Quantum Inf Process (2016) 15:3799–3813
DOI 10.1007/s11128-016-1371-3

The enhanced measurement-device-independent quantum key distribution with two-intensity decoy states

Jian-Rong Zhu[1,2] · Feng Zhu[1,2] · Xing-Yu Zhou[1,2] · Qin Wang[1,2,3]

Received: 21 February 2016 / Accepted: 15 June 2016 / Published online: 28 June 2016

Abstract We put forward a new scheme for implementing the measurement-device-independent quantum key distribution (QKD) with weak coherent source, while using only two different intensities. In the new scheme, we insert a beam splitter and a local detector at both Alice's and Bob's side, and then all the triggering and non-triggering signals could be employed to process parameter estimations, resulting in very precise estimations for the two-single-photon contributions. Besides, we compare its behavior with two other often used methods, i.e., the conventional standard three-intensity decoy-state measurement-device-independent QKD and the passive measurement-device-independent QKD. Through numerical simulations, we demonstrate that our new approach can exhibit outstanding characteristics not only in the secure transmission distance, but also in the final key generation rate.

Keywords Quantum key distribution · Decoy state · Weak coherent light

1 Introduction

In the past few decades, the quantum key distribution (QKD) has attracted extensive attention from the scientific world, which is mainly attributed to its theoretical uncon-

✉ Qin Wang
qinw@njupt.edu.cn

1 Institute of Signal Processing Transmission, Nanjing University of Posts and Telecommunications, Nanjing 210003, China

2 Key Lab of Broadband Wireless Communication and Sensor Network Technology, Nanjing University of Posts and Telecommunications, Ministry of Education, Nanjing 210003, China

3 Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China

ditional security ensured by laws of quantum mechanics [1–3]. But unfortunately, practical legitimate users, usually named Alice and Bob, can only possess imperfect devices, e.g., non-ideal single-photon sources, imperfect single-photon detectors and lossy channels. Then a malicious eavesdropper, Eve, who might own the most advance computational power and technology, can carry out corresponding attacks by making use of the loopholes due to imperfections [4–10]. In order to countermeasure the so-called photon-number-splitting (PNS) attack [4–6], the decoy-state method was created [11–16]. Moreover, the measurement-device-independent quantum key distribution (MDI-QKD) [17,18] has been invented to defeat the more powerful side-channel attacks [7–10]. Hitherto, under current technology the MDI-QKD seems to possess the highest level security among different protocols.

Recently, different schemes of MDI-QKD have been widely studied both theoretically and experimentally. For example, some apply different number of decoy states [19,20], and others employ either weak coherent states (WCS) [20–22] or heralded single-photon sources (HSPS) [23–25]. However, for those schemes applying decoy states with one, two or three intensities, the performance is poorer than the asymptotic case of using infinite number of decoy states. In this paper, we propose a new method of the decoy-state MDI-QKD that uses a weak coherent source. Although it only needs two intensities, it offers better performance compared with most other existing MDI-QKD methods, e.g., the standard three-intensity decoy-state MDI-QKD and the passive decoy-state MDI-QKD.

Our paper is organized as follows: In Sect. 2, we introduce some basic notations for the configuration of our QKD setups and then describe our new proposed two-intensity decoy-state MDI-QKD step by step. In Sect. 3, we derive a formula giving the lower bound of the counting rate and the upper bound of quantum-bit error rate (QBER) from the two-single-photon pulses. In Sect. 4, we present the corresponding numerical simulations and compare our new proposal with other existing schemes, e.g., the standard three-intensity decoy-state MDI-QKD and the passive MDI-QKD. In Sect. 5, we analyze the finite data size effect in practical implementations. In Sect. 6, a summary and conclusions are given.

2 The new proposed MDI-QKD with two-intensity weak coherent light

Before describing our new two-intensity MDI-QKD protocol, let us first briefly review the local triggering setup [26]. As is illustrated in Fig. 1, denote the two input states of the beam splitter (BS) as ρ and σ (Fock diagonal states) , where t is the transmittance of the BS. The two Fock diagonal states (ρ and σ) can be expressed as:

$$\rho = \sum_{n=0}^{\infty} p_n \left|n\right\rangle \left\langle n\right|, \qquad \sigma = \sum_{n=0}^{\infty} r_n \left|n\right\rangle \left\langle n\right|. \tag{1}$$

If we properly select the above two input modes, then we can get a classical correlation between the two outcome signals, which means we can get different photon-number statistics in the signal mode a by conditional detecting the signal in mode b. Here we suppose that the Fock states in the two input ports are both weak coherent

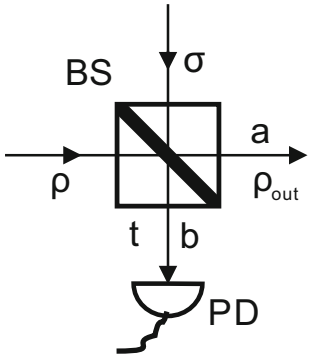

Fig. 1 Local triggering setup: ρ and σ (two states which are diagonal in the Fock basis) represent the two input states of a beam splitter (BS); t is the transmittance of the BS; the two output modes of the BS are denoted as a and b, respectively; ρ_{out} represents the output state from mode **a**, *PD* the single-photon detector

sources (WCS), which are generated by attenuated lasers. Hence, they can be written as:

$$\rho = e^{-\mu_1} \sum_{n=0}^{\infty} \frac{{\mu_1}^n}{n!} |n\rangle \langle n|, \qquad \sigma = e^{-\mu_2} \sum_{n=0}^{\infty} \frac{{\mu_2}^n}{n!} |n\rangle \langle n|, \tag{2}$$

where μ_1 and μ_2 are the average photon numbers of the two input signals, respectively. The expression for $p_{n,m}$, which is the joint probability of having n photons in mode a and m photons in output mode b, can be expressed:

$$p_{n,m} = \frac{\nu^{n+m} e^{\nu}}{n!m!} \frac{1}{2\pi} \int_0^{2\pi} \gamma(\theta)^n (1 - \gamma(\theta))^m \mathrm{d}\theta. \tag{3}$$

