Efficient implementation of the decoy-state measurement-device-independent quantum key distribution with heralded single-photon sources

Qin Wang[1,*] and Xiang-Bin Wang[2,3,†]

[1]*Institute of Signal Processing and Transmission, Nanjing University of Posts and Telecommunications, Nanjing 210003, China*
[2]*Department of Physics and State Key Laboratory of Low Dimensional Quantum Physics, Tsinghua University, Beijing 100084, China*
[3]*Jinan Institute of Quantum Technology, Shandong Academy of Information Technology, Jinan, China*

(Received 6 June 2013; published 26 November 2013)

We study decoy-state measurement-device-independent quantum key distribution using heralded single-photon sources. This has the advantage that the observed error rate in the X basis is at higher order and not so large. We calculate the key rate and transmission distance for two cases: one using only triggered events, and the other using both triggered and nontriggered events. We compare the key rates of various protocols and find that our scheme using triggered and nontriggered events can give a higher key rate and a longer secure distance. Moreover, we also show the different behavior of our scheme when using different heralded single-photon sources, i.e., in Poisson or thermal distributions. We demonstrate that the former can generate a higher secure key rate than the latter and can thus work more efficiently in practical quantum key distributions.

DOI: 10.1103/PhysRevA.88.052332 PACS number(s): 03.67.Dd, 42.50.Ct, 78.67.Hc, 78.47.D−

I. INTRODUCTION

It is well known that quantum key distribution (QKD) stands out compared with conventional cryptography due to its unconditional security based on the laws of physics. It allows two legitimate users, say Alice and Bob, to share secret keys even in the present of a malicious eavesdropper Eve. But its security proofs often contain certain assumptions either about the sources or about the detection systems, and usually practical setups have imperfections. Therefore, the in-principle unconditional security can actually conflict with realistic implementations, and the imperfections might be exploited by Eve to hack the system [1–4].

In order to achieve the final goal of unconditional security in practice, different approaches have been proposed, such as the decoy-state method [5–9], device-independent quantum key distribution (DI-QKD) [10,11] and recently measurement-device-independent quantum key distribution (MDI-QKD) [12,13]. Among them, decoy-state MDI-QKD seems to be a promising candidate considering its lower technical demands.

Decoy-state MDI-QKD has been studied extensively with either infinitely many different intensities [12] or a few intensities [14]. However, efficient decoy-state MDI-QKD with a heralded source was not shown. We know that weak coherent states (WCSs) have at least two drawbacks: one is the large vacuum component, and the other is the significant multiphoton probabilities. The former leads to a rather limited transmission distance, since the dark count contributes lots of bit-flip errors for long distance. The latter results in a quite low key generation rate. In the existing MDI-QKD setup [12,13], all detections are done in the Z basis. There are events of two incident photons presenting on the same side of the beam splitter and no incident photon on the other side. Such a case can cause a quite high observed error rate in the X basis. Although in principle one can deduce the phase-flip error rate by comparison of the observed error rates in the X basis for different groups of pulses as shown in Ref. [14], the high error rate in the X basis can still greatly decrease the key rate in real implementations when we take statistical fluctuations into account. Fortunately, besides the WCSs, there is another easily implementable source, the heralded single-photon source (HSPS). The source can eliminate those drawbacks and give much better performance than WCSs in the QKD [15,16], since the dark count can be brought to a negligible level for a triggered source. Moreover, the cause of the high error rate in the X basis does not exist for a HSPS due to a high-order small probability for events with two photons present on the same side of the beam splitter.

We also note that it is impossible to use an infinite number of decoy states in a realistic MDI-QKD; therefore, people often use one or two decoy states to estimate the behavior of the vacuum, the single-photon, and the multiphoton states [8,15].

Here in this work, we study MDI-QKD with heralded single-photon sources. A schematic of the method is shown in Fig. 1. We use both triggered and nontriggered events of HSPSs to precisely estimate the lower bound of the two-single-photon contribution (Y_{11}) and the upper bound of the quantum bit-error rate (QBER) of two-single-photon pulses (e_{11}). As a result, we get a much longer transmission distance and a much higher key generation rate compared with existing decoy-state MDI-QKD methods [14], and come close to the result of infinitely many different intensities. After presenting the schematic setup of the method, we shall present formulas using Y_{11} and e_{11} for calculating the key rate in Sec. II. In Sec. III, we proceed numerical simulations with practical parameters and compare the results with existing schemes. Finally, we give conclusions in Sec. IV.

