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

Qin Wang\textsuperscript{1} and Xiang-Bin Wang\textsuperscript{2,\dagger}

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

Abstract

We present an efficient proposal on using both the triggered and non-triggered events of her-alded single-photon sources for the measurement-device-independent quantum key distribution. We compare our new scheme with the existing methods using either weak coherent sources or heralded single photon sources, and find that our new scheme can give higher key rate and 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 distribution. We demonstrate that the former can generate a relatively higher secure key rate than the latter, and can thus work more efficiently in practical quantum key distributions.

PACS number(s): 42.50.Ct, 78.67.Hc, 78.47.D-

\textsuperscript{*}Electronic address: qinw@njupt.edu.cn
\textsuperscript{†}Electronic address: xbwang@mail.tsinghua.edu.cn
I. INTRODUCTION

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

In order to solve the conflicts between the theory and the practice, different approaches have been proposed, such as the decoy-state method [5–9], the device-independent quantum key distribution (DI-QKD) [10, 11] and recently the measurement-device-independent quantum key distribution (MDI-QKD) [12, 13]. Among them, the MDI-QKD seems to be a very promising candidate considering its relatively lower technical demanding.

People [12, 13] have given out security proofs for the MDI-QKD and demonstrated that it can offer excellent security by removing all side-channel attacks on measurement devices. In particular, the decoy-state MDI-QKD was studied extensively with infinite different intensities [12] and a few intensities [15]. However, the efficient decoy-state MDIQKD with heralded source is not shown. We know that weak coherent states (WCSs) at least have two drawbacks: one is the large vacuum component, and the other is the significant multi-photon 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 one results in a quite low key generation rate. In the existing MDI-QKD [12, 13] setup, all detections are done in Z basis. There are events of two incident photons presenting on the same side of the beam-splitter and no incident photon on another side. Such a case can cause a quite high observed error rate in X basis. Though in principle one can deduce the phase-flip error rate by comparison of the observed error rate in X basis for different groups of pulses as shown in [13], the high error rate in X basis can still decrease the key rate drastically in the real implementation when we take the statistical fluctuation into consideration. Fortunately, besides the WCSs, there is another practically easy implementable source, the heralded single-photon source (HSPS). The source can eliminate those drawbacks, and give much
better performance than WCSs in the QKD [16, 17], since the dark count can be eliminated to a negligible level for a triggered source. The cause of high error rate in X basis does not exist for a HSPS because the probability for events of two incidents photons on the same side of the beam-splitter is a high order small value.

We also note that it is impossible to use 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 multi-photon states [8, 16].

Here in this work, we study MDI-QKD with heralded single-photon sources. We use both the triggered and non-triggered 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 an much longer transmission distance and a much higher key generation rate compared with existing decoy-state MDI-QKD methods [15], and come close to the result of infinite different intensities. After presenting the schematic set-up of the method, we shall present formulas such as $Y_{11}$ and $e_{11}$ for calculating the key rate in Sec. II. In Sec. III, we proceed numerical simulations with practical parameters and compare 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 the parametric-down conversion (PDC) source is [18, 19]:

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

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

or

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

or
FIG. 1: (Color online) (a). A schematic setup of the method. Alice and Bob randomly prepare HSPSs from PDC processes in a 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 beamsplitter (BS) and then each enter 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 and Bob’s side are sent to Charlie, and corresponding counting rates are recorded individually.

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 UTP. $\Delta t_c$ is the coherence time of the emission, and $\Delta t$ is the duration of the pump pulse. As demonstrated in [20, 21], we can either get a thermal distribution or a poisson distribution by adjusting the experimental conditions, e.g. changing the duration of the pump pulses. Below, we will at first use HSPSs with poisson distributions as an example to describe our new MDI-QKD scheme, and then compare it with the case of with thermal distributions.

We denote $q^v_n$ as the probability of triggering at Alice or Bob’s detector when $n$-photon state is emitted,

$$q^v_0 = d_v,$$

and

$$q^v_n = 1 - (1 - \eta_v)^n.$$
for \( i \geq 1 \). Here \( \nu \) can be A (Alice) or B (Bob), \( \eta_{\nu} \) and \( d_{\nu} \) are the detection efficiency and the dark count rate at Alice (Bob)’s side, respectively. Then the corresponding non-triggering probability is \((1 - q_{\nu}^w)\).