The parameters ν, $\gamma(\theta)$, and ζ are defined as follows:

$$\nu = \mu_1 + \mu_2, \tag{4}$$

$$\gamma(\theta) = \frac{\mu_1 t + \mu_2(1-t) + \zeta \cos\theta}{\nu}, \tag{5}$$

$$\zeta = 2\sqrt{\mu_1 \mu_2 (1-t) t}. \tag{6}$$

Here the parameter t means the transmittance of a beam splitter. If Alice does not consider the measurement result in mode b, then the probability of having n photons in mode a can be given as:

$$p_n(\nu) = \sum_{m=0}^{\infty} p_{n,m} = \frac{\nu^n}{n!} \frac{1}{2\pi} \int_0^{2\pi} \gamma(\theta)^n e^{-\nu\gamma(\theta)} \mathrm{d}\theta. \tag{7}$$

When considering the detection results of Alice, the joint probability for finding n photons in mode a and no click in Alice's threshold photon detector can be denoted as $p_n^{\bar{t}}$. We can express it as:

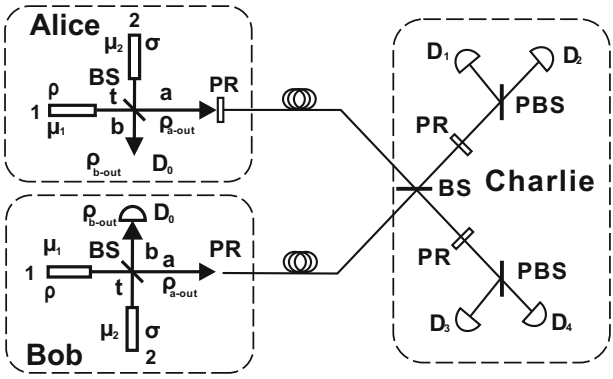

Fig. 2 Schematic setup of the new two-intensity decoy-state MDI-QKD. At Alice (Bob)'s side, ρ and σ interfere at a BS with a transmittance t. μ_i $(i = 1, 2)$ corresponds to the intensity of the input light; a and b each denotes one of the output modes; D_0 represents the local threshold single-photon detector, with a detection efficiency η_A (η_B) at Alice's (Bob's) side. At the UTP's (Charlie's) side, pulses from Alice and Bob interfere at a 50:50 BS and then each enters a polarizing beam splitter (PBS); D_i $(i = 1, 2, 3, 4)$ represents the single-photon detector, with a detection efficiency η_C; PR represents a polarization rotator

$$\begin{aligned} \bar{p_n^t}(\nu) &= (1-\varepsilon)\sum_{m=0}^{\infty}(1-\eta_A)^m p_{n,m} \\ &= (1-\varepsilon)\frac{\nu^n e^{-\eta_A \nu}}{n!}\frac{1}{2\pi}\int_0^{2\pi}\gamma(\theta)^n e^{-(1-\eta_A)\nu\gamma(\theta)}\mathrm{d}\theta. \end{aligned} \tag{8}$$

Here ε refers to the dark count rate and η_A is the detection efficiency of Alice's threshold detector. In the same way, we can denote another parameter p_n^t, which represents the probability of having n photons in mode a and observing a click in Alice's threshold detector at the same time. We finally get the following expression:

$$p_n^t(\nu) = p_n(\nu) - \bar{p_n^t}(\nu). \tag{9}$$

In our new protocol, both Alice and Bob possess this kind of BS devices, separately sending out optical pulses to the untrusted third part (UTP), named Charlie. Charlie who may be controlled by Eve applies a joint measurement on the two-pulse signals from both Alice and Bob and publicly announces the measurement results after all signal transmission is finished. The schematic of our experimental setup is shown in Fig. 2.

Now let us describe our new proposal step by step by using a polarization coding scheme as an example:

First, both Alice and Bob randomly modulate their pulses in input 1 into two different intensities, μ and μ', and interfere it with the local reference beam from input 2 at a BS. The two output modes are denoted as mode a and mode b, respectively. Mode b is used for detection with the local detector (D_0); Mode a is randomly encoded into one of the four polarization states, i.e., horizontal (H), vertical (V), 45° (+) and

135° (−) polarizations, and sent out to the UTP. Meantime, Alice (Bob) sends out a triggering signal whenever D_0 clicks.

Second, the UTP carries out partial Bell-state projection measurements on the pulses from Alice and Bob, recording all the successful events. Besides, the UTP classifies all the successful events into two species, the *triggered* and the *non-triggered*. After all the signal transmission finished, the UTP publicly announces his measurement results.

Third, based on the UTP's announcement, Alice (Bob) applies post-selection and bit-flip operations on the qubits in her (his) hand, obtaining the raw key.

Fifth, Alice and Bob carry out error correction and a privacy amplification processes to achieve the final key.

It is worth noting that the main differences between our new scheme and the old passive QKD schemes are the following: At both Alice and Bob's side, light in input 2 (σ) is fixed with intensity μ_2, and light in input 1 (ρ) is randomly modulated into two different intensities, μ and μ' ($\mu < \mu'$), where μ refers to the decoy state and μ' represents the signal state. According to Eq. (4), for each μ and μ', we have corresponding ν and ν , with $\nu = \mu + \mu_2$, and $\nu' = \mu' + \mu_2$ individually. Moreover, we also have relevant values for p_n, $p_n^{\bar{t}}$ and p_n^t for each μ and μ'. That is to say, by modulating light (in input 1) into μ and μ', we can obtain six types of nonzero counting events. By properly choosing two of them, i.e., $p_n^t(\nu)$ and $p_n(\nu')$, we can denote them as c and $c^{'}$, respectively. Then in the photon-number space, we have

$$\rho_l = \sum_n l_n |n\rangle \langle n|, \quad (l = c, c^{'}) \tag{10}$$

where

$$\begin{aligned} c_n(\mu_i) &= p_n(\nu_i) - p_n^{\bar{t}}(\nu_i), \\ c_n^{'}(\mu_i') &= p_n(\nu_i'), \end{aligned} \tag{11}$$

with $i = A, B$.