II. IMPROVED METHOD OF DECOY-STATE MDI-QKD WITH HERALDED SOURCE

A. The method and formulas

We know that the state of a two-mode field from a parametric down-conversion (PDC) source is [17,18]

$$|\Psi\rangle_{TS} = \sum_{n=0}^{\infty} \sqrt{P_n}\, |n\rangle_T\, |n\rangle_S\, ,$$

$$P_n(x) = \frac{x^n}{(1+x)^{n+1}}\ (\Delta t_c \gg \Delta t),$$

[*] qinw@njupt.edu.cn
[†] xbwang@mail.tsinghua.edu.cn

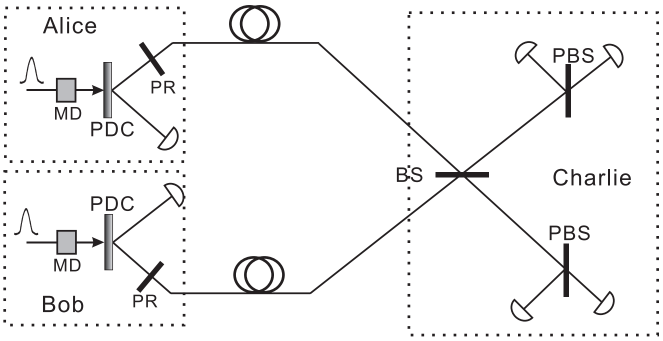

FIG. 1. (a) A schematic setup of the method. Alice and Bob randomly prepare HSPSs from parametric down-conversion (PDC) processes in a Bennett-Brassard 1984 (BB84) polarization state with a polarization rotator (PR). Decoy states are generated by changing the power of each pump laser with a modulator (MD). Signal pulses from Alice and Bob interfere at a 50:50 beam splitter (BS) and then each enters a polarizing beam splitter (PBS) projecting the input photons into either horizontal (H) or vertical (V) polarization states. Four single-photon detectors are employed at the third party, Charlie's side, to detect the results. Moreover, both the triggered and nontriggered events at Alice's and Bob's sides are sent to Charlie, and corresponding counting rates are recorded individually.

or

$$P_n(x) = e^{-x}\frac{x^n}{n!}\ (\Delta t_c \ll \Delta t),$$

where $|n\rangle$ represents an n-photon state, and x is the intensity (average photon number) of one mode. Mode T (trigger) is detected by Alice or Bob, and mode S (signal) is sent out to the untrusted third party (UTP). Δt_c is the coherence time of the emission, and Δt is the duration of the pump pulse. As demonstrated in Refs. [19,20], we can get either a thermal distribution or a Poisson distribution by adjusting the experimental conditions, e.g., by changing the duration of the pump pulses. Below, we will first use HSPSs with Poisson distributions as an example to describe our MDI-QKD scheme and then compare it with the case of thermal distributions.

We denote by q_n^υ the probability of triggering a count at Alice or Bob's detector when an n-photon state is emitted,

$$q_0^\upsilon = d_\upsilon$$

and

$$q_n^\upsilon = 1-(1-d_\upsilon)(1-\eta_\upsilon)^n,$$

for $i \geqslant 1$. Here υ can be A (Alice) or B (Bob), and η_υ and d_υ are the detection efficiency and the dark count rate at Alice's (Bob's) side, respectively. For simplicity, we may omit the superscript or subscript v later if there is no confusion. Then the corresponding nontriggering probability is $(1-q_n)$.

We request Alice (or Bob) to randomly change the intensity of her (or his) pump light among three values, so that the intensity of one mode is randomly changed among 0, μ_A (or μ_B), and μ'_A (or μ'_B) (and $\mu_A < \mu'_A$, $\mu_B < \mu'_B$). We define the subclass of source pulses in which Alice uses intensity x, and Bob uses intensity y as *source* $\{x,y\}$, $x \in \{0,\mu_A,\mu'_A\}$ and $y \in \{0,\mu_B,\mu'_B\}$. After triggering detection, there are four classes of states at each side from the two-mode fields of two different intensities, as there are triggered and nontriggered states for each intensity. In principle, here we have many choices in implementing decoy-state MDI-QKD. For example, we may use all events in both intensities; use only triggered events of both intensities; or use triggered events in one intensity and nontriggered events in the other. Here we shall study the following two cases: (1) use of only triggered events in both intensities; (2) use of nontriggered events from the stronger field and triggered events from the weaker field for the estimation of Y_{11}, and then use of the triggered events from the stronger pulses for the final key distillation. We declare that, first, both cases can lead to a longer transmission distance than that obtained using WCSs, and second, both the key rate and the secure transmission distance in the second case are better than in the first case.

