16,24–26]. However, there still exists some disadvantages for their results. In Ref. [13], Lo *et al.* analyze the security of decoy-state MDI-QKD assuming infinitely long data and infinitely many decoy states, which are impractical due to the limited resource in practical situations. In Refs. [16,24,25], the authors considered the effect of the finite-size data and a finite number of decoy states, but their analysis has two disadvantages: first, the authors estimate the contribution of single-photon pulses by solving the nonlinear minimization problem, but not giving general formulas liking the regular decoy state QKD; second, four states (vacuum + two-weak decoy state) are needed to close the asymptotic limit of

*shsun@nudt.edu.cn

†nmliang@nudt.edu.cn

infinitely decoy states. Furthermore, we will show that, in the following, our method can perform better than the method of Ma's [24], and the key rate estimated by our method is larger than that of Ma's method. In Ref. [26], Wang presents general formulas for the decoy state MDI-QKD with three intensity states (vacuum + weak decoy state), but their formulas are very relaxant, and no secret key can be generated when these formulas are applied. Therefore, a more stringent security bound and the general theory of decoy state MDI-QKD is imperative.

In this paper, we discuss the decoy state MDI-QKD with vacuum + weak decoy state, in which both Alice and Bob use three kinds of states with different intensity (one signal state, one decoy state, and one vacuum state). Then we derive general formulas to estimate the yield Y_{11} and error rate e_{11} for the fraction of signals in which both Alice and Bob send a single-photon pulse to Charlie. The numerical simulations show that our formulas are very tight, and our vacuum + weak decoy-state method asymptotically approaches the theoretical limit of the infinite decoy-state method.

II. PROTOCOL

In this paper, we consider the following decoy state MDI-QKD protocol [13,16,24].

(1) Alice randomly generates three kinds of pulses with different intensity: the signal state with a intensity μ_2, the decoy state with a intensity μ_1, and the vacuum state with a intensity $\mu_0 \equiv 0$. Without loss of generality, we assume that $\mu_2 > \mu_1 > 0$. For each pulse, Alice randomly chooses her basis from $\{x,z\}$ and bit from $\{0,1\}$. Then she modulates her information on each pulse and sends it to Charlie, which can be fully controlled by Eve. At the same time, Bob performs the same processing as Alice, and the intensities of Bob's pulse are noted as ν_2, ν_1, and $\nu_0 \equiv 0$ ($\nu_2 > \nu_1 > 0$) for signal state, decoy state, and vacuum state, respectively.

(2) Charlie performs BSM, and tells her measurement results to Alice and Bob through a public channel. Then Alice and Bob compare their basis for each pulse. If they use the same basis and Charlie has a successional BSM event, they keep this bit as a raw key.

(3) For each case that Alice's intensity is μ_i, Bob's intensity is ν_j, and the basis is $\omega = x,z$, Alice and Bob estimate the parameters of channel, including the total gain $Q^{\omega}_{\mu_i\nu_j}$, the total error rate $E^{\omega}_{\mu_i\nu_j}$, and the yield (error rate) of both Alice and Bob send a single-photon pulse, noted as Y^{ω}_{11} (e^{ω}_{11}). With these parameters, Alice and Bob can estimate the final key rate, which is given by [13,24]

$$R \geqslant \mu_2\nu_2 e^{-\mu_2-\nu_2} Y^z_{11}\left[1 - H\left(e^x_{11}\right)\right] - Q^z_{\mu_2\nu_2} f H\left(E^z_{\mu_2\nu_2}\right), \quad (1)$$

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. Note that $Q^z_{\mu_2\nu_2}$ and $E^z_{\mu_2\nu_2}$ are directly measured in experiment; thus Alice and Bob need to estimate the lower bound of Y^z_{11} and upper bound of e^x_{11} to maximize her key rate. The main contribution of this paper is that we give two tight formulas to estimate Y^z_{11} and e^x_{11} with only vacuum + decoy state. Here we assume that only the signal states of Alice and Bob, μ_2 and ν_2, are used to distill the secret key. The decoy states are used to estimate the parameters of channel.