In order to analyze our new scheme, we firstly assume the following condition holds true for any $\mu^{'} \geq \mu$ and $n \geqslant 2$ [19]:

$$\frac{c_n^{'}(\mu^{'})}{c_n(\mu)} \geq \frac{c_{n-1}^{'}(\mu^{'})}{c_{n-1}(\mu)} \geq \frac{c_1^{'}(\mu^{'})}{c_1(\mu)}. \tag{12}$$

This assumption will be readdressed later on.

3 Derivation of Y_{11}^L and e_{11}^U

In order to calculate the final key generation rate, the counting rate and the QBER of the two-single-photon pluses should first be estimated. Here Alice and Bob randomly modulate their pulses in input 1 into μ_i and μ_i', ($\mu_i < \mu_i', i = A, B$), individually. For simplicity, we denote the intensity from Alice or Bob as x and y, respectively, where

$x \in \{\mu_A, \mu'_A\}$ and $y \in \{\mu_B, \mu'_B\}$. Then we can calculate the average gain ($S^W_{x,y}$) and average quantum-bit error ($T^W_{x,y} =: E^W_{x,y} S^W_{x,y}$) with the following expressions:

$$S^W_{x,y} = \sum_{m,n=0}^{\infty} l_n(x) l_m(y) Y^W_{nm}, \tag{13}$$

$$E^W_{x,y} S^W_{x,y} = \sum_{m,n=0}^{\infty} l_n(x) l_m(y) e^W_{nm} Y^W_{nm}, \tag{14}$$

where W represents the X or Z basis; $l = c, c'$; Y^W_{nm} and e^W_{nm} each corresponds to the yield and the QBER when Alice sends out an n-photon pulse and Bob sends out an m-photon pulse; $E^W_{x,y}$ is the average QBER. In the MDI-QKD, two bases (Z and X) have been used for preparing, transmitting and measuring. Usually the Z basis is used for distilling the secure keys, while the X basis is only for error testing. For simplicity, we suppose the MDI-QKD has been implemented with the two bases independently. Hereafter, the superscript W will be omitted without causing any confusion.

With Eq. (13), $S_{\mu,\mu}$ and $S_{\mu',\mu'}$ can be written as:

$$\begin{aligned} S_{\mu,\mu} = {} & \tilde{S}_{00} + c_1^2(\mu) Y_{11} + c_1(\mu) \sum_{m=2}^{\infty} c_m(\mu) Y_{1m} \\ & + c_1(\mu) \sum_{n=2}^{\infty} c_n(\mu) Y_{n1} \\ & + \sum_{n,m=2}^{\infty} c_n(\mu) c_m(\mu) Y_{nm}, \end{aligned} \tag{15}$$

$$\begin{aligned} S_{\mu',\mu'} = {} & \tilde{S}'_{00} + c_1^{'2}(\mu') Y_{11} + c'_1(\mu') \sum_{m=2}^{\infty} c'_m(\mu') Y_{1m} \\ & + c'_1(\mu') \sum_{n=2}^{\infty} c'_n(\mu') Y_{n1} \\ & + \sum_{n,m=2}^{\infty} c'_n(\mu') c'_m(\mu') Y_{nm}, \end{aligned} \tag{16}$$

where $\tilde{S}_{00} = S_{\mu,0} + S_{0,\mu} - S_{0,0}$, $\tilde{S}'_{00} = S_{\mu',0} + S_{0,\mu'} - S'_{0,0}$. Denote $\kappa =: \frac{c'_1(\mu') c'_2(\mu')}{c_1(\mu) c_2(\mu)}$. By combining Eqs. (15) and (16), we get

$$Y_{11} = \frac{\kappa (S_{\mu,\mu} - \tilde{S}_{00}) - (S_{\mu',\mu'} - \tilde{S}'_{00}) + \tau}{\kappa c_1^2(\mu) - c_1^{'2}(\mu')}, \tag{17}$$

where

$$\begin{aligned}\tau = &\sum_{m=2}^{\infty}\left[c_1^{'}(\mu')c_m^{'}(\mu') - \kappa c_1(\mu)c_m(\mu)\right]Y_{1m}\\ &+\sum_{n=2}^{\infty}\left[c_1^{'}(\mu')c_n^{'}(\mu') - \kappa c_1(\mu)c_n(\mu)\right]Y_{n1}\\ &+\sum_{n,m=2}^{\infty}\left[c_n^{'}(\mu')c_m^{'}(\mu') - \kappa c_n(\mu)c_m(\mu)\right]Y_{nm}.\end{aligned}$$

Below we denote $\tau = h_1 + h_2 + h_3$. According to Eq. (12), we have $\tau > 0$, which follows from

$$\begin{aligned}h_1 &= \sum_{m=2}^{\infty}\left[c_1^{'}(\mu')c_m^{'}(\mu') - \kappa c_1(\mu)c_m(\mu)\right]Y_{1m}\\ &= \sum_{m=2}^{\infty}\frac{c_1^{'}(\mu')}{c_2(\mu)}\left[c_2(\mu)c_m^{'}(\mu') - c_2^{'}(\mu')c_m(\mu)\right]Y_{1m} \geq 0;\\ h_2 &= \sum_{n=2}^{\infty}\left[c_1^{'}(\mu')c_n^{'}(\mu') - \kappa c_1(\mu)c_n(\mu)\right]Y_{n1}\\ &= \sum_{n=2}^{\infty}\frac{c_1^{'}(\mu')}{c_2(\mu)}\left[c_2(\mu)c_n^{'}(\mu') - c_2^{'}(\mu')c_n(\mu)\right]Y_{n1} \geq 0;\\ h_3 &= \sum_{m,n=2}^{\infty}\left[c_n^{'}(\mu')c_m^{'}(\mu') - \kappa c_n(\mu)c_m(\mu)\right]Y_{nm}\\ &\geq \sum_{m,n=2}^{\infty}\frac{c_n(\mu)c_m^{'}(\mu')}{c_1(\mu)c_2(\mu)}\left[c_1(\mu)c_2^{'}(\mu') - c_1^{'}(\mu')c_2(\mu)\right]Y_{nm} \geq 0.\end{aligned}$$