As shown in Ref. [12], we use the rectilinear basis (Z) as the key generation basis, and the diagonal basis (X) for error testing only. We denote by $Y_{mn}^{W,t}$, $S_{mn}^{W,t}$, and $e_{mn}^{W,t}$ the yield, the gain, and the QBER of the triggered signals, respectively, where n and m represent the numbers of photons sent by Alice and Bob, and W represents the Z or X basis. Similarly, we also define $Y_{mn}^{W,nt}$, $S_{mn}^{W,nt}$, and $e_{mn}^{W,nt}$ as the corresponding values for the nontriggered events. Note that the gain $S_{x,y}^{W,t}$ is defined as $n_{x,y}^{W,t}/N_{x,y}^{W}$, if $n_{x,y}^{W,t}$ and $N_{x,y}^{W}$ are the number of *detected* events after triggering at both sides and the number of total events (no matter whether triggered or not) among the subclass of source pulses for which Alice uses intensity x, Bob uses intensity y, and both of them are prepared in basis W. A similar definition is also used for $S_{x,y}^{W,nt}$, the gain of nontriggered sources in basis W. All gains can be directly experimentally observed and thus are regarded as *known* values. The yield $\{Y_{mn}^{W,t}\}$ is defined as the the rate of producing a successful event for a two-pulse state $|m\rangle \otimes |n\rangle$ prepared in the W basis after triggering. A similar definition is also used for nontriggered pulses. Asymptotically, we have $Y_{mn}^{W,t} = Y_{mn}^{W,nt}$. Therefore we shall use only Y_{mn}^{W} for both of them. Note the the yield of Y_{mn}^{W} is not directly observed in the experiment and our first major task is to deduce the lower bound of Y_{11}^{W} based on the known values $\{S_{xy}^{W,t}\},\{S_{xy}^{W,nt}\}$. Here we assume that the decoy-state method is implemented in different bases *separately*; therefore we shall omit the superscript W hereafter provided that this does not cause any confusion.

The un-normalized density matrix for a triggered event from the two-mode field of intensity r is

$$\rho_r^t = \left(\sum_0^\infty q_n P_n(r)\,|n\rangle\,\langle n|\right). \tag{1}$$

Also, we have the following density matrix for a nontriggered event at Alice's side:

$$\rho_r^{nt} = \left(\sum_0^\infty (1-q_n) P_n(r)\,|n\rangle\,\langle n|\right). \tag{2}$$

Using the conclusions in Ref. [14], we can obtain the yield of single-photon pairs once we know the source state. For triggered events, we have

$$S^{t}_{x,y} = \tilde{S}^{t}_{00} + \eta_A\eta_B x e^{-x} y e^{-y} Y_{11} + \eta_A x e^{-x}\sum_{n=2}^{\infty}[1-(1-\eta_B)^n]e^{-y}\frac{y^n}{n!}Y_{1n} + \eta_B y e^{-y}\sum_{m=2}^{\infty}[1-(1-\eta_A)^m]e^{-x}\frac{x^m}{m!}Y_{m1}$$
$$+ \sum_{m=2,n=2}^{\infty} e^{-x}\frac{x^m}{m!}e^{-y}\frac{y^n}{n!}[1-(1-\eta_A)^m][1-(1-\eta_B)^n]Y_{mn}. \tag{3}$$

Here $\tilde{S}^{t}_{00} = \mathcal{L}_A + \mathcal{L}_B - \mathcal{L}_0$, and $\mathcal{L}_A = d_B e^{-y}\sum_{m=0}^{\infty}[1-(1-d_A)(1-\eta_A)^m]e^{-x}\frac{x^m}{m!}Y_{m0}$, $\mathcal{L}_B = d_A e^{-x}\sum_{n=0}^{\infty}[1-(1-d_B)(1-\eta_B)^n]e^{-y}\frac{y^n}{n!}Y_{0n}$, $\mathcal{L}_0 = d_A d_B e^{-x}e^{-y}Y_{00}$. According to the definition of the gains above, one easily finds that $\mathcal{L}_A = S^{t}_{x0}$, $\mathcal{L}_B = S^{t}_{0y}$, and $\mathcal{L}_0 = S^{t}_{00}$. All these gains are known values. Therefore, $\tilde{S}^{t}_{00} = S^{t}_{x0} + S^{t}_{0y} - S^{t}_{00}$ is also a *known* value. Similarly, we also have the following equation for the nontriggered events:

$$S^{nt}_{x,y} = \tilde{S}^{nt}_{00} + (1-\eta_A)(1-\eta_B)x e^{-x} y e^{-y} Y_{11} + (1-\eta_A)x e^{-x}\sum_{n=2}^{\infty}(1-\eta_B)^n e^{-y}\frac{y^n}{n!}Y_{1n} + (1-\eta_B)y e^{-y}$$
$$\times\sum_{m=2}^{\infty}(1-\eta_A)^m e^{-x}\frac{x^m}{m!}Y_{m1} + \sum_{m=2,n=2}^{\infty} e^{-x}\frac{x^m}{m!}e^{-y}\frac{y^n}{n!}(1-\eta_A)^m(1-\eta_B)^n Y_{mn}, \tag{4}$$

where $\tilde{S}^{nt}_{00} = S^{nt}_{x0} + S^{nt}_{0y} - S^{nt}_{00}$, and also $S^{nt}_{x0} = (1-d_B)e^{-y}\sum_{m=0}^{\infty}[(1-d_A)(1-\eta_A)^m]e^{-x}\frac{x^m}{m!}Y_{m0}$, $S^{nt}_{0y} = (1-d_A)e^{-x}\sum_{n=0}^{\infty}[(1-d_B)(1-\eta_B)^n]e^{-y}\frac{y^n}{n!}Y_{0n}$, $S^{nt}_{00} = (1-d_A)(1-d_B)e^{-x}e^{-y}Y_{00}$. They are regarded as known values. Now let us use $S^{t}_{\mu,\mu}$ and $S^{nt}_{\mu',\mu'}$ to estimate a tight bound on Y_{11}. Denoting $k = \frac{(1-\eta_A)(1-\eta_B)^2}{\eta_A[1-(1-\eta_B)^2]}(\frac{\mu'}{\mu})^3 e^{2\mu-2\mu'}$, and combining Eqs. (4) and (3), we obtain

$$Y_{11} = \frac{k\big(S^{t}_{\mu,\mu} - \tilde{S}^{t}_{00}\big) - \big(S^{nt}_{\mu',\mu'} - \tilde{S}^{nt}_{00}\big) + \mathcal{K}}{[k\eta_A\eta_B\mu^2 e^{-2\mu} - (1-\eta_A)(1-\eta_B)\mu'^2 e^{-2\mu'}]} \tag{5}$$

and

$$\mathcal{K} = \sum_{n=2}^{\infty}\left\{(1-\eta_A)\mu' e^{-2\mu'}(1-\eta_B)^n\frac{\mu'^n}{n!} - k\eta_A\mu e^{-2\mu}[1-(1-\eta_B)^n]\frac{\mu^n}{n!}\right\}Y_{1n}$$
$$+ \sum_{m=2}^{\infty}\left\{(1-\eta_B)\mu' e^{-2\mu'}(1-\eta_A)^m\frac{\mu'^m}{m!} - k\eta_B\mu e^{-2\mu}[1-(1-\eta_A)^m]\frac{\mu^m}{m!}\right\}Y_{m1}$$
$$+ \sum_{m=2,n=2}^{\infty}\left\{(1-\eta_A)^m(1-\eta_B)^n e^{-2\mu'}\frac{\mu'^m}{m!}\frac{\mu'^n}{n!} - k[1-(1-\eta_A)^m][1-(1-\eta_B)^n]e^{-2\mu}\frac{\mu^m}{m!}\frac{\mu^n}{n!}\right\}Y_{mn}. \tag{6}$$

To lower-bound Y_{11} here, we can choose to set the following simultaneous conditions:

$$[k\eta_A\eta_B\mu^2 e^{-2\mu} - (1-\eta_A)(1-\eta_B)\mu'^2 e^{-2\mu'}] \leqslant 0, \quad \mathcal{K} \leqslant 0. \tag{7}$$

When both the conditions above are met, we have the following inequality for the lower bound of Y_{11}:

$$Y_{11} \geqslant Y^{L}_{11} \equiv \frac{k\big(S^{t}_{\mu,\mu} - \tilde{S}^{t}_{00}\big) - \big(S^{nt}_{\mu',\mu'} - \tilde{S}^{nt}_{00}\big)}{[k\eta_A\eta_B\mu^2 e^{-2\mu} - (1-\eta_A)(1-\eta_B)\mu'^2 e^{-2\mu'}]}. \tag{8}$$