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, \( \mu \), and \( \mu' \) (and \( \mu < \mu' \)). We define the subclass of source pulses that Alice uses intensity \( x \), Bob uses intensity \( y \) as source \( \{x, y\} \), each \( x \) and \( y \) can be any values from \( \{0, \mu, \mu'\} \). As shown latter, we shall use the gain of triggered events from the source of intensity \( \mu \) and the gain of non-triggered events from source of intensity \( \mu' \) to calculate the yield for states of a single photon from each side, \( Y_{11} \). Numerical results show that the key rate of the method is very close to the ideal case where we use infinite intensities, and the method is more efficient than a method that obtains \( Y_{11} \) by using the gains of triggered events from both sources of intensity \( \mu \) and \( \mu' \). As shown in \([12, 15]\), we use the rectilinear basis (Z) as the key generation basis, and the diagonal basis (X) for error testing only. We denote \( Y_{mn}^{W,t}, S_{mn}^{W,t} \), and \( e_{mn}^{W,t} \) to be the yield, the gain and the QBRE of the triggered signals respectively, where \( n, m \) represent the number of photons sent by Alice and Bob, and \( W \) represent the Z or X basis. Similarly, we also define \( Y_{mn}^{W,nt}, S_{mn}^{W,nt} \), and \( e_{mn}^{W,nt} \) as corresponding values for the non-triggered 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 side and the number of total events (no matter triggered or not) among the subclass of source pulses that Alice uses intensity \( x \), Bob uses intensity \( y \) and both of them are prepared in basis \( W \). Similar definition is also used for \( S_{x,y}^{W,nt} \), the gain of non-triggered sources in basis \( W \). All gains are observed directly in the experiment therefore they are regarded as known values. The yield \( \{Y_{mn}^{W,t}\} \) is defined as the rate of producing a successful event for two-pulse state \(|m\rangle \otimes |n\rangle \) prepared in \( W \) basis after triggering. Similar definition is also used for non-triggered pulses. Asymptotically, we have \( Y_{mn}^{W,t} = Y_{mn}^{W,nt} \). Therefore we shall only use \( Y_{mn}^{W,t} \) 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 to implement the decoy-state method in different bases separately, therefore we shall omit the superscript \( W \) here after provided that this does not make any confusion.
The un-normalized density matrix for the two-pulse state of a triggered event is

$$\rho_{x,y}^t = \left( \sum_{n=0}^{\infty} p_n^A |n\rangle \langle n| \right) \otimes \left( \sum_{n=0}^{\infty} p_n^B |n\rangle \langle n| \right)$$

(1)

with $p_n^A = q_n^AP_n(x)$ and $p_n^B = q_n^BP_n(y)$ . According to the definitions above, we have

$$S_{x,y}^t = \tilde{S}_{00}^t + \eta_A \eta_B x e^{-x} y e^{-y} Y_{11} + \eta_A x e^{-x} \sum_{n=2}^{\infty} (1 - (1 - \eta_B)^n) e^{-y} \frac{y^n}{n!} Y_{1n} + \eta_B y e^{-y} \sum_{m=2}^{\infty} (1 - (1 - \eta_A)^m)$$

$$e^{-x} \frac{x^m}{m!} Y_{m1} + \sum_{m=2, n=2}^{\infty} e^{-x} \frac{x^m}{m!} e^{-y} \frac{y^n}{n!} (1 - (1 - \eta_A)^m)(1 - (1 - \eta_B)^n) Y_{mn}.$$  

(2)

Here $\tilde{S}_{00}^t = \mathcal{L}_A - \mathcal{L}_B - \mathcal{L}_0$ and $\mathcal{L}_A = d_B e^{-y} \sum_{m=2}^{\infty} [d_A + 1 - (1 - \eta_A)^m] e^{-x} \frac{x^m}{m!} Y_{m0}$, $\mathcal{L}_B = d_A e^{-x} \sum_{n=0}^{\infty} [d_B + 1 - (1 - \eta_B)^n] e^{-y} \frac{y^n}{n!} Y_{0n}$, $\mathcal{L}_0 = d_A d_B e^{-x} e^{-y} Y_{00}$. According to the definition of gains above, one easily finds that fact $\mathcal{L}_A = S_{x0}^t, \mathcal{L}_B = S_{0y}^t, \mathcal{L}_0 = S_{00}^t$. All these gains are known values. Therefore $\tilde{S}_{00}^t = S_{x0}^t + S_{0y}^t - S_{00}^t$ is a known value. Similarly, for the non-triggered events, we have

