SCIENTIFIC REPORTS

OPEN

Realizing the measure-device-independent quantum-key-distribution with passive heralded-single photon sources

Received: 23 February 2016
Accepted: 28 September 2016
Published: 19 October 2016

Qin Wang[1,2,3], Xing-Yu Zhou[1,2] & Guang-Can Guo[1,2,3]

In this paper, we put forward a new approach towards realizing measurement-device-independent quantum key distribution with passive heralded single-photon sources. In this approach, both Alice and Bob prepare the parametric down-conversion source, where the heralding photons are labeled according to different types of clicks from the local detectors, and the heralded ones can correspondingly be marked with different tags at the receiver's side. Then one can obtain four sets of data through using only one-intensity of pump light by observing different kinds of clicks of local detectors. By employing the newest formulae to do parameter estimation, we could achieve very precise prediction for the two-single-photon pulse contribution. Furthermore, by carrying out corresponding numerical simulations, we compare the new method with other practical schemes of measurement-device-independent quantum key distribution. We demonstrate that our new proposed passive scheme can exhibit remarkable improvement over the conventional three-intensity decoy-state measurement-device-independent quantum key distribution with either heralded single-photon sources or weak coherent sources. Besides, it does not need intensity modulation and can thus diminish source-error defects existing in several other active decoy-state methods. Therefore, if taking intensity modulating errors into account, our new method will show even more brilliant performance.

The quantum key distribution (QKD) allows two legitimate users, usually called Alice and Bob, to share the secure cryptographic keys even at the existence of a malicious eavesdropper, Eve[1]. In principle, QKD can offer unconditional security guaranteed by the law of quantum physics[2–4]. However, due to existing imperfections in real-life QKD devices, Eve can take advantage of those loopholes and hack present QKD systems. For instance, under the circumstances of imperfect light sources, Eve can carry out the so-called photon-number-splitting (PNS) attack[5–7]. Fortunately, the decoy-state method was proposed to counter the PNS attack[8–10], dramatically improving the performance of practical QKD system[11–14]. Moreover, in order to countermeasure all the potential attacks directed on the detection devices, the measurement-device-independent quantum-key-distribution (MDI-QKD) protocols were proposed[15,16], which seems very promising in the implementations of QKD[17–27].

During the past few years, the MDI-QKD has been widely investigated using either the heralded-single photon sources (HSPS) or the weak coherent sources (WCS). By applying different number of decoy states, all of them can be classified into two types: the passive setup with only one intensity, and the active device with more than one intensity. For those active device, implementing two-, three- or four-intensity decoy states[17–25], where in real-life, an acousto- or electro-optic modulator is often used to switch between different decoy states with high speed, they will inevitably result in intensity uncertainty during parameter estimations, and thus deteriorate their practical performance. For passive setups[28], one has to do the worst-case parameter estimation on the contributions from two-single-photon pulses owning to very few input parameters. Here, we will present a new scheme on implementing the MDI-QKD protocol with HSPS while using only one-intensity decoy state. In this scheme, we record all the successful detection events and mark them with different tags by classifying the heralding photons

[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. Correspondence and requests for materials should be addressed to Q.W. (email: qinw@njupt.edu.cn)