With the conditions above, we can get the lower bound for the two-single-photon counting rate in the Z basis (Y_{11}^{Z}):

$$Y_{11}^{Z} \geq \mathrm{Y}_{11}^{Z,L} := \frac{c_1{}'(\mu')c_2{}'(\mu')(S_{\mu,\mu}^{Z} - \tilde{S}_{00}^{Z}) - c_1(\mu)c_2(\mu)(S_{\mu',\mu'}^{Z} - \widetilde{S}_{00}^{Z\,\prime})}{c_1{}'(\mu')c_1(\mu)\left[c_1(\mu)c_2{}'(\mu') - c_1{}'(\mu')c_2(\mu)\right]}. \quad (18)$$

Similarly, we can get the upper bound of the QBER for two-single-photon pulses in the X basis (e_{11}^{X}):

$$e_{11}^{X} \leq \mathrm{e}_{11}^{X,U} := \frac{E_{\mu,\mu}^{X}S_{\mu,\mu}^{X} - E_{\mu,0}^{X}S_{\mu,0}^{X} - E_{0,\mu}^{X}S_{0,\mu}^{X} + E_{0,0}^{X}S_{0,0}^{X}}{c_1^2(\mu)Y_{11}^{X}}. \quad (19)$$

With the formulae above, we can now calculate the final key generation rate with [18,24]:

$$R \geq c_1^{'2}(\mu')Y_{11}^Z[1 - H_2(e_{11}^X)] - S_{\mu',\mu'}^Z f H_2(E_{\mu',\mu'}^Z), \tag{20}$$

where f is a factor for the cost of error correction efficiency, and here we take $f = 1.16$. $H_2(x)$ is the binary Shannon information function, given by $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$.

4 Numerical simulation for MDI-QKD

We can now numerically calculate the key generation rate and compare the performance of our method with other schemes, e.g., the passive MDI-QKD and the three-intensity MDI-QKD. Here we assume that the UTP is located in the middle of Alice's and Bob's transmission link and that the detectors of the UTP are identical, e.g., have the same dark count rate Y_0 and detection efficiency η_C. Moreover, the detection efficiency η_C does not depend on the incoming signals. The gains and error rates, which can be observed in the experiment, could be estimated with linear model channels. According to the linear model in [24], the state $|n\rangle\langle n|$ from Alice can be changed into $\sum_{k=0}^{n} C_n^k \eta^k (1-\eta)^{n-k} |k\rangle\langle k|$, when it arrives to the UTP. Here C_n^k is the binomial coefficient, defined as $C_n^k =: \frac{n!}{k!(n-k)!}$; η is the transmittance from Alice to the UTP.

Depending on the transmittance distance, we can set the values for $S_{\mu,\mu}$, $S_{\mu',\mu'}$, $E_{\mu,\mu}$ and $E_{\mu',\mu'}$, which probably would be the observed in real experiments. So after setting the values mentioned above, the parameters of Y_{11}^Z and e_{11}^X can be obtained. Furthermore, we can calculate the key generation rate with the formula in Eq. (20).

For a fair comparison, we use the same the numerical parameters as in [18,23], with $\alpha = 0.2$ dB/km, $\eta_C = 0.145$, $d_C = 3 \times 10^{-6}$, $e_d = 0.015$, $\eta_i = 0.75$ and $d_i = 10^{-6}$ ($i = A, B$) in our simulations. Moreover, we use the same value of μ_2 as in [26], $\mu_2 = 10^{-4}$. Then we do a simulation for the two-single-photon contributions (Y_{11} and e_{11}), the optimal intensity for the signal state (μ') and the final key generation rate by using different methods. The corresponding simulation results are shown in Figs. 3, 4 and 5. Here, we need to stress that during our simulation we have numerically checked that all the parameters used can satisfied the conditions in Eq. (12).

In Fig. 3, we compare the estimated values for the counting rate of two-single-photon pulses (Y_{11}) (a) and the QBER of two-single-photon pulses (e_{11}) (b) by using different methods. W_1 and W_3 each represents the passive MDI-QKD (W_1) and the standard three-intensity decoy-state MDI-QKD (W_3), respectively. W_2 corresponds to the new proposed two-intensity MDI-QKD. Moreover, we also plot for the ideal case of using infinite number of decoy states (W_0) (W_0 corresponds to the experimental setup in Fig. 2, and it is the same hereafter). In order to give a fair comparison, at each distance we have used the optimal intensity for the signal state ($\mu^{'}$) in all the above methods and set a reasonable value for the decoy state ($\mu = 0.1$) in both the new proposed two-intensity decoy-state scheme and the standard three-intensity decoy-state method. From Fig. 3a, b, we find that all the three practical schemes (W_1, W_2