Note that, when the phase of pulse sent by Alice and Bob is totally randomized, the quantum channel can be considered as a photon-number channel model [21,24], and the state of Alice and Bob is $\rho_\mu = \sum_{n=0}^{\infty} \frac{\mu^n}{n!} e^{-\mu} |n\rangle\langle n|$, where $\mu = \{\mu_i,\nu_j | i,j = 0,1,2\}$. Thus the total gain and error rate of Alice's intensity μ_i and Bob's intensity ν_j can be written as [24]

$$\begin{aligned} Q^{\omega}_{\mu_i\nu_j} &= \sum_{n,m=0}^{\infty} \frac{\mu_i^n \nu_j^m}{n!m!} e^{-\mu_i-\nu_j} Y^{\omega}_{nm}, \\ E^{\omega}_{\mu_i\nu_j} Q^{\omega}_{\mu_i\nu_j} &= \sum_{n,m=0}^{\infty} \frac{\mu_i^n \nu_j^m}{n!m!} e^{-\mu_i-\nu_j} Y^{\omega}_{nm} e^{\omega}_{nm}, \end{aligned} \quad (2)$$

where Y^{ω}_{nm} (e^{ω}_{nm}) is the yield (error rate) when Alice sends n-photon pulse, Bob sends m-photon pulse, and the basis ω is used by them. Obviously, according to Eq. (2), if infinite decoy states are used, Alice and Bob can exactly obtain Y^z_{11} and e^x_{11}. However, the resource is finite in practical situations; thus only a finite decoy state can be used by the legitimate parties. In the following, we give two tight formulas to bound these parameters, which are the main contributions of this paper. The numerical simulations show that our formulas with only vacuum + weak decoy state can asymptotically approach the theoretical limit of infinite decoy states.

III. LOWER BOUND OF Y^{ω}_{11}

Note that the expression of Eq. (2) is independent on ω; thus when there is no ambiguity, we neglect the superscript ω in the following of this paper. Then the total gain $Q_{\mu_i\nu_j}$ can be written as

$$\begin{aligned} e^{\mu_i+\nu_j} Q_{\mu_i\nu_j} &= \sum_{n,m=0}^{\infty} \frac{\mu_i^n \nu_j^m}{n!m!} Y_{nm} \\ &= \sum_{m=0}^{\infty} \frac{\nu_j^m}{m!} Y_{0m} + \mu_i \left(Y_{10} + \nu_j Y_{11} + \sum_{m=2}^{\infty} \frac{\nu_j^m}{m!} Y_{1m} \right) \\ &\quad + \sum_{n=2}^{\infty} \frac{\mu_i^n}{n!} \left(Y_{n0} + \nu_j Y_{n1} + \sum_{m=2}^{\infty} \frac{\nu_j^m}{m!} Y_{nm} \right) \\ &= e^{\nu_j} Q_{0\nu_j} + e^{\mu_i} Q_{\mu_i 0} - Q_{00} + \mu_i\nu_j Y_{11} \\ &\quad + h(\mu_i,\nu_j), \end{aligned} \quad (3)$$

where

$$h(\mu_i,\nu_j) = \sum_{m=2}^{\infty} \frac{\mu_i \nu_j^m}{m!} Y_{1m} + \sum_{n=2}^{\infty} \frac{\mu_i^n \nu_j}{n!} Y_{n1} + \sum_{n,m=2}^{\infty} \frac{\mu_i^n \nu_j^m}{n!m!} Y_{nm}. \quad (4)$$

Thus we will have

$$\begin{aligned} &e^{\mu_2+\nu_2} Q_{\mu_2\nu_2} - e^{\mu_1+\nu_1} Q_{\mu_1\nu_1} \\ &= g_1 + (\mu_2\nu_2 - \mu_1\nu_1) Y_{11} + \sum_{m=2}^{\infty} \frac{\mu_2\nu_2^m - \mu_1\nu_1^m}{m!} Y_{1m} \\ &\quad + \sum_{n=2}^{\infty} \frac{\mu_2^n\nu_2 - \mu_1^n\nu_1}{n!} Y_{n1} + \sum_{n,m=2}^{\infty} \frac{\mu_2^n\nu_2^m - \mu_1^n\nu_1^m}{n!m!} Y_{nm} \end{aligned}$$