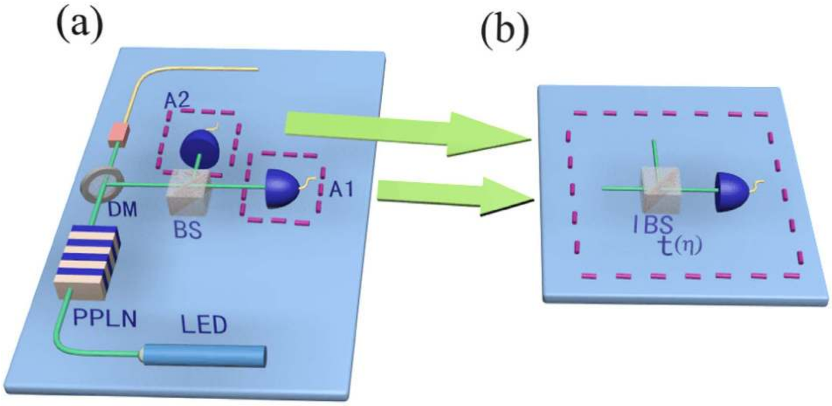

Figure 1. (**a**) The schematic setup of generating the passive HSPS. The pump light is generated from a light emitting diode (LED). After passing though the Periodically Poled Lithium Niobate (PPLN) crystal, the parametric down-conversion photon pairs (idler and signal) are separated by a dichroic mirror (DM). The idler mode is split into two parts by a beam-splitter (BS) and sent into two single-photon detectors (A_1 and A_2) respectively. (**b**) The illustration of single-photon detection in the idler mode, where an imaginary beam-splitter (IBS) is positioned before each local detector. t is the IBS transmissivity.

into different species, so that we can possess many input parameters and carry out very accurate estimations for the two-single-photon pulse contributions.

The paper is organized as follow: At the beginning, we present the core idea on how to generate the passive heralded single-photon sources; Second, we propose to implement the passive heralded single-photon sources into the MDI-QKD; Third, we carry out corresponding numerical simulations and compare its performance with other often used decoy-state proposals, e.g., the standard three-intensity decoy-state MDI-QKD using either the HSPS or the WCS. Finally, a summary and outlook are given at the end of the paper.

The passive heralded single-photon sources

Normally, the HSPS can be generated from the parametric down-conversation (PDC) process, which can be either a thermal or poissonian distribution[12]. For simplicity, here we use the poissonian distributed PDC source as an example to describe the scheme. (In the case of thermal distribution, it will show similar behavior). The PDC process can generate a squeezed two-mode field, each denoted as the idler mode (I mode) and the signal mode (S mode) individually. The two-mode field can be written as: $|\Psi\rangle_{\mathrm{IS}} = \sum_{n=0}^{\infty}\sqrt{\mathrm{P_n}}|n\rangle_{\mathrm{I}}|n\rangle_{\mathrm{S}}$, where $|n\rangle$ represents an n-photon state, $P_n(\mu) = \frac{\mu^n}{n!}e^{-\mu}$, and μ is the average photon number per time slot.

In most former HSPS schemes, the idler mode is often locally detected with a photon diode at the sender's side, and the signal mode is encoded with useful information and sent to the receiver through the quantum channel. Meanwhile, the sender delivers a synchronization signal to the receiver whenever the local phot-diode clicks. This is the so-called HSPS. However, below we will configure the devices in a different manner.

The schematic setup of our new scheme on generating the passive HSPS is shown in Fig. 1, where the most important change is to split the idler mode into two paths and then send each into a local single-photon detector (A_1 and A_2) separately. In all, the click events in the two local detectors may consist of four kinds of possibilities, each denoted as X_i ($i = 1, 2, 3, 4$): (1) Non-clicking; (2) Only one clicking at A_1; (3) Only one clicking at A_2; (4) Clicking at both A_1 and A_2.

We define $\mathrm{P}_{\mathrm{X_i}|n}$ as the probability of the X_i events occurring if given an n-photon state in the idler mode. Then the signal state will be projected into $\rho = \sum f_n \mathrm{P}_{\mathrm{X_i}|n}|n\rangle\langle n|$ (un-normalized), where f_n is the photon-number distribution in the S mode. In the following, let's derive the construction of the X_i event. To simplify the description, let's begin with perfect detector efficiency for A_1 and A_2, and we will deal a bit later in the manuscript with non-unity detector efficiency by assuming "imaginary beam splitters".

First, we denote $\mathrm{P}_{\mathrm{x_i}|s_1s_2}$ as the probability of the X_i event occurring given a $|s_1s_2\rangle$ projection state. For a vacuum projection state, the corresponding local detector will click with a probability of d_i (the dark count rate), and non-clicking with a probability of $(1 - d_i)$. While for a non-vacuum projection state, the local detector will surely click with 100% probability. We can then list all the probabilities of the four (X_i) events taking place as shown in Table 1.