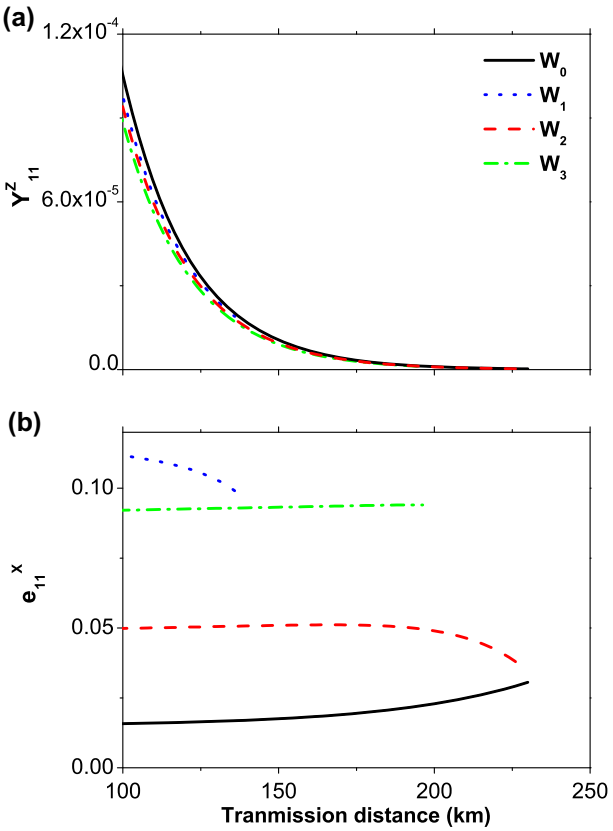

Fig. 3 Comparison for the counting rate (Y_{11}) (**a**) and the quantum-bit error rate (e_{11}) (**b**) from two-single-photon pulses by using different methods, i.e., the passive MDI-QKD (W_1), the standard three-intensity decoy-state MDI-QKD (W_3) and the new proposed two-intensity decoy-state method (W_2). W_0 represents the case of using an infinite number of decoy states. Here we reasonably set $\mu = 0.1$ for the decoy state in both the new proposed two-intensity decoy-state scheme and the standard three-intensity decoy-state method, and in all the schemes we use the optimal intensity for the signal state (μ') at each distance

and W_3) show similar estimation values of Y_{11}, while they show drastically different performance for e_{11}. Obviously, our new proposed two-intensity scheme (W_2) exhibits significantly lower estimation value of e_{11} than the other two.

In Fig. 4, we plot the optimal intensity ($\mu^{'}$) at each distance with different methods. Similar in Fig. 3, W_0 represents the ideal case of using infinite number of decoy states, W_1 and W_3 each corresponds to the result of using the passive decoy-state scheme and the conventional three-intensity decoy-state method, respectively, and W_2 refers to the result of using our new proposal. From Fig. 4, we find that the optimal intensity ($\mu^{'}$) in our new method is much higher than in the other two practical methods (W_1 and W_3), getting much closer to the asymptotic case of using an infinite number of decoy states (W_0).

In Fig. 5a, b, we compare either the absolute key generation rate or the relative key generation rate between using different methods. In Fig. 5a, W_0, W_1 and W_3

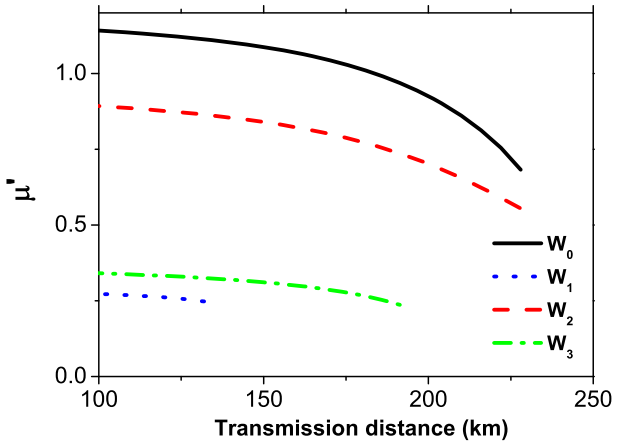

Fig. 4 Comparison of the optimal value of signal state (μ') for MDI-QKD in different methods, i.e., the passive MDI-QKD method with WCS (W_1), the three-intensity MDI-QKD method with WCS (W_3) and the new method proposed by us (W_2). Besides, the *solid curve* (W_0) represents the MDI-QKD method with infinite decoy states

each corresponds to the asymptotic case of using infinite number of decoy states, the passive decoy-state scheme and the conventional decoy-state method. W_2 refers to the result of using our new proposal. Obviously, our new method (W_2) presents a much higher key generation rate than the other two practical methods (W_1 and W_3) and approaches the ideal case of using infinite number of decoy states (W_0) very closely. Moreover, in order to give a vivid comparison between these three practical methods, we plot the ratio of the key generation rate between using our new scheme and other two practical methods (W_1 and W_3) in Fig. 5b. Excitingly, our new proposal exhibits more than two times improvement in the key generation rate than conventional three-intensity decoy-state method at longer distance (>150 km), and more than ten times improvement compared to the passive decoy-state scheme at distances longer than 120 km, see the left axis in Fig. 5b. The improvement is on the one hand due to the relatively high optimal intensity used in our new scheme as shown in Fig. 4, and on the other hand, it is attributed to the more precise estimation on the QBER of single-photon pulses (e_{11}), see Fig. 3b.

5 Statistical fluctuations

In the practical implementation of QKD, Alice and Bob can only send finite number of pulses within reasonable experimental time, which will inevitably induce statistical fluctuation. Below we will account for the finite data size effect in real-life experiments.

As we know, the statistical fluctuation effect can be calculated by applying the deviation theory, e.g., the Chernoff bound [27]. The measurement outcome of the overall gain and the quantum-bit errors in the W basis satisfies