Since the values of μ and μ' can be chosen separately, the above conditions can be easily satisfied in practice. In particular, in the symmetric case that $\eta_A = \eta_B = \eta$, the conditions on Eq. (7) reduce to

$$\mu \geqslant (1-\eta)\mu'. \tag{9}$$

For simplicity, we shall use such a condition for all calculations. Actually, directly applying Eqs. (16) and (2) of Ref. [14] together with Eqs. (1) and (2) here can also lead to Eqs. (8) and (9). This confirms Eqs. (8) and (9). Then the gains of the two-single-photon pulses for the triggered and nontriggered signals (μ') are

$$S^{t}_{11} = \eta^2\mu'^2 e^{-2\mu'}Y_{11}, \tag{10}$$

$$S^{nt}_{11} = (1-\eta)^2\mu'^2 e^{-2\mu'}Y_{11}. \tag{11}$$

As mentioned above, we use two bases in this protocol, i.e., the Z basis and the X basis. We use the former to generate real keys, and the latter only for error testing. After the error test, we get the bit-flip error rates for the triggered and nontriggered pulses as $E^{t}_{\mu,\mu}$ and $E^{nt}_{\mu',\mu'}$. In order to calculate the final key rate, we also need to know the phase-flip error rate of two-single-photon pulses in the Z basis, i.e., $e^{ph,t}_{11}$ (or $e^{ph,nt}_{11}$), which is equal to the bit-flip rate in the X basis, $e^{X,t}_{11}$ (or $e^{X,nt}_{11}$), whose values can be represented as

$$e^{X,t}_{11} \leqslant \frac{E^{X,t}_{\mu,\mu}S^{X,t}_{\mu,\mu} - E^{X,t}_{\mu,0}S^{X,t}_{\mu,0} - E^{X,t}_{0,\mu}S^{X,t}_{0,\mu} + E^{X,t}_{0,0}S^{X,t}_{0,0}}{S^{\omega,t}_{11}} \equiv e^{X}_{a} \tag{12}$$

or

$$e_{11}^{X,nt} \leqslant \frac{E_{\mu',\mu'}^{X,nt} S_{\mu',\mu'}^{X,nt} - E_{\mu',0}^{X,nt} S_{\mu',0}^{X,nt} - E_{0,\mu'}^{X,nt} S_{0,\mu'}^{X,nt} + E_{0,0}^{X,nt} S_{0,0}^{X,nt}}{S_{11}^{\omega,nt}} \equiv e_b^X. \tag{13}$$

Combining the two bounds, we have [21]

$$e_{11}^X \leqslant e_{11}^{X,U} = \min\left\{e_a^X, e_b^X\right\}. \tag{14}$$

Now we can calculate the final key generation rate for the triggered signal pulses (μ') as

$$R^t \geqslant \{q^2 P_1^2(\mu') Y_{11}^{Z,t}[1 - H_2(e_{11}^X)] - S_{\mu',\mu'}^{Z,t} f(E_{\mu',\mu'}^{Z,t}) H_2(E_{\mu',\mu'}^{Z,t})\}, \tag{15}$$

where $f(E_{\mu'})$ is a factor for the cost of error correction given existing error correction systems in practice, and we assume $f = 1.16$ here [12]. $H_2(x)$ is the binary Shannon information function, given by

$$H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x).$$

We have not considered the effects of base mismatch in the Bennett-Brassard 1984 (BB84) protocol [22]. Actually, one can choose the basis in a biased way [23] and the effect can vanish asymptotically. In fact, the nontriggered events and the triggered events from weaker fields can also be used to distill secret keys as shown in Ref. [24]. However, for simplicity, in the following simulations we consider only the triggered components from the stronger field.

III. NUMERICAL SIMULATION

With the formulas above, we can now numerically calculate the key rate and compare the secret key generation rate of our MDI-QKD scheme with those of existing methods [12,15]. Moreover, we will show the different results of our proposed scheme using different HSPSs, i.e., with Poisson or thermal distributions. Below, for simplicity, we assume that the UTP is located midway between 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 probably be observed for the gains and error rates in normal cases using a linear model [12,25] where the state $|n\rangle\langle n|$ from Alice changes to

$$\sum_{k=0}^{n} C_n^k \eta^k (1-\eta)^{n-k} |k\rangle\langle k|, \tag{16}$$

where η is the transmittance from Alice to the UTP. Using this model, we can set values (which probably would be the observed values in experiments) for S_{xy}^t, S_{xy}^{nt}, E_{xy}^t, and E_{xy}^{nt} according to the transmission distance. After setting these values, we can find the distance-dependent key rate via Eq. (15). For this purpose, we have developed a general model to simulate the probably observed gains and error rates and hence the final key rate under a linear loss channel, given any source state [25].