$$\begin{aligned}
&\geqslant g_1+(\mu_2\nu_2-\mu_1\nu_1)Y_{11}+a\sum_{m=2}^{\infty}\frac{\mu_2\nu_1^m+\mu_1\nu_2^m}{m!}Y_{1m}\\
&\quad+b\sum_{n=2}^{\infty}\frac{\mu_2^n\nu_1+\mu_1^n\nu_2}{n!}Y_{n1}+c\sum_{n,m=2}^{\infty}\frac{\mu_2^n\nu_1^m+\mu_1^n\nu_2^m}{n!m!}Y_{nm}\\
&\geqslant g_1+(\mu_2\nu_2-\mu_1\nu_1)Y_{11}+\alpha[h(\mu_2,\nu_1)+h(\mu_1,\nu_2)]\\
&=g_1+g_2+g_3-(\mu_1\nu_1-\mu_2\nu_2+\alpha\mu_2\nu_1+\alpha\mu_1\nu_2)Y_{11},
\end{aligned}\tag{5}$$

where we use the fact that for any $n,m\geqslant 2$, the following inequalities always hold, which are given by

$$\begin{aligned}
\frac{\mu_2\nu_2^m-\mu_1\nu_1^m}{\mu_2\nu_1^m+\mu_1\nu_2^m}&\geqslant\frac{\mu_2\nu_2^2-\mu_1\nu_1^2}{\mu_2\nu_1^2+\mu_1\nu_2^2}\equiv a\geqslant 0,\\
\frac{\mu_2^n\nu_2-\mu_1^n\nu_1}{\mu_2^n\nu_1+\mu_1^n\nu_2}&\geqslant\frac{\mu_2^2\nu_2-\mu_1^2\nu_1}{\mu_2^2\nu_1+\mu_1^2\nu_2}\equiv b\geqslant 0,\\
\frac{\mu_2^n\nu_2^m-\mu_1^n\nu_1^m}{\mu_2^n\nu_1^m+\mu_1^n\nu_2^m}&\geqslant\frac{\mu_2^2\nu_2^2-\mu_1^2\nu_1^2}{\mu_2^2\nu_1^2+\mu_1^2\nu_2^2}\equiv c\geqslant 0,
\end{aligned}\tag{6}$$

and $\alpha=\min\{a,b,c\}$. Here g_1, g_2, and g_3 are defined as

$$\begin{aligned}
g_1&=e^{\nu_2}Q_{0\nu_2}+e^{\mu_2}Q_{\mu_20}-e^{\nu_1}Q_{0\nu_1}-e^{\mu_1}Q_{\mu_10},\\
g_2&=\alpha\left(e^{\mu_2+\nu_1}Q_{\mu_2\nu_1}-e^{\nu_1}Q_{0\nu_1}-e^{\mu_2}Q_{\mu_20}+Q_{00}\right),\\
g_3&=\alpha\left(e^{\mu_1+\nu_2}Q_{\mu_1\nu_2}-e^{\nu_2}Q_{0\nu_2}-e^{\mu_1}Q_{\mu_10}+Q_{00}\right).
\end{aligned}\tag{7}$$

It is easy to check that for any α, $\mu_1\nu_1-\mu_2\nu_2+\alpha\mu_2\nu_1+\alpha\mu_1\nu_2>0$ always holds. Also, note that the expressions of equations from (3) to (7) are the same for both the z basis and x basis. Thus the lower bound of Y_{11}^{ω} is given by

$$Y_{11}^{\omega}\geqslant\underline{Y_{11}^{\omega}}\equiv\frac{g_1^{\omega}+g_2^{\omega}+g_3^{\omega}-e^{\mu_2+\nu_2}Q_{\mu_2\nu_2}^{\omega}+e^{\mu_1+\nu_1}Q_{\mu_1\nu_1}^{\omega}}{\mu_1\nu_1-\mu_2\nu_2+\alpha\mu_2\nu_1+\alpha\mu_1\nu_2}.\tag{8}$$

where $\omega=z,x$.