Second, we define $\mathrm{P}_{s_1s_2|n}$ as the probability of projecting an n-photon state into state $|s_1s_2\rangle$. For an n-photon number state, after passing through a beam-splitter (BS) in the idler mode, it is changed into:

$$\frac{1}{\sqrt{n!}}(Ta_1^{\dagger} + Ra_2^{\dagger})^n|0\rangle = \frac{1}{\sqrt{n!}}\sum_{k=0}^{n}\mathrm{C}_n^k R^{n-k}T^k a_1^{\dagger k} a_2^{\dagger n-k}|0\rangle, \tag{1}$$

Case	$P_{1\|s_1s_2}$	$P_{2\|s_1s_2}$	$P_{3\|s_1s_2}$	$P_{4\|s_1s_2}$
$X_1: s_1=0, s_2=0$	$(1-d_1)(1-d_2)$	$d_1(1-d_2)$	$d_2(1-d_1)$	d_1d_2
$X_2: s_1\neq 0, s_2=0$	0	$(1-d_2)$	0	d_2
$X_3: s_1=0, s_2\neq 0$	0	0	$(1-d_1)$	d_1
$X_4: s_1\neq 0, s_2\neq 0$	0	0	0	1

Table 1. Probability of the (X_i) event occurring.

where the right side of the equation follows a binomial distribution, and C_n^k is the binomial coefficient, defined as $C_n^k =: \frac{n!}{k!(n-k)!}$; T^2 represents the transmission efficiency of the BS, denoted as t; R^2 corresponds to the reflection efficiency, denoted as $(1-t)$.

As illustrated in Fig. 1, after the first BS we combine the coupling efficiency and detection efficiency in each path, and treat it as the transmission efficiency (η_i, $i=1, 2$) of an imaginary beam-splitter (IBS), and the loss corresponds to the reflection efficiency $(1-\eta_i)$. After passing through the two IBSs, only the transmitted photons are collected. Now the state can be expressed as:

$$\begin{aligned} |\Psi\rangle = \frac{1}{\sqrt{n!}}\sum_{k=0}^{n}\sum_{s_2=0}^{n-k}\sum_{s_1=0}^{k} C_n^k T^k R^{n-k} C_k^{s_1} T_1^{s_1} R_1^{k-s_1} C_{n-k}^{s_2} T_2^{s_2} R_2^{n-k-s_2} a_1'^{\dagger s_1} a_2'^{\dagger s_2} b_1'^{\dagger k-s_1} \\ b_2'^{\dagger n-k-s_2}|0\rangle, \end{aligned} \tag{2}$$

where $\mathrm{T_i} = \sqrt{\eta_\mathrm{i}}$, and $\mathrm{R_i} = \sqrt{1-\eta_\mathrm{i}}$, $(i=1, 2)$.

Then we can get the corresponding projection probability as:

$$\begin{aligned} \mathrm{P}_{s_1s_2|n} &= \frac{1}{n!}\sum_{k=0}^{n}\sum_{s_2=0}^{n-k}\sum_{s_1=0}^{k} |C_n^k C_k^{s_1} C_{n-k}^{s_2} T^k R^{n-k} T_1^{s_1} R_1^{k-s_1} T_2^{s_2} R_2^{n-k-s_2}|^2 s_1! s_2! (k-s_1)! \\ &\quad \times (n-k-s_2)! \\ &= \sum_{k=0}^{n}\sum_{s_2=0}^{n-k}\sum_{s_1=0}^{k} \frac{n!}{s_1! s_2! (k-s_1)! (n-k-s_2)!} t^k (1-t)^{n-k} \eta_1^{s_1} \eta_2^{s_2} \\ &\quad \times (1-\eta_1)^{k-s_1} (1-\eta_2)^{n-k-s_2}. \end{aligned} \tag{3}$$

For any input n-photon state, the probability of occurring the X_i heralding event can be written as:

$$\mathrm{P}_{\mathrm{x_i}|n} = \sum_{s_1,s_2} \mathrm{P}_{\mathrm{x_i}|s_1s_2} \cdot \mathrm{P}_{s_1s_2|n}. \tag{4}$$

The corresponding heralded signal state is :

$$\rho = \sum_{n,s_1,s_2} f_n \mathrm{P}_{\mathrm{x_i}|s_1s_2} \cdot \mathrm{P}_{s_1s_2|n} |n\rangle\langle n|, \tag{5}$$

where the analysis of $\mathrm{P}_{\mathrm{x_i}|s_1s_2}$ can be found in Table 1, and $\mathrm{P}_{s_1s_2|n}$ has been formulated in Eq. (3). Now with the above, we can do the calculation for any X_i event and any quantum efficiency.