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

(3)

where $\tilde{S}_{00}^{nt} = S_{x0}^{nt} + S_{0y}^{nt} - S_{00}^{nt}$. And also $S_{x0}^{nt} = (1 - d_B) e^{-y} \sum_{m=0}^{\infty} [(1 - \eta_A)^m - d_A] e^{-x} \frac{x^m}{m!} Y_{m0}$, $S_{0y}^{nt} = (1 - d_A) e^{-x} \sum_{n=0}^{\infty} [(1 - \eta_B)^n - d_B] e^{-y} \frac{y^n}{n!} Y_{0n}$, $S_{00}^{nt} = (1 - d_A)(1 - d_B) e^{-x} e^{-y} Y_{00}$. These are regarded as known values. Now let’s use $S_{\mu,\mu'}^{nt}$ and $S_{\mu',\mu}^{nt}$ to estimate a tight bound of Y

Denoting $k = \frac{(1 - \eta_A)(1 - \eta_B)^2}{(1 - \eta_A)(1 - \eta_B)^2} (\mu^2)^{2\mu - 2 \mu'}$, and combining Eq. (3) and (2), we obtain

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

(4)

and

$$\mathcal{K} = \sum_{n=2}^{\infty} [(1 - \eta_A) \mu^2 e^{-2 \mu'} (1 - \eta_B)^n \mu^n \frac{n!}{n!} - k \eta_A \mu e^{-2 \mu'} (1 - \eta_B)^n \mu^n \frac{n!}{n!}] Y_{1n} +$$

$$\sum_{m=2}^{\infty} [(1 - \eta_B) \mu e^{-2 \mu'} (1 - \eta_A)^m \mu^m \frac{m!}{m!} - k \eta_B \mu e^{-2 \mu'} (1 - \eta_A)^m \mu^m \frac{m!}{m!}] Y_{m1} +$$

$$\sum_{m=2, n=2}^{\infty} [(1 - \eta_A)^m (1 - \eta_B)^n e^{-2 \mu'} \mu^m \mu^n \frac{m!}{m!} n! - k [(1 - \eta_A)^m] [(1 - \eta_B)^n] e^{-2 \mu'} \mu^m \mu^n \frac{m!}{m!} n!] Y_{mn}.$$  

(5)
To lower bound $Y_{11}$ here, we can choose to set the following simultaneous conditions:

$$[k\eta_A\eta_B\mu^2 e^{-2\mu} - (1 - \eta_A)(1 - \eta_B)\mu'^2 e^{-2\mu'}] \leq 0; \ K \leq 0 \quad (6)$$

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

$$Y_{11} \geq Y_{11}^L \equiv \frac{k(S^t_{\mu,\mu} - \tilde{S}_{00}^t) - (S^nt_{\mu',\mu'} - \tilde{S}_{00}^nt)}{[k\eta_A\eta_B\mu^2 e^{-2\mu} - (1 - \eta_A)(1 - \eta_B)\mu'^2 e^{-2\mu'}]}.$$  \quad (7)

(since the value of $\mu$ and $\mu'$ 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.(6) reduce to

$$\mu \geq \mu'(1 - \eta) \left[ \frac{1 - (1 - \eta)^2}{1 - (1 - \eta)^m} \right]^{m-2} \quad (8)$$

for all $m \geq 3$. For simplicity, we shall use such a condition for all calculations. Then the gain of the two-single-photon pulses for the triggered and non-triggered signals ($\mu'$) are:

$$S_{11}^t = \eta^2 \mu'^2 e^{-2\mu'} Y_{11}, \quad (9)$$

$$S_{11}^nt = (1 - \eta)^2 \mu'^2 e^{-2\mu'} Y_{11}. \quad (10)$$

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 test. After error test, we get the bit-flip error rates for the triggered and non-triggered signals ($\mu'$) as:

$$E_{\mu,\mu}^t = \min \{ e_{a1}^X, e_{b1}^X \} \quad (13)$$

Now we can calculate the final key generation rate for the triggered signal pulses ($\mu'$) as:

$$R^t \geq \frac{1}{2} \left\{ p_A^t p_B^t Y_{11}^Z [1 - H_2(e_{11}^Z)] - S_{\mu',\mu'}^Z f(E_{\mu',\mu'}^Z) H_2(E_{\mu',\mu'}^Z) \right\}. \quad (14)$$
where the factor of $\frac{1}{2}$ comes from the cost of the basis mismatch in Bennett-Brassard 1984 (BB84) protocol; $f(E_{\mu'})$ 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