IV. UPPER BOUND OF e_{11}^{ω}

According to Eqs. (2) and (3), we have

$$e^{\mu_1+\nu_1}Q_{\mu_1\nu_1}E_{\mu_1\nu_1}=g_4+\mu_1\nu_1Y_{11}e_{11}+h'(\mu_1,\nu_1),\tag{9}$$

where

$$\begin{aligned}
g_4&=e^{\nu_1}Q_{0\nu_1}E_{0\nu_1}+e^{\mu_1}Q_{\mu_10}E_{\mu_10}-Q_{00}E_{00},\\
h'(\mu_1,\nu_1)&=\sum_{m=2}^{\infty}\frac{\mu_1\nu_1^m}{m!}Y_{1m}e_{1m}+\sum_{n=2}^{\infty}\frac{\mu_1^n\nu_1}{n!}Y_{n1}e_{n1}\\
&\quad+\sum_{n,m=2}^{\infty}\frac{\mu_1^n\nu_1^m}{n!m!}Y_{nm}e_{nm}.
\end{aligned}\tag{10}$$

Obviously, $h'(\mu_1,\nu_1)\geqslant 0$; thus the upper bound of e_{11}^{ω} can be written as

$$e_{11}^{\omega}\leqslant\overline{e_{11}^{\omega}}\equiv\frac{e^{\mu_1+\nu_1}Q_{\mu_1\nu_1}^{\omega}E_{\mu_1\nu_1}^{\omega}-g_4^{\omega}}{\mu_1\nu_1\underline{Y_{11}^{\omega}}},\tag{11}$$

where $\omega=z,x$, and $\underline{Y_{11}^{\omega}}$ and g_4 are given by Eqs. (8) and (10), respectively.

V. NUMERICAL SIMULATION

Note that, when Eve is absent, the total gains and error rates of Alice's intensity μ_i and Bob's intensity ν_j are given by [16,24]

$$\begin{aligned}
Q_{\mu_i\nu_j}^{x}&=2y^2[1+2y^2-4yI_0(s)+I_0(2s)],\\
Q_{\mu_i\nu_j}^{x}E_{\mu_i\nu_j}^{x}&=e_0Q_{\mu_i\nu_j}^{x}-2(e_0-e_d)y^2[I_0(2s)-1],\\
Q_{\mu_i\nu_j}^{z}&=Q_C+Q_E,\\
Q_{\mu_i\nu_j}^{z}E_{\mu_i\nu_j}^{z}&=e_dQ_C+(1-e_d)Q_E,
\end{aligned}\tag{12}$$

where

$$\begin{aligned}
Q_C&=2(1-P_d)^2e^{-\mu'/2}[1-(1-P_d)e^{-\eta_a\mu_i/2}]\\
&\quad\times[1-(1-P_d)e^{-\eta_b\nu_j/2}],\\
Q_E&=2P_d(1-P_d)^2e^{-\mu'/2}[I_0(2s)-(1-P_d)e^{-\mu'/2}],
\end{aligned}\tag{13}$$

$I_0(s)$ is the modified Bessel function of the first kind, e_d is the misalignment-error probability, $e_0=1/2$ is the error rate of background, P_d is the dark count of a single-photon detector, η_a (η_b) is the transmission of Alice (Bob), and $\mu'=\eta_a\mu_i+\eta_b\nu_j$, $s=\sqrt{\eta_a\mu_i\eta_b\nu_j}/2$, and $y=(1-P_d)e^{\mu'/4}$.

Submitting Eq. (12) into Eqs. (8) and (11), we can estimate the lower bound of yield Y_{11}^{z} and upper bound of error rate e_{11}^{x} when both Alice and Bob send a single-photon state. The estimated parameters of Y_{11} and e_{11} are shown in Figs. 1(b) and 1(c), respectively, which clearly shows that our vacuum + weak decoy-state method is very close to the asymptotic limit of the infinite decoy-state method. Then,