In the following, we will denote the above X_1, X_2 and X_3 events as the x, y and z state respectively. Correspondingly, in the photon-number space, we have $\rho_\xi = \sum_n P_n^\xi |n\rangle\langle n|$, with $P_n^\xi = f_n \mathrm{P}_{\mathrm{x_i}|n}$, $(\xi = x, y, z)$.

According to Eqs (1–5), we get the simplified photon-number distribution for the x, y and z state as

$$\begin{aligned} P_n{}^x &= (1-d)^2(1-\eta_A)^n \frac{\mu^n}{n!} e^{-\mu}, \\ P_n{}^y &= (1-d)(1-\eta_A)^n \left[\left(1+\frac{t\eta_A}{1-\eta_A}\right)^n + d - 1\right] \frac{\mu^n}{n!} e^{-\mu}, \\ P_n{}^z &= (1-d)(1-\eta_A)^n \left[\left(\frac{1-t\eta_A}{1-\eta_A}\right)^n + d - 1\right] \frac{\mu^n}{n!} e^{-\mu}. \end{aligned} \tag{6}$$

Here for simplicity we have assumed that all the local detectors have the same dark count rate, i.e., $d_i = d$. Besides, we reasonably set $t \in \left[0, \frac{1}{2}\right]$, and $\eta_A \in [0, 1]$.

For any $n \geqslant 2$, we find

$$\begin{aligned}\frac{{P_n}^y}{{P_n}^x}-\frac{{P_{n-1}}^y}{{P_{n-1}}^x} &= \frac{\left(1+\frac{t\eta_A}{1-\eta_A}\right)^n+d-1}{1-d}-\frac{\left(1+\frac{t\eta_A}{1-\eta_A}\right)^{n-1}+d-1}{1-d_A}\\ &= \frac{\frac{t\eta_A}{1-\eta_A}\left(1+\frac{t\eta_A}{1-\eta_A}\right)^{n-1}}{1-d}\geq 0\end{aligned} \tag{7}$$

and

$$\begin{aligned}\frac{{P_n}^z}{{P_n}^y} &\geq \frac{\left(1+\frac{t\eta_A}{1-\eta_A}\right)\left[1+\frac{(1-t)\eta_A}{1-\eta_A}\right]^{n-1}+d-1}{\left(1+\frac{t\eta_A}{1-\eta_A}\right)^n+d-1}=\frac{\left[1+\frac{(1-t)\eta_A}{1-\eta_A}\right]^{n-1}+\frac{d-1}{1+\frac{t\eta_A}{1-\eta_A}}}{\left(1+\frac{t\eta_A}{1-\eta_A}\right)^{n-1}+\frac{d-1}{1+\frac{t\eta_A}{1-\eta_A}}}\\ &\geq \frac{\left[1+\frac{(1-t)\eta_A}{1-\eta_A}\right]^{n-1}+d-1}{\left(1+\frac{t\eta_A}{1-\eta_A}\right)^{n-1}+d-1}=\frac{{P_{n-1}}^z}{{P_{n-1}}^y}.\end{aligned} \tag{8}$$

With the conditions above, we get the following inequalities:

$$\begin{aligned}\frac{{P_n}^y}{{P_n}^x} \geqslant \frac{{P_{n-1}}^y}{{P_{n-1}}^x} \geqslant \frac{{P_1}^y}{{P_1}^x},\\ \frac{{P_n}^z}{{P_n}^y} \geqslant \frac{{P_{n-1}}^z}{{P_{n-1}}^y} \geqslant \frac{{P_1}^z}{{P_1}^y}.\end{aligned} \tag{9}$$

For further discussion, we define another useful quantity $G(i,\,j,\,k)=({g_i}^x-{g_j}^x)({g_j}^y-{g_k}^y)-({g_i}^y-{g_j}^y)({g_j}^x-{g_k}^x)$ where ${g_l}^\xi:=\frac{{P_l}^\xi}{{P_l}^z}$, $\xi = x, y, z, l\geqslant 1$.