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

In fact, the non-triggered events can also be used to derived secret keys as shown in [22]. However, for simplicity, in the following simulations we consider only the triggered components.

B. Some remarks on Eqs.(4) and (6)

General formulas for $s_{11}$ and the conditions were presented in in Ref.[15]. Where it assumes that Alice (Bob) has three sources, denoted as 0, $\mu_A$, $\mu_A'$ (0, $\mu_B$, $\mu_B'$). Denote $\rho_x$ ($\rho_y$) as the density operator for source $x$ ($y$) at Alice’s (Bob’s) side, and $x$ ($y$) can take any value from 0, $\mu_A$, $\mu_A'$ (0, $\mu_B$, $\mu_B'$).

$$\rho_0 = |0\rangle\langle0|; \rho_{\mu_A} = \sum_k a_k |k\rangle\langle k|; \rho_{\mu_A'} = \sum_k a'_k |k\rangle\langle k|; \rho_{\mu_B} = \sum_k b_k |k\rangle\langle k|; \rho_{\mu_B'} = \sum_k b'_k |k\rangle\langle k|,$$

and it shows that

$$s_{11} = s_{11}^L + \frac{\zeta_1 + \zeta_2 + \xi}{K_0 a_1 b_1 - a'_1 b'_1}$$

and $s_{11}^L$ is given by the right hand side of Eq.(16) in Ref. [15], $K_0, \zeta_1, \zeta_2, \xi$ are all defined there [15]. To make sure $s_{11} \geq s_{11}^L$, we need the fraction $\frac{\zeta_1 + \zeta_2 + \xi}{K_0 a_1 b_1 - a'_1 b'_1} \geq 0$. In order that the result is physically meaningful, we also need $s_{11}^L > 0$ Ref. [15] requests both the numerator and the denominator to be non-negative. This indeed gives meaningful physical result ($s_{11}^L > 0$) for many sources, such as the coherent light and the triggered state of the PDC light. Mathematically, the whole fraction can also be non-negative if we choose both the numerator and the denominator to be non-positive. Given such a mathematical choice, normal sources like coherent states, triggered state of the PDC light does not give a positive value for $s_{11}^L$. However, here in our case, we use triggered results for $\mu$ and non-triggered results for $\mu'$. We find that $s_{11}^L$ is indeed positive and the key rate can be optimized under such a mathematical setting.
III. NUMERICAL SIMULATION

With formulas above, we can now numerically calculate the key rate and compare the secret key generation rate of our new MDI-QKD scheme with existing methods \[12, 15\]. Moreover, we will show the different results of our proposed scheme using different HSPSs, i.e., in poissonian or thermal distributions. Below for simplicity, we assume that the UTP locates in the middle of Alice and Bob, and the UTP’s detectors are identical, i.e., they have the same dark count rate and detection efficiency, and their detection efficiency does not depend on the incoming signals.

We shall estimate what values would be probably observed for the gains and error rates in the normal cases by the linear model as in \[8, 9\]:

\[
Y_n = d_C + 1 - (1 - \eta_C)^n, \quad \eta_C = \eta \times 10^{-\alpha L/10};
\]

\[
e_n = \frac{e_0 d_C + e_1 [1 - (1 - \eta_C)^n]}{d_C + 1 - (1 - \eta_C)^n},
\]

where \(\eta_C\) \((i = A, B)\) is the combined overall transmittance and detection efficiency between Alice (or Bob) and the UTP; \(L\) is the corresponding transmit distance; \(\eta_C\) and \(d_C\) are the transmission rate and dark count rate at the UTP’s side, respectively; \(e_n\) is the QBER of an n-photon state; and \(\alpha\) is the channel loss rate. Using this model, we can set values (probably would-be observed values in experiments) for \(S_{t,xy}^t\), \(S_{nt,xy}^t\), \(E_{t,xy}^t\) and \(E_{nt,xy}^t\) according to transmission distance. After setting these values, we can find the distance dependent key rate by Eq. (14).