$$N^W_{x,y}\hat{S}^W_{x,y} = N^W_{x,y}S^W_{x,y} + \delta_{x,y}, \tag{21}$$

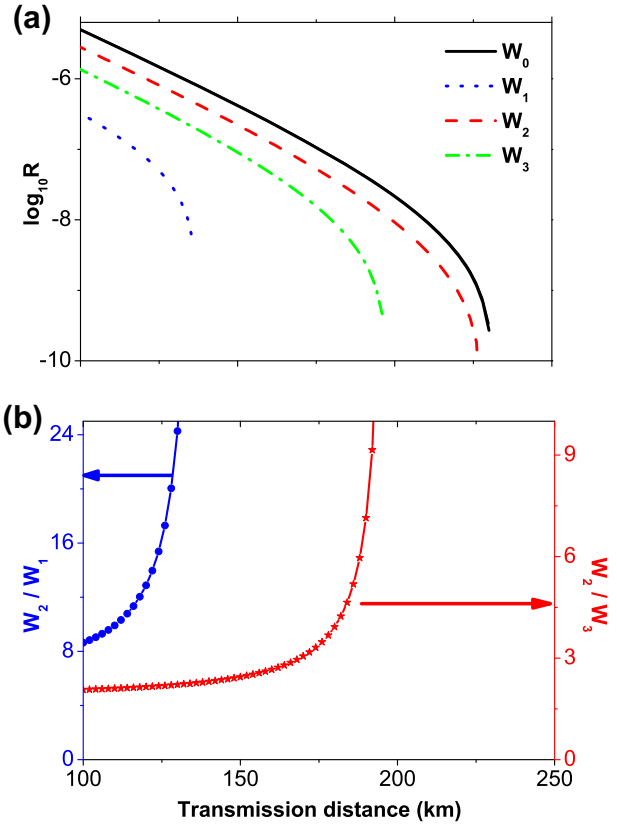

Fig. 5 Comparison of the absolute key generation rate (**a**) and the relative key generation rate (**b**) for MDI-QKD between using different methods. In **a**, from the bottom to the top, each line corresponds to the passive MDI-QKD (W_1), the three-intensity MDI-QKD (W_3), the new proposed two-intensity MDI-QKD (W_2) and the asymptotic case of using infinite decoy states (W_0). In **b**, it shows the ratio of the key generation rates between our new scheme and the passive MDI-QKD method in the *left axis* and displays the ratio of the key generation rates between our scheme and conventional three-intensity decoy state in the *right axis*. Here we reasonably set $\mu = 0.1$ for the decoy state and optimize the value of μ' for the signal state at each distance in all the methods

$$N^W_{x,y}\hat{T}^W_{x,y} = N^W_{x,y}T^W_{x,y} + \widetilde{\delta}_{x,y}, \tag{22}$$

with probability 1-2$\varepsilon_{x,y}$, where $T^W_{x,y} := E^W_{x,y}S^W_{x,y}$, $\delta_{x,y} \in [-\Delta_{x,y}, \hat{\Delta}_{x,y}]$, $\widetilde{\delta}_{x,y} \in [-\Delta_1, \hat{\Delta}_2]$, $\Delta_{x,y} = g(N^W_{x,y}\hat{S}^W_{x,y}, \varepsilon^4_{x,y}/16)$, $\hat{\Delta}_{x,y} = g(N^W_{x,y}\hat{S}^W_{x,y}, \varepsilon^{3/2}_{x,y})$, $\Delta_1 = g(N^W_{x,y}\hat{E}^W_{x,y}\hat{S}^W_{x,y}, \varepsilon^4_{x,y}/16)$, $\Delta_2 = g(N^W_{x,y}\hat{E}^W_{x,y}\hat{S}^W_{x,y}, \varepsilon^{3/2}_{x,y})$ and $g(a,b) = \sqrt{2a\ln(b^{-1})}$. Here $\varepsilon_{x,y}$ denotes the following probabilities: $\Pr(N^W_{x,y}S^W_{x,y} - N^W_{x,y}\hat{S}^W_{x,y} \geq \Delta_{x,y}) \leq \varepsilon_{x,y}$, $\Pr(N^W_{x,y}\hat{S}^W_{x,y} - N^W_{x,y}S^W_{x,y} \geq \hat{\Delta}_{x,y}) \leq \varepsilon_{x,y}$; $\Pr(N^W_{x,y}T^W_{x,y} - N^W_{x,y}\hat{T}^W_{x,y} \geq \Delta_1) \leq \varepsilon_{x,y}$, $\Pr(N^W_{x,y}\hat{T}^W_{x,y} - N^W_{x,y}T^W_{x,y} \geq \Delta_2) \leq \varepsilon_{x,y}$ [27]. $N^W_{x,y}$ is the number of pulses in the W basis, with the intensities of x and y sent by Alice and Bob, respectively.

According to Eq. (21), we have

$$S_{x,y}^{W}-\frac{\Delta_{x,y}}{N_{x,y}^{W}}\leq\hat{S}_{x,y}^{W}\leq S_{x,y}^{W}+\frac{\hat{\Delta}_{x,y}}{N_{x,y}^{W}}. \tag{23}$$

Then we can obtain the following inequalities

$$S_{x,y}^{W}\leq\varsigma\left(S_{x,y}^{W}\right):=\hat{S}_{x,y}^{W}+\frac{\Delta_{x,y}}{N_{x,y}^{W}}, \tag{24}$$

$$S_{x,y}^{W}\geq\widetilde{\varsigma}\left(S_{x,y}^{W}\right):=\hat{S}_{x,y}^{W}-\frac{\hat{\Delta}_{x,y}}{N_{x,y}^{W}}, \tag{25}$$

$$T_{x,y}^{W}\leq\xi\left(T_{x,y}^{W}\right):=\hat{T}_{x,y}^{W}+\frac{\Delta_{1}}{N_{x,y}^{W}}, \tag{26}$$

$$T_{x,y}^{W}\geq\widetilde{\xi}\left(T_{x,y}^{W}\right):=\hat{T}_{x,y}^{W}-\frac{\Delta_{2}}{N_{x,y}^{W}}. \tag{27}$$

According to Eqs. (18), (24) and (25), we obtain

$$Y_{11}^{Z}\geq\mathrm{Y}_{11}^{Z,L}:=\frac{c_{1}{}'(\mu')c_{2}{}'(\mu')\left[\widetilde{\varsigma}\left(S_{\mu,\mu}^{Z}\right)-\varsigma\left(\tilde{S}_{00}^{Z}\right)\right]-c_{1}(\mu)c_{2}(\mu)\left[\varsigma\left(S_{\mu',\mu'}^{Z}\right)-\widetilde{\varsigma}\left(\tilde{S}_{00}^{Z}{}'\right)\right]}{c_{1}{}'(\mu')c_{1}(\mu)\left[c_{1}(\mu)c_{2}{}'(\mu')-c_{1}{}'(\mu')c_{2}(\mu)\right]}. \tag{28}$$