For any $k-j\geqslant j-i\geqslant 0$, we can demonstrate

$$G(i,\,j,\,k)\geqslant 0. \tag{10}$$

See the "Proof" section for the detailed proof. With the two inequalities, one can directly apply Wang's formulas for the yield and phase-flip rate of single-photon pairs in ref. 25.

Implementing the passive HSPS into the MDI-QKD

The MDI-QKD was designed to remove all possible side-channel attacks and show attractive performance in real-life implementation. In MDI-QKD, both Alice and Bob send signals to an untrusted third party (UTP), Charlie. After a Bell state measurement, Charlie announces whether the measurement is successful. Then the successful event will be employed for key distribution. In order to make the MDI-QKD more practical, usually a decoy-state method is implemented in parallel. In most other schemes, it requires both Alice and Bob to randomly modulate their signal light into different intensities, and then do estimations with corresponding successful events. While here in our new scheme, only one-intensity signal light is applied at either Alice or Bob's side, and then process parameter estimations by considering different counting events conditional on case X_i ($i = 1, 2, 3$, i.e., x, y and z state) as introduced above. The schematic experimental setup of the scheme is shown in Fig. 2.

In fact, the security of our proposal is equivalent to the processes as following: First, both Alice and Bob send out all heralded signal pulses (signal mode), and the UTP records all the successful counting events by do projecting measurement; Second, Alice and Bob start to send out heralding signals from local detectors, and correspondingly the UTP can divide all the successful counting events into different species (signal states or decoy states) and marked with different tags; Third, the UTP announce the tags of each successful event, and the legitimate users apply corresponding bit-flip operations and get the raw keys; Moreover, error correction and privacy amplification processes are carried out; Finally, people carry out parameter estimation processes. From the above, we find that during the signal transmission Eve is unable to judge which is the signal state and which is the decoy state, and has to apply the same attack strategy on all the pulses (signal state and decoy state), and his eavesdropping will certainly be discovered by the legitimate users by error tests.

In this scheme, for simplicity, we assume both Alice and Bob possess the same passive setup for signal generation. Then each of them can send out signals with x, y and z state individually. Whenever Alice sends out an α state and Bob sends out a β, with $\alpha,\,\beta\in(x,\,y,\,z)$, the average counting rate ($Q^W_{\alpha,\beta}$) and the mean quantum-bit errors ($T^W_{\alpha,\beta}:=E^W_{\alpha,\beta}Q^W_{\alpha,\beta}$) can be written as:

$$Q^W_{\alpha,\beta}=\sum_{n,m=0}^{\infty}{P_n}^\alpha{P_m}^\beta Y^W_{nm}\quad and\quad T^W_{\alpha,\beta}=\sum_{n,m=0}^{\infty}{P_n}^\alpha{P_m}^\beta e^W_{nm}Y^W_{nm}, \tag{11}$$

where we label W as the Z- or X-basis. The Z- or X-basis can be considered independently, hereafter we shall therefore omit the superscript W without causing any confusion. The subscripts n, m each represents the numbers