In the MDI-QKD, \(Y_{m,n} = [d_C + 1 - (1 - \eta_A^m)]d_C + 1 - (1 - \eta_B^m)\), and \(e_{m,n} = \frac{e_0 d_C + e_1 [1 - (1 - \eta_A^m)]d_C + e_1 [1 - (1 - \eta_B^m)]}{Y_{m,n}}\). For a fair comparison, we use the same parameters as in \[12, 23\], see Table I, except that Alice (Bob) uses an extra detector for heralding signals with a detection efficiency of \(\eta_A\) (\(\eta_B\)) and dark count rate of \(d_A\) (\(d_B\)).

In practical implementations, people often use a non-degenerate PDC process and obtain a visible and a telecommunication wavelength in mode T and S, respectively. To simplify the simulations, we assume both Alice and Bob have the same silicon avalanche photodiodes, whose detection efficiency and dark count rate are \(\eta_A = \eta_B = 0.9\), \(d_A = d_B = 10^{-6}\), respectively. At each distance, we choose the optimal value of \(\mu'\), and meantime referring the value of \(\mu\) from Eq. (8), so as to maximize the key generation rate. Our simulation results are shown in Figs. 2 - 4.

Fig. 2(a) displays the comparison of the final key generation rate between different schemes. The solid black line (W0) is Lo’s asymptotic case with infinite decoy states in WCS \[12\], the dashed green line (W1) is Wang’s three decoy-state method with WCSs \[15\],
TABLE I: Parameters used in numerical simulations: $\alpha$ is the channel loss, $e_d$ is the misalignment probability, $d_C$ and $\eta_C$ are the dark count rate and the detection efficiency per detector at the UTP’s side, respectively.

| $\alpha$ (dB/km) | $e_d$ (%) | $d_C$ | $\eta_C$ (%) |
|------------------|-----------|-------|---------------|
| 0.2              | 0.75      | $3\times10^{-5}$ | 14.5          |

FIG. 2: (Color online) (a). Comparison of the final key generation rates vs distance between our proposed scheme and the ones in Ref. [12] and Ref. [15]. W0: in finite intensities with WCSs; W1: three-intensity method with WCSs; H0: infinite intensities with HSPSs; H1: our proposed method with triggered and non-triggered HSPSs. (b). Optimal values of $\mu'$ for each curves that are listed in (a). The WCSs and the HSPSs used here are all in Poisson distribution.

the solid blue line (H0) shows the asymptotic case with HSPSs, and the red dotted line (H1) represents the result of our new scheme with triggered and non-triggered HSPSs. In the simulations above, we use the optimal values of $\mu'$ at each distance for all the lines. Just the difference is: For the asymptotic cases (W0 and H0), the fraction of two-single-photon counts and the QBER of two-single-photon pulses are known exactly; For the normal three
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 intensity $\mu$ and $\mu'$ to calculate $Y_{11}$ [15]. The HSPSs used here are all in poisson distributions. (b). Corresponding optimal values of $\mu'$ for all the lines in (a).

decoy-state case (W1), we use the parameters shown in Table I and assume a reasonable value for $\mu$ (0.2); While for our new scheme (H1), we use the same parameters as in Table I except that $\eta_A = \eta_B = 0.9$, and borrowing the relationship of $\mu$ and $\mu'$ from Eq. (8). Fig. 2(b) shows corresponding optimal values of $\mu'$ for each line in Fig. 2(a). Besides, The WCSs and the HSPSs used here are all in poisson distributions.

Fig. 3(a) and (b) are the comparison of our new MDI-QKD scheme with normal three decoy-state method [15] with HSPSs. Fig. 3(a) shows the the final key generation rate vs transmit distance, and Fig. 3(b) corresponds to the optimal values of $\mu'$. The lines H0 and H1 each corresponds to the asymptotic case with infinite decoy states and our new scheme, respectively. H2 represents the result of using normal three decoy-state method. Here the HSPSs used are all in poisson distributions.

Fig. 4(a) and (b) describe the different behavior of our new MDI-QKD scheme when using HSPSs in different distributions. The lines H0 and H1 each represents the result of
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.