For a fair comparison, we use the same parameters as in Refs. [12,26] (see Table I), except that Alice (Bob) uses an extra detector for heralding signals with a detection efficiency of η_A (η_B) and dark count rate of d_A (d_B).

TABLE I. Parameters used in numerical simulations: α is the channel loss, e_d is the misalignment probability, and d_c and η_c are the dark count rate and the detection efficiency per detector at the UTP's side, respectively.

α (dB/km)	e_d (%)	d_c	η_c (%)
0.2	1.5	3×10^{-6}	14.5

In practical implementations, people often use a nondegenerate PDC process and obtain a visible and a telecommunication wavelength in modes T and S, respectively. To simplify the simulations, we assume that both Alice and Bob have the same silicon avalanche photodiodes. We do the calculation for the conditions of detection $\eta_A = \eta_B = 0.75$ (or 0.9), and $d_A = d_B = 10^{-6}$. At each distance, in order to maximize the key generation rate, we set $\mu = (1-\eta)\mu'$ and use the optimal μ' for the case of using both triggered and nontriggered events; for other cases we set $\mu = 0.1$ and use the optimal value of μ'. Our simulation results are shown in Figs. 2–4.

Figure 2(a) displays the comparison of the final key generation rate between different schemes. The curve $W0$ is the case of using an infinite number of decoy states with WCSs [12], $W1$ represents Wang's three-decoy-state method with WCSs [15], $H01$ (or $H02$) shows the asymptotic case with HSPSs, and H1 (or H2) represents the result of our scheme with triggered and nontriggered HSPSs. In the simulations above, we use the optimal values of μ' at each distance for all the curves. The only difference is that, for the asymptotic cases ($W0$, $H01$, and $H02$), the fraction of two-single-photon counts and the QBER of two-single-photon pulses are known

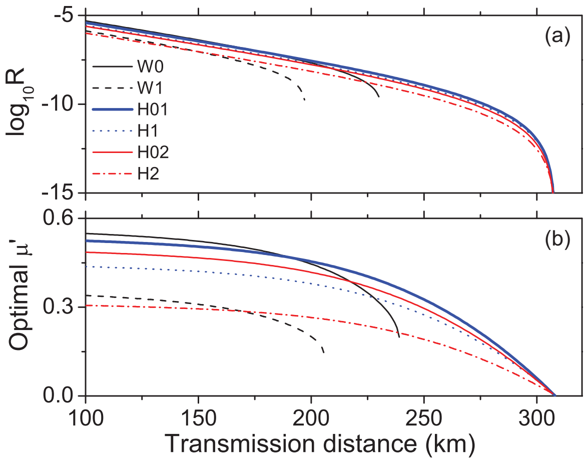

FIG. 2. (Color online) (a) Comparison of the final key generation rates vs distance between our proposed scheme and the ones in Refs. [12] and [15]. $W0$, infinite intensities with WCSs [12]; $W1$, three-intensity method with WCSs; $H01$ and $H02$, infinite intensities with HSPSs; $H1$ and $H2$, our proposed method with triggered and nontriggered HSPSs. (b) Optimal values of μ' for each curve listed in (a). The WCSs and the HSPSs used here are all in Poisson distributions. We have chosen the heralding detection efficiency to be 0.9 for curves $H01$ and $H1$, and 0.75 for curves $H02$ and $H2$.