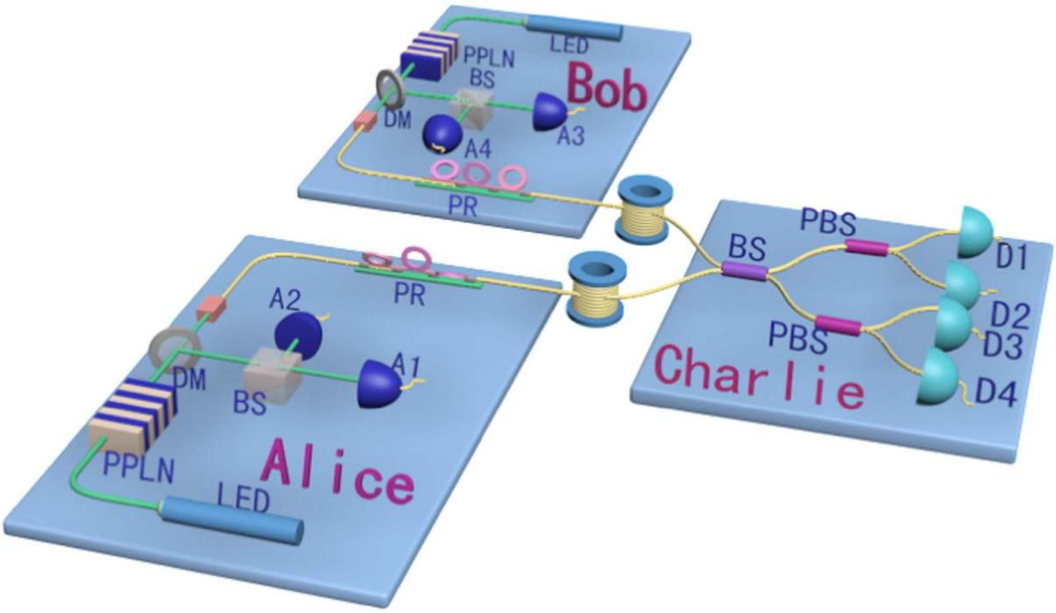

Figure 2. The schematic setup of our new passive-decoy state MDI-QKD protocol. Alice and Bob generate the passive HSPS as illustrated in Fig. 1, and randomly code each signal pulse into one of the four polarization states (horizontal (*H*), vertical (*V*), 45 degrees (+) and 135 degrees (−)) with a polarization rotator (PR). Then they simultaneously send their signal pulses to the third party (Charlie) through the quantum channel. Charlie apply a partial Bell-state projection measurement on pulses from both Alice and Bob. A_i ($i=1, 2, 3, 4$): triggering single-photon detectors. D_i ($i=1, 2, 3, 4$): triggered single-photon detectors. PBS: polarization beam-splitter. BS: beam-splitter.

of the photons sent by Alice or Bob respectively. Y_{nm}^{W} and e_{nm}^{W} each corresponds to the conditional yield or the error rate when Alice sends an *n*-photon state and Bob sends an *m*-photon state. $E_{\alpha,\beta}^{W}$ denotes the average quantum-bit error-rate.

Below we define

$$\widetilde{Q}_{\alpha,\beta} := \sum_{n,m=1}^{\infty} P_n^{\alpha} P_m^{\beta} Y_{nm} \quad and \quad \widetilde{T}_{\alpha,\beta} := \sum_{n,m=1}^{\infty} P_n^{\alpha} P_m^{\beta} e_{nm} Y_{nm} \tag{12}$$

with

$$\begin{aligned} \widetilde{Q}_{\alpha,\beta} &= Q_{\alpha,\beta} - {P_0}^{\alpha} Q_{0\beta} - {P_0}^{\beta} Q_{\alpha 0} + {P_0}^{\alpha} {P_0}^{\beta} Q_{00}, \\ \widetilde{T}_{\alpha,\beta} &= T_{\alpha,\beta} - {P_0}^{\alpha} T_{0\beta} - {P_0}^{\beta} T_{\alpha 0} + {P_0}^{\alpha} {P_0}^{\beta} T_{00}. \end{aligned} \tag{13}$$

According to Wang *et al.*'s work in ref. 25, once the source states satisfy the inequalities in (9) and (10), we can immediately get the lower-bound of the counting rate for the two-single-photon pulses (Y_{11}^{L}) as

$$Y_{11}^{L} = \frac{({P_1}^{\alpha} {P_2}^{\beta} + {P_1}^{\beta} {P_2}^{\alpha}) \widetilde{Q}_{\alpha,\alpha} - {P_1}^{\alpha} {P_2}^{\alpha} (\widetilde{Q}_{\alpha,\beta} + \widetilde{Q}_{\beta,\alpha})}{P_1^{\alpha 2} ({P_1}^{\alpha} {P_2}^{\beta} - {P_1}^{\beta} {P_2}^{\alpha})}. \tag{14}$$