(b) Optimal $\mu$.

From the comparison above we find that:

(i). Our new scheme of using triggered and non-triggered signals can work excellently close to the asymptotic case with infinite decoy-state method as in Fig 2(a) and (b). On one hand, it is due to the precise estimation of the tight bounds of $Y_{11}$ and $e_{11}$ by using both triggered and non-triggered signals as shown in Eq. (7) and (11-13); On the other hand, because we find optimal values for both $\mu$ and $\mu'$ at each distance by referring the relationship of $\mu$ and $\mu'$ from Eq. (8).

(ii). Our new MDI-QKD scheme with HSPSs can transmit a much longer distance compared with the one with WCSs (> 30km here) as shown in Fig. 2(a), which benefits from the substantial low vacuum components in the heralded signals.
(iii). In our new scheme, the HSPSs in poisson distributions show similar key generation rates as WCSs at short distances (< 200 km) and much higher key rates at long distances (> 200 km) as shown in Fig. 2(a), this is attributed to a much higher optimal value of $\mu'$ being used as shown in Fig. 2(b).

Moreover, our new scheme shows much better performance than normal decoy-state methods even when using the same HSPSs as shown in Fig. 3(a), because of a much higher optimal value of $\mu'$ being used as shown in Fig. 3(b).

In addition, when both applying our new scheme with HSPSs, the one in poisson distribution has better performance than the one in thermal distribution as shown in Fig. 4(a) and (b), that is benefit from a relatively higher single-photon probability in poisson distribution. It clearly demonstrates the necessity of exploiting poissonian distributed HSPS sources in QKD.

IV. CONCLUSIONS

In summary, we have studied the decoy-state MDI-QKD with heralded single photon source by using the triggered events of intensity $\mu$ and non-triggered events of the intensity $\mu'$. We show that this proposed implementation offers both a higher key generation rate and a longer transmission distance compared with existing realization methods. Therefore, it looks promising for practical applications in the near future.

V. ACKNOWLEDGMENTS

The author-Q. Wang thanks professor Z. Yang and B. Y. Zheng for useful discussion and kind support during the work. We also 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 and No. 60725416, and 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 Semiclassic. Opt. 8, 939 (1996).
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); N. Lütkenhaus, Phys. Rev. A, 61, 052304 (2000).

C. H. F. Fung et al., Phys. Rev. A 75, 032314 (2007); B. Qi et al., Quantum Inf. Comput. 7, 73 (2007); Y. Zhao et al., Phys. Rev. A 78, 042333 (2008).

L. Lydersen et al., Nature Photonics 4, 686 (2010); N. Jain, et al., Phys. Rev. Lett. 107, 110501 (2011).

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

D. Gottesman, H. K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. 4, 325 (2004).

W. Y. Hwang, Phys. Rev. Lett., 91, 057901 (2003);

X. B. Wang, Phys. Rev. Lett., 94, 230503 (2005);

H. K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett., 94, 230504 (2004).

D. Mayers and A. C. C. Yao, in Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS98) (IEEE Computer Society, Washington, DC, 1998), p. 503; A. Acn, N. Gisin, and L. Masanes, Phys. Rev. Lett. 97, 120405 (2006); A. Acn et al., Phys. Rev. Lett. 98, 230501 (2007).

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).

H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. 108, 130503 (2012).

S. L. Braunstein and S. Pirandola, preceding article, Phys. Rev. Lett. 108, 130502 (2012).

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.

X. B. Wang, Phys. Rev. A 87, 012320 (2013).

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

Q. Wang and A. Karlsson, Phys. Rev. A 76, 014309 (2007).

B. Yurke and M. Potasek, Phys. Rev. A 36, 3464 (1987).

N. Lütkenhaus, Phys. Rev. A 61, 052304 (2000).

S. Mori, J. Söderholm, N. Namekata and S. Inoue, 264, 156 (2006).

G. Ribordy, J. Brendel, J. D. Gautier, N. Gisin and H. Zbinden, Physical Review A, 63, 012309 (2000).

Adachi Y., Yamamoto T., Koashi M., and Imoto N., Phys. Rev. Lett. 99, 180503 (2007).
[23] R. Ursin, et al., Nat. Phys. 3, 481 (2007).