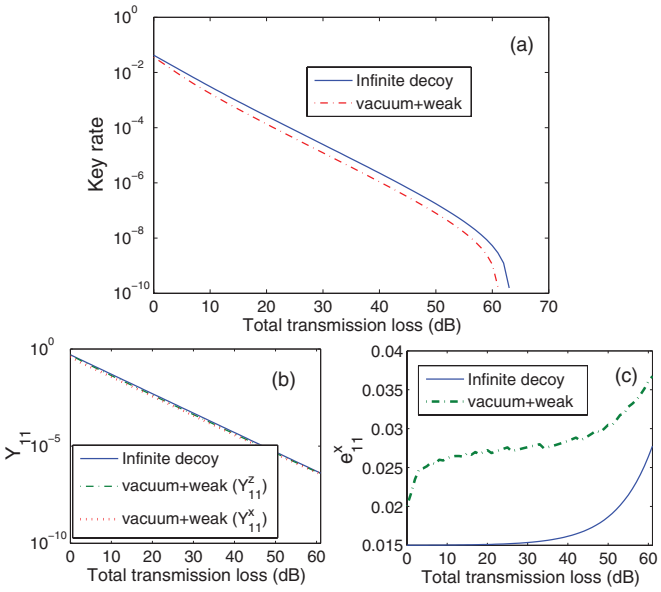

FIG. 1. (Color online) Key rate of decoy-state MDI-QKD. The solid line is obtained for the infinite decoy-state method, in which the exact Y_{11}^{z} and e_{11}^{x} are known. The dot-dashed line is obtained for our vacuum + weak decoy-state method, in which the lower bond of Y_{11}^{z} and the upper bound of e_{11}^{x} are given by Eqs. (8) and (11), respectively. The key rate is maximized by optimizing the intensity of pulse, which is shown in Fig. 2. The same parameters as Ref. [24] are used in our simulations, which are $e_d=1.5\%$, $P_d=3\times10^{-6}$, and $f=1.16$.

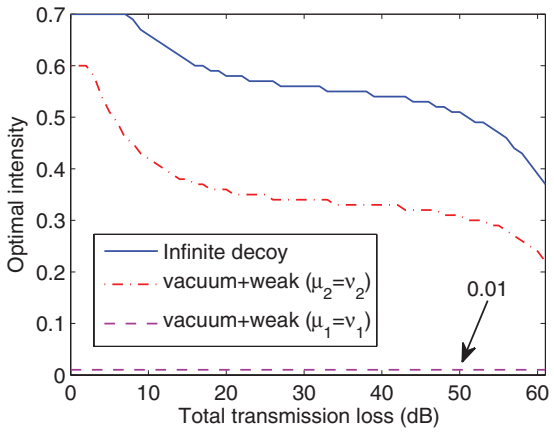

FIG. 2. (Color online) Optimal intensity for signal state and decoy state to maximize the key rate. The optimal intensity is obtained by researching the intensity of signal state (μ_2 and ν_2) and decoy state (μ_1 and ν_1) from 0.01 to 0.6 with a step 0.01. In the simulations, we assume that $\eta_a = \eta_b$, $\mu_2 = \nu_2$, and $\mu_1 = \nu_1$. Other parameters are the same as Fig. 1.

with these parameters, we can estimate the key rate, which is shown in Fig. 1(a). It clearly shows that the key rate with our method is also very close to the asymptotic limit of the infinite decoy-state method. Note that the key rate is maximized by optimizing the intensity of the signal state and the decoy state. The optimal intensity for our method and infinite decoy-state method are shown in Fig. 2. It shows clearly that the optimal signal intensity is the order of $O(1)$, which is the same as the regular decoy state.

Furthermore, our method can perform better than the method proposed by Ma *et al.* [24], which estimated the contribution of the single-photon state, Y_{11}^z and e_{11}^x, by solving the nonlinear minimization problem. The results are listed in Table I. It clearly shows that the key rate estimated by our method is larger than that of Ma's method.

VI. STATISTICAL FLUCTUATION

In practical situations, the length of the raw key is also finite, which will induce statistical fluctuation for the parameter estimation. In this section, we considered the effect of finite length of the raw key based on the standard statistical analysis [23,24], in which the lower bound and upper bound of

TABLE I. Comparison between our method and Ma's method. We assume that $\eta_a = \eta_b = 0.1$. Here we directly take the results of Ma's method from Ref. [24].