Similarly, we can get the upper bound of the quantum-bit error-rate for the two-single-photon pulses (e_{11}^{U})[25]:

$$e_{11}^{U} = \frac{1}{\gamma^2 Y_{11}^{L}} \begin{vmatrix} \widetilde{T}_x & \widetilde{T}_y & \widetilde{T}_z \\ {P_2}^x & {P_2}^y & {P_2}^z \\ {P_3}^x & {P_3}^y & {P_3}^z \end{vmatrix}, \tag{15}$$

where $\gamma = P_1^z P_2^z P_3^z G(1, 2, 3)$, for $\xi \in (x, y, z)$, $\widetilde{T}_{\xi} := ({g_2}^y - {g_3}^y) \widetilde{T}_{\xi,x} - ({g_2}^x - {g_3}^x) \widetilde{T}_{\xi,y} + ({g_3}^y {g_2}^x - {g_3}^x {g_2}^y) \widetilde{T}_{\xi,z}$.

In the new scheme, the Z-basis is used for key generation, and the X-basis is for error testing. From Eqs (14) and (15), we can obtain the lower-bound for the yield of two-single-photon pulses in the Z basis ($Y_{11}^{Z,L}$) and the upper-bound for the quantum-bit error-rate of two-single-photon pulses in the X basis ($e_{11}^{X,U}$). Moreover, the average counting rate and the mean quantum-bit error-rate can be observed experimentally. With all the above, we can calculate the secure key generation rate with the following formula:

η_C	d_C	e_d	e_0	γ
14.5%	3.0×10^{-6}	1.5%	0.5	0.2 dB/km

Table 2. Parameters values for simulations. η_C and d_C are the detection efficiency and dark count rate at the UTP's side; e_d is the probability that the survived photon hits the wrong detector, which is independent of the transmission distance, and e_0 is the error rate of dark count; γ is the channel loss constant.

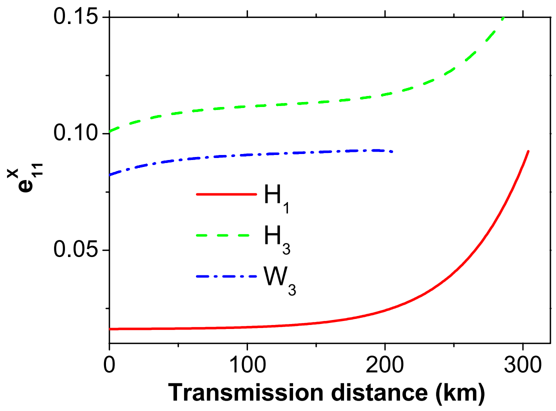

Figure 3. Comparison of the estimation value of e_{11}^{X} between different methods. The solid line (H_1) refers to our new scheme, the dashed line (H_3) represents the standard three-intensity decoy-state MDI-QKD using HSPS, and the dash-dotted line (W_3) corresponds to the case of using conventional three-intensity decoy-state MDI-QKD using WCS. For simplicity, we set the intensity of the decoy state as $\nu = 0.1$ for H_3 and W_3.

$$R \geq (P_1^{y2} + P_1^{z2}) Y_{11}^{Z,L}[1 - H(e_{11}^{X,U})] - Q_{y,y}^{Z} f H(E_{y,y}^{Z}) - Q_{z,z}^{Z} f H(E_{z,z}^{Z}), \quad (16)$$

where f is the error correction efficiency, and here we take $f = 1.16$[16,18]; $H(p) := -p\log_2(p) - (1-p)\log_2(1-p)$. To simplify the calculation, we only use the y and z state for the key distillation. In fact, all the four kinds of events (X_i, $i = 1, 2, 3, 4$) can be used to distill the final keys. That means the performance of the new scheme should be even better when taking all the successful events into consideration.

Numerical simulation

With the formulae above, we can perform a numerical simulation for our new passive scheme on the decoy-state MDI-QKD, and further compare its performance with other practical methods, e.g. the conventional three-intensity decoy-state MDI-QKD using either WCS or HSPS[17,22]. In real-life experiment, the average gains and the average quantum-bit error-rates can be directly measured. While in numerical simulations, we should use a reasonable model to predict what *should probably be observed* in experiment. By referring the linear model in ref. 19, we can give a prediction for the *probably observed* values of the gains and the quantum-bit error-rates. For fair comparison, we assume the same parameters as in refs 16 and 18 in our simulation, see Table 2.