Similarly, we can obtain the modified upper bound of single-photon quantum-bit error rate

$$e_{11}^{X}\leq e_{11}^{X,U}:=\frac{\xi\left(T_{\mu,\mu}^{X}\right)-\widetilde{\xi}\left(T_{\mu,0}^{X}\right)-\widetilde{\xi}\left(T_{0,\mu}^{X}\right)+\xi\left(T_{0,0}^{X}\right)}{c_{1}^{2}\left(\mu\right)Y_{11}^{X,L}}+\Omega\left(N^{Z}Y_{11}^{Z},N^{X}Y_{11}^{X},\varepsilon_{e}\right), \tag{29}$$

where $\Omega\left(a,b,c\right)=\sqrt{(a+1)\ln\left(c^{-1}\right)/[2b\left(a+b\right)]}$. Therefore, Eq. (20) can be modified as:

$$\begin{aligned}R\geqslant&-S_{\mu',\mu'}^{Z}fH_{2}(E_{\mu',\mu}^{Z})+c_{1}{}'(\mu')^{2}Y_{11}^{Z,L}[1-H_{2}(e_{11}^{X,U})]\\&-\tfrac{1}{N_{\mathrm{tol}}}(\log_{2}\tfrac{8}{\epsilon_{\mathrm{cor}}}+2\log_{2}\tfrac{2}{\varepsilon_{1}\varepsilon_{2}}+2\log_{2}\tfrac{1}{2\varepsilon_{\mathrm{PA}}}).\end{aligned} \tag{30}$$

The protocol is ϵ_{sec}-secret and ϵ_{cor}-correct, where $\epsilon_{\mathrm{sec}}=2(2\varepsilon_{e}+\varepsilon_{1}+\varepsilon_{2})+3\varepsilon_{\mu,\mu}+2\varepsilon_{\mu',\mu'}+\varepsilon_{b}+\varepsilon_{\mathrm{PA}}$ [27]. N_{tol} denotes number of total pulses emitted by Alice and Bob. For simplicity, we fix $\epsilon_{\mathrm{sec}}=10^{-10}$, $\epsilon_{\mathrm{cor}}=10^{-15}$ and set each error term to a common value ε , thus ϵ_{sec}=15ε. Besides, we suppose that the length of pulses is the same for each pair of intensities of Alice and Bob. Moreover, we have assumed the number of pulses sent by Alice (or Bob) have the proportion: $N_{\mu'}^{W}:N_{\mu}^{W}=1:1$.

In practical QKD implementation, the data size usually ranges between 10^{12} and 10^{14} [28–30]. We draw out corresponding numerical simulation results for our new proposed two-intensity decoy-state MDI-QKD and the standard three-intensity decoy-state protocols by accounting for statistical fluctuations, see Fig. 6. Obviously, the

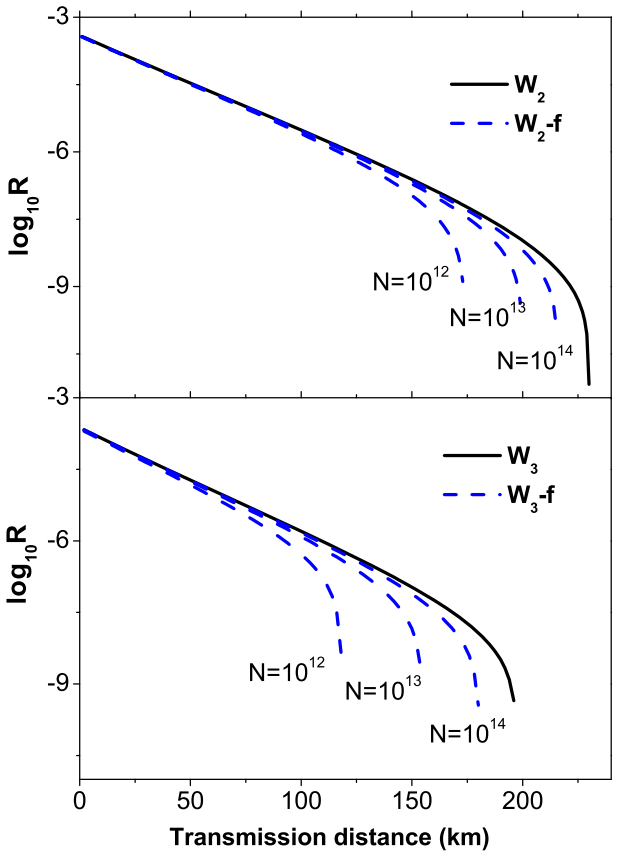

Fig. 6 Key generation rates of MDI-QKD using the new method proposed by us with statistical fluctuation, compared with the finite data case of using the three-intensity MDI-QKD method with WCS . The *black solid curve* W_2 (W_3) refers to the case without statistical fluctuation, and the rest of the curves W_2-f (W_3-f) represent the case when taking statistical fluctuation into account

secure key generation rates will drop down with reducing the total number of pulses. However, it decreases more slowly in our new two-intensity scheme than the three-intensity one, e.g., in our new scheme a quite high key rate can still be obtained at the distance of 170 km with the data size of 10^{12}.

6 Conclusion

In summary, we have presented a practical scheme of implementing two-intensity weak coherent light into the MDI-QKD. In contrast to the conventional three-intensity decoy-state MDI-QKD, in our new proposal we insert a beam splitter and a local detector at both Alice's and Bob's side, and then both the triggering and non-triggering signals could be employed to process parameter estimations. While compared with the original passive decoy-state MDI-QKD, the main differences are: Alice (or Bob)

randomly modulates her (or his) seeding pulses into two different intensities. By combing with both their triggering and non-triggering characteristics, the detection results at Charlie's side could be divided into many different events. Therefore, we could obtain more input parameters and achieve more precise estimations for the two-single-photon contributions.

To analyze our proposal, we carry out corresponding numerical simulations. Our simulation results demonstrate that our new scheme exhibits drastically enhanced performance compared with two other existing methods both in the transmission distance and in the final key generation rate, approaching very closely to the asymptotic case of using infinite number of decoy states. Moreover, even when taking statistical fluctuation into account, our scheme can still give a quite high key generation rate at a long transmission distance (>170 km). In addition, our scheme only needs linear optics and can be easily realized with current technology. Therefore, it may have a promising application in the future of the quantum key distribution.