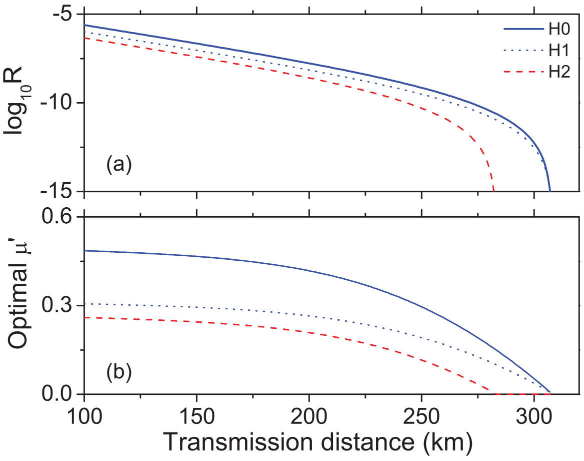

FIG. 3. (Color online) (a) Comparison of the final key generation rates with HSPSs using different methods. $H0$, infinite intensities; $H1$ a few intensities of this work; $H2$, key rates of a few intensities using triggered events in sources of intensities μ and μ' to calculate Y_{11} [15]. The HSPSs used here are all in Poisson distributions. (b) Corresponding optimal values of μ' for all the lines in (a). We have chosen all heralding detection efficiencies to be 0.75.

exactly; for the normal three-decoy-state case ($W1$), we use the parameters shown in Table I and assume a reasonable value for μ (0.1); while for our scheme ($H1$ and $H2$), we use the same parameters as in Table I except that $\eta_A = \eta_B = 0.9$ (or 0.75), and borrow the relationship of μ and μ' from Eq. (9). Figure 2(b) shows corresponding optimal values of μ' for each curve in Fig. 2(a). In addition, the WCSs and HSPSs used here are all in Poisson distributions.

Figures 3(a) and 3(b) show the comparison of our MDI-QKD scheme with the normal three-decoy-state method [15] using HSPSs. Figure 3(a) shows the the final key generation rate vs transmission distance, and Fig. 3(b) corresponds to the optimal values of μ'. The curves $H0$ and $H1$ correspond to the asymptotic case with an infinite number of decoy states and our scheme, respectively. $H2$ represents the result of using the normal three-decoy-state method. Here the HSPSs used are all in Poisson distributions.

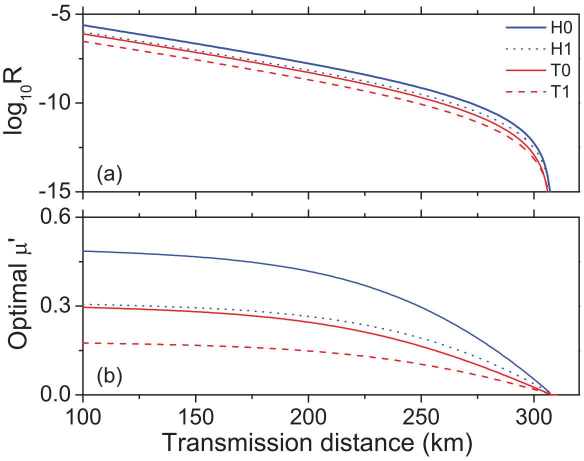

FIG. 4. (Color online) (a) Comparison of the final key generation rates of MDI-QKD with HSPSs in different photon-number distributions. $H0$, infinite intensities, Poisson distribution; $H1$, a few intensities of this work, Poisson distribution; $T0$, infinite intensities, thermal distribution; $T1$, a few intensities of this work, thermal distribution. We have chosen all heralding detection efficiencies to be 0.75.

Figures 4(a) and 4(b) describe the different behavior of our MDI-QKD scheme when using HSPSs in different distributions. The curves $H0$ and $H1$ represent the results of using the infinite-decoy-state method and our scheme, respectively, both using HSPSs in Poisson distributions. The lines $T0$ and $T1$ correspond to the results with thermal distributions.

From the comparison above we find the following:

(i) Our scheme of using triggered and nontriggered signals can work excellently close to the asymptotic case with infinite decoy states as in Figs. 2(a) and 2(b). This is due to the precise estimation of the tight bounds on Y_{11} and e_{11} by using both triggered and nontriggered signals.

(ii) Our MDI-QKD scheme with HSPSs can transmit over a much longer distance compared with the one with WCSs (>70 km here) as shown in Fig. 2(a), which benefits from the substantial low-vacuum components in the heralded signals.

(iii) In our scheme, the HSPSs in Poisson distributions show similar key generation rates as WCSs at short distances, and much higher key rates at long distances as shown in Fig. 2(a). This is attributed to a much higher optimal value of μ' being used, as shown in Fig. 2(b).

(iv) According to our calculation here, the protocol using Eq. (8) can have a higher key rate than the one using only triggered events, as shown in Fig. 3(a), because of a much higher optimal value of μ' being used as shown in Fig. 3(b).