Parameters	Our method ($\mu_2 = \nu_2 = 0.36$)	Ma's method with vacuum + weak ($\mu_2 = \nu_2 = 0.5$)
Y_{11}^z	4.1967×10^{-3}	4.6043×10^{-3}
e_{11}^x	2.7241%	10.2126%
R	1.3548×10^{-4}	6.8877×10^{-5}

experimental results, $Q^{\omega}_{\mu_i\nu_j}$ and $E^{\omega}_{\mu_i\nu_j}$, are given by

$$\begin{aligned} \underline{Q^{\omega}_{\mu_i\nu_j}} \leqslant Q^{\omega}_{\mu_i\nu_j} \leqslant \overline{Q^{\omega}_{\mu_i\nu_j}}, \\ \underline{Q^{\omega}_{\mu_i\nu_j}E^{\omega}_{\mu_i\nu_j}} \leqslant Q^{\omega}_{\mu_i\nu_j}E^{\omega}_{\mu_i\nu_j} \leqslant \overline{Q^{\omega}_{\mu_i\nu_j}E^{\omega}_{\mu_i\nu_j}}, \end{aligned} \tag{14}$$

where $\underline{Q^{\omega}_{\mu_i\nu_j}} = Q^{\omega}_{\mu_i\nu_j}(1-\beta_q)$, $\overline{Q^{\omega}_{\mu_i\nu_j}} = Q^{\omega}_{\mu_i\nu_j}(1+\beta_q)$, $\underline{Q^{\omega}_{\mu_i\nu_j}E^{\omega}_{\mu_i\nu_j}} = Q^{\omega}_{\mu_i\nu_j}E^{\omega}_{\mu_i\nu_j}(1-\beta_{eq})$, $\overline{Q^{\omega}_{\mu_i\nu_j}E^{\omega}_{\mu_i\nu_j}} = Q^{\omega}_{\mu_i\nu_j}E^{\omega}_{\mu_i\nu_j}(1+\beta_{eq})$, and $\beta_q = n_\alpha/\sqrt{N^{\omega}_{\mu_i\nu_j}Q^{\omega}_{\mu_i\nu_j}}$, $\beta_{eq} = n_\alpha/\sqrt{N^{\omega}_{\mu_i\nu_j}Q^{\omega}_{\mu_i\nu_j}E^{\omega}_{\mu_i\nu_j}}$. Here $N^{\omega}_{\mu_i\nu_j}$ is the length of pulse of Alice's intensity μ_i, Bob's intensity ν_j, and ω basis. n_α is the standard deviation, which is related to the failure probability of the security analysis. For example, if $n_\alpha = 5$, the failure probability is 5.73×10^{-7} [24]. Thus the lower bound of Y_{11}^{ω} and upper bound of e_{11}^{ω}, which are given by Eqs. (8) and (11), should be rewritten as

$$\begin{aligned} Y_{11}^{\omega} \geqslant \underline{\underline{Y_{11}^{\omega}}} &\equiv \frac{\underline{g_1^{\omega}} + \underline{g_2^{\omega}} + \underline{g_3^{\omega}} - e^{\mu_2+\nu_2}\overline{Q^{\omega}_{\mu_2\nu_2}} + e^{\mu_1+\nu_1}\underline{\underline{Q^{\omega}_{\mu_1\nu_1}}}}{\mu_1\nu_1 - \mu_2\nu_2 + \alpha\mu_2\nu_1 + \alpha\mu_1\nu_2}, \\ e_{11}^{\omega} \leqslant \overline{\overline{e_{11}^{\omega}}} &\equiv \frac{e^{\mu_1+\nu_1}\overline{Q^{\omega}_{\mu_1\nu_1}E^{\omega}_{\mu_1\nu_1}} - \underline{g_4^{\omega}}}{\mu_1\nu_1\underline{\underline{Y_{11}^{\omega}}}}, \end{aligned} \tag{15}$$

where $\underline{g_k^{\omega}}(k = 1,2,3)$ and $\underline{g_4^{\omega}}$ are given by Eqs. (7) and (10).

Submitting the equations above into Eq. (1), we can estimate the secret key rate with a finite length of data, which is shown in Fig. 3. It clearly shows that the finite length of the raw key will obviously compromise the secret key rate. In the simulations, we assume the standard deviation is $n_\alpha = 5$ and the length of data is the same for each pair of intensities of Alice and Bob.