Acknowledgments We gratefully acknowledge the financial support from the National Natural Science Foundation of China through Grants Nos. 11274178, 61475197 and 61590932, the Natural Science Foundation of the Jiangsu Higher Education Institutions through Grant No. 15KJA120002, the Outstanding Youth Project of Jiangsu Province through Grant No. BK20150039 and the Priority Academic Program Development of Jiangsu Higher Education Institutions through Grant No. YX002001.

References

1. Lo, H.-K., Chau, H.F.: Unconditional security of quantum key distribution over arbitrarily long distances. Science **283**, 2050 (1999)
2. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. **85**, 441 (2000)
3. Mayers, D.: Unconditional security in quantum cryptography. J. ACM **48**, 351 (2001)
4. Brassard, G., Lütkenhaus, N., Mor, T., Sanders, B.C.: Limitations on practical quantum cryptography. Phys. Rev. Lett. **85**, 1330 (2000)
5. Lütkenhaus, N.: Security against individual attacks for realistic quantum key distribution. Phys. Rev. A **61**, 052304 (2000)
6. Lütkenhaus, N., Jahma, M.: Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. New J. Phys. **4**, 44.1 (2002)
7. Makarov, V., Anisimov, A., Skaar, J.: Effects of detector efficiency mismatch on security of quantum cryptosystems. Phys. Rev. A **74**, 022313 (2006)
8. Qi, B., Fung, C.-H.F., Lo, H.-K., et al.: Time-shift attack in practical quantum cryptosystems. Quantum Inf. Comput. **7**, 073 (2007)
9. Fung, C.-H.F., Qi, B., Tamaki, K., Lo, H.-K.: Phase-remapping attack in practical quantum-key-distribution systems. Phys. Rev. A **75**, 032314 (2007)
10. Li, H.-W., Wang, S., Huang, J.-Z.: Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources. Phys. Rev. A **84**, 062308 (2011)
11. Hwang, W.Y.: Quantum key distribution with high loss: toward global secure communication. Phys. Rev. Lett. **91**, 057901 (2003)
12. Wang, X.-B.: Beating the photon-number-splitting attack in practical quantum cryptography. Phys. Rev. Lett. **94**, 230503 (2005)
13. Lo, H.-K., Ma, X.-F., Chen, K.: Decoy state quantum key distribution. Phys. Rev. Lett. **94**, 230504 (2005)
14. Wang, Q., Wang, X.-B., Guo, G.C.: Practical decoy-state method in quantum key distribution with a heralded single-photon source. Phys. Rev. A **75**, 012312 (2007)
15. Wang, Q., Wang, X.-B.: Improved practical decoy state method in quantum key distribution with parametric down-conversion source. Europhys. Lett. **79**, 40001 (2007)

16. Wang, Q., Chen, W., Xavier, G.: Experimental decoy-state quantum key distribution with a sub-poissionian heralded single-photon source. Phys. Rev. Lett. **100**, 090501 (2008)
17. Braunstein, S.L., Pirandola, S.: Side-channel-free quantum key distribution. Phys. Rev. Lett. **108**, 130502 (2012)
18. Lo, H.K., Curty, M., Qi, B.: Measurement-device-independent quantum key distribution. Phys. Rev. Lett. **108**, 130503 (2012)
19. Zhou, Y.-H., Yu, Z.-W., Wang, X.-B.: Tightened estimation can improve the key rate of measurement-device-independent quantum key distribution by more than 100. Phys. Rev. A **89**, 052325 (2014)
20. Wang, X.B.: Measurement-device-independent quantum key distribution. Phys. Rev. A **87**, 012320 (2013)
21. Tamaki, K., Lo, H.-K., Fung, C.-H.F., Qi, B.: Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw. Phys. Rev. A **85**, 042307 (2012)
22. Ma, X., Razavi, M.: Alternative schemes for measurement-device-independent quantum key distribution. Phys. Rev. A **86**, 062319 (2012)
23. Wang, Q., Wang, X.-B.: An efficient implementation of the decoy-state measurement-device-independent quantum key distribution with heralded single-photon sources. Phys. Rev. A **88**, 052332 (2013)
24. Wang, Q., Wang, X.-B.: Simulating of the measurement-device independent quantum key distribution with phase randomized general sources. Sci. Rep. **4**, 04612 (2014)
25. Wang, D., Li, M., Zhu, F., Yin, Z.-Q., Chen, W., Han, Z.-F., Guo, G.-C., Wang, Q.: Quantum key distribution with the single-photon-added coherent source. Phys. Rev. A **90**, 062315 (2014)
26. Curty, M., Ma, X., Qi, B., Moroder, T.: Passive decoy state quantum key distribution with practical light sources. Phys. Rev. A **81**, 022310 (2010)
27. Curty, M., Xu, F., Cui, W., Lim, C.C.W., Tamaki, K., Lo, H.-K.: Finite-key analysis for measurement-device-independent quantum key distribution. Nat. Commun. **5**, 3732 (2014)
28. Tang, Y.L., Yin, H.L., Chen, S.J., Liu, Y., Zhang, W.J., Jiang, X., Zhang, L., Wang, J., You, L.X., Guan, J.Y., Yang, D.X., Wang, Z., Liang, H., Zhang, Z., Zhou, N., Ma, X., Chen, T.Y., Zhang, Q., Pan, J.W.: Measurement-device-independent quantum key distribution over 200 km. Phys. Rev. Lett. **114**, 069901 (2015)
29. Comandar, L.C., Lucamarini, M., Frohlich, B.: Quantum key distribution without detector vulnerabilities using optically seeded lasers. Nat. Photonics **10**, 312C315 (2016)
30. Wang, S., Yin, Z.-Q., Chen, W.: Experimental demonstration of quantum key distribution without monitoring of the signal disturbance. Nat. Photonics **9**, 832C836 (2015)