(v) As in Refs. [17,27], the HSPS source with the Poisson distribution has better performance than the one with the thermal distribution as shown in Figs. 4(a) and 4(b). This is because the Poisson distribution has a higher single-photon probability.

In all our calculations, we did not normalize the triggered or nontriggered states, e.g., Eqs. (1) and (2). Hence the gains and the key rates calculated here are in units of the rate averaged over all pumped events of a certain intensity in a certain basis. For example, in the H and V basis, there are N'_z times that both Alice and Bob used stronger pump lights. Among these events, they obtain N'_{tn} events of triggering at both sides and n'_{tz} successful events. Then the gain in our definition is n'_{tz}/N'_z. If we want the key rate averaged over the number of triggered states, our results in each figure become several times larger, since they should be multiplied by a factor $1/F$, where F is the normalization factor.

IV. CONCLUSIONS AND DISCUSSION

In summary, we have studied decoy-state MDI-QKD with a heralded single-photon source. We show that this proposed implementation offers a longer transmission distance compared with existing realization methods. Therefore, it looks promising for practical applications in the future.

ACKNOWLEDGMENTS

Q.W. thanks Professor Z. Yang and B. Y. Zheng for useful discussions and kind support during the work. We gratefully acknowledge the financial support from the National

High-Tech Program of China through Grants No. 2011AA010800 and No. 2011AA010803, the NSFC through Grants No. 11274178, No. 11174177, No. 60725416 and No. 11311140250, and the 10000 Plan of Shandong Province.

[1] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995); H. P. Yuen, Quantum Semiclass. Opt. **8**, 939 (1996).

[2] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000); N. Lütkenhaus and M. Jahma, New J. Phys. **4**, 44 (2002).

[3] C. H. F. Fung, B. Qi, K. Tamaki, and H. K. Lo, Phys. Rev. A **75**, 032314 (2007); B. Qi, C. H. F. Fung, H. K. Lo, and X. Ma, Quantum Inf. Comput. **7**, 73 (2007); Y. Zhao, C. H. F. Fung, B. Qi, C. Chen, and H. K. Lo, Phys. Rev. A **78**, 042333 (2008).

[4] L. Lydersen *et al.*, Nat. Photon. **4**, 686 (2010); N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, Phys. Rev. Lett. **107**, 110501 (2011).

[5] H. Inamori, N. Lütkenhaus, and D. Mayers, Eur. Phys. J. D **41**, 599 (2007).

[6] D. Gottesman, H. K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **5**, 325 (2004).

[7] W. Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[8] X. B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).

[9] H. K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).

[10] D. Mayers and A. Yao, in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS98)* (IEEE Computer Society, Washington, DC, 1998), p. 503; A. Acín, N. Gisin, and L. Masanes, Phys. Rev. Lett. **97**, 120405 (2006); A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, *ibid*. **98**, 230501 (2007).

[11] N. Gisin, S. Pironio, and N. Sangouard, Phys. Rev. Lett. **105**, 070501 (2010); M. Curty and T. Moroder, Phys. Rev. A **84**, 010304(R) (2011).

[12] H. K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

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

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

[15] Q. Wang, X. B. Wang, and G. C. Guo, Phys. Rev. A **75**, 012312 (2007).

[16] Q. Wang and A. Karlsson, Phys. Rev. A **76**, 014309 (2007).

[17] B. Yurke and M. Potasek, Phys. Rev. A **36**, 3464 (1987).

[18] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).

[19] S. Mori, J. Söderholm, N. Namekata, and S. Inoue, Opt. Commun. **264**, 156 (2006).

[20] G. Ribordy, J. Brendel, J. D. Gauthier, N. Gisin, and H. Zbinden, Phys. Rev. A **63**, 012309 (2000).

[21] For those nontriggered events, the observed error rate in the X basis is rather large. To avoid this drawback, one can choose to use the triggered events, i.e., Eq. (13) in estimating the errors in the X basis and hence the phase-flip rate.

[22] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.

[23] H. K. Lo, H. F. Chau, and M. Ardehali, J. Cryptol. **18**, 133 (2005).

[24] Y. Adachi, T. Yamamoto, M. Koashi, and N. Imoto, Phys. Rev. Lett. **99**, 180503 (2007).

[25] Q. Wang and X. B. Wang, arXiv:1311.1739.

[26] R. Ursin *et al.*, Nat. Phys. **3**, 481 (2007).

[27] W. Helwig, W. Mauerer, and C. Silberhorn, Phys. Rev. A **80**, 052326 (2009).