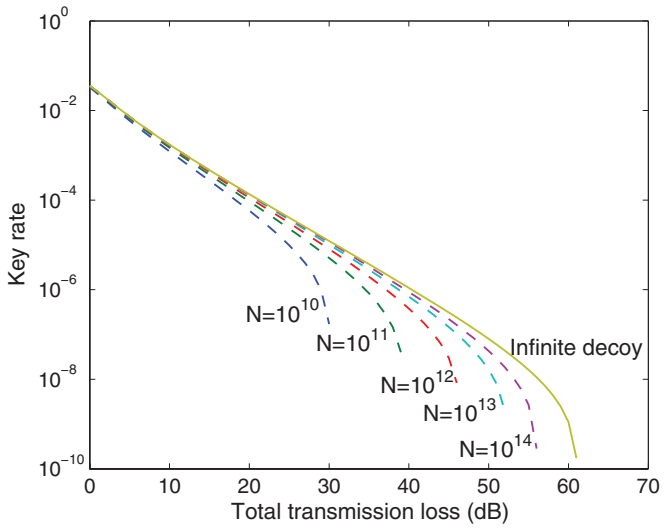

FIG. 3. (Color online) Key rate of decoy-state MDI-QKD with statistical fluctuation. The solid line is obtained for the infinite decoy-state method with infinite length of data. The dashed lines are obtained for our vacuum + weak decoy state with different length of data. In the simulations, we assume that five standard deviations ($n_\alpha = 5$) are used. N is the length of data.

VII. CONCLUSIONS

The MDI-QKD can exclude all the detection loopholes in practical situations, and when it is combined with the decoy-state method, the final key generated by the MDI-QKD is unconditional security; even the practical weak coherent sources are used by Alice and Bob. However, the security of decoy-state MDI-QKD is incomplete. In this paper, we discuss the decoy-state MDI-QKD with vacuum + weak decoy state, in which both Alice and Bob use three kinds of state with different intensity (one signal state, one decoy state, and one vacuum state). Then we derive general formulas to estimate the yield and error rate for the fraction of signals in which both Alice and Bob send a single-photon pulse to Charlie. The numerical simulations show that our formulas are very tight, and our method with the vacuum + weak decoy-state method asymptotically approaches the theoretical limit of the general decoy-state method (with an infinite number of decoy states).

ACKNOWLEDGMENTS

This work is supported by the National Natural Science Foundation of China, Grants No. 61072071, No. 11204377, and No. U1204602. L.M.L. is supported by the Program for NCET. M.G. is supported by National High-Tech Program of China, Grant No. 2011AA010803. S.H.S. is supported by the Fund of Innovation, Graduate School of NUDT, Grant No. B100203.

[1] C. H. Bennett and G. Brassard, *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
[2] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[3] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[4] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).
[5] S.-H. Sun, M.-S. Jiang, and L.-M. Liang, Phys. Rev. A **83**, 062331 (2011).
[6] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photon. **4**, 686 (2010).
[7] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H. K. Lo, Phys. Rev. A **78**, 042333 (2008).
[8] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 022320 (2006).
[9] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006).
[10] C.-H. F. Fung, B. Qi, K. Tamaki, and H. K. Lo, Phys. Rev. A **75**, 032314 (2007).
[11] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
[12] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, New J. Phys. **11**, 045021 (2009).
[13] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[14] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, arXiv:1204.0738.
[15] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang *et al.*, arXiv:1209.6178.
[16] X.-F. Ma and M. Razavi, Phys. Rev. A **86**, 062319 (2012).
[17] K. Tamaki, H. K. Lo, C.-H. F. Fung, and B. Qi, Phys. Rev. A **85**, 042307 (2012).
[18] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).
[19] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[20] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[21] H.-K. Lo, X.-F. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[22] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[23] X.-F. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).
[24] X. Ma, C.-H. F. Fung, and M. Razavi, Phys. Rev. A **86**, 052305 (2012).
[25] T.-T. Song, Q.-Y. Wen, F.-Z. Guo, and X. Q. Tan, Phys. Rev. A **86**, 022332 (2012).
[26] X.-B. Wang, arXiv:1207.0392.