In the source generation part, the non-degenerate parametric down-conversion process is often used to generate non-degenerated photon pairs, e.g., one is within the telecommunication wavelength range suitable for fiber transmission, and the other is within the visible wavelength range, convenient for detection. Therefore, it is reasonable to assume the local detectors with a detection efficiency of 75%, and a dark count rate of 10^{-6} (commercial products SPCM-NIR-16 or SPCM-AQRH-16 APD)[25]. Corresponding simulation results have been displayed in Figs 3, 4, 5 and 6.

In Fig. 3, we compare the estimation value for the quantum-bit error-rate of two-single-photon pulses (e_{11}^{X}) among our new scheme (H_1), the conventional three-intensity decoy-state MDI-QKD using HSPSs (H_3)[22] and the standard three-intensity decoy-state MDI-QKD using WCSs (W_3)[17]. We can find from Fig. 3 that, our new scheme shows significantly lower bound of the e_{11} than the other two schemes, which is on one hand due to the many kinds of successful counting events, and on the other hand owning to the usage of the newest estimating formula, Eq. (15).

The comparison of Y_{11} in the Z basis between the above three methods is shown in Fig. 4. The conventional three-intensity decoy-state MDI-QKD using the HSPS (H_3) and using the WCS (W_3) shows a similar level of Y_{11}^{Z}. In contrast to them, the new proposed passive MDI-QKD (H_1) obviously exhibits higher values.

In Fig. 5, we show a comparison for the optimal intensity of the signal state (μ) for different kinds of methods. Compared with the other two lines (W_3 and H_3), our new passive scheme (H_1) presents superior values from the beginning to the end.

Moreover, we show a comparison for the key generation rate (R) for our new passive scheme(H_1), for the standard three-intensity decoy-state MDI-QKD using HSPSs (H_3), and for the conventional three-intensity decoy-state MDI-QKD using WCSs (W_3), see Fig. 6(a). Compared with the other two proposals, the performance

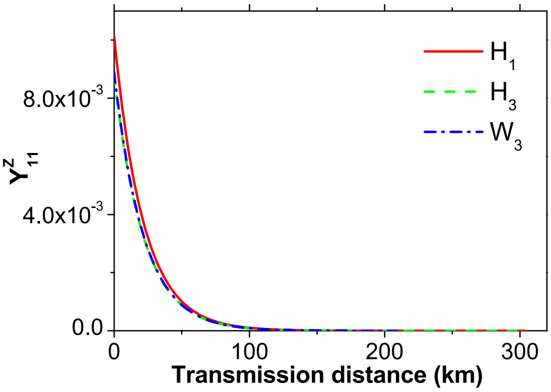

Figure 4. Comparison of the estimation value of Y_{11}^{Z} between different methods. The solid line (H_1) refers to our new scheme, the dashed line (H_3) represents the standard three-intensity decoy-state MDI-QKD using HSPS, and the dash-dotted line (W_3) corresponds to the case of using conventional three-intensity decoy-state MDI-QKD using WCS. For simplicity, we set the intensity of the decoy state as $v = 0.1$ for H_3 and W_3.

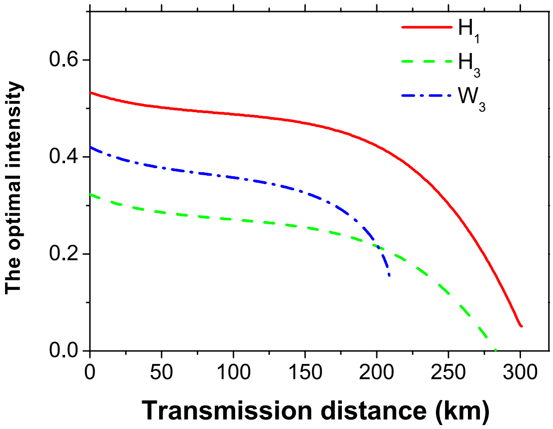

Figure 5. Comparison of the optimal intensity of the signal state *u* between different methods. The solid line (H_1) refers to our new scheme, the dashed line (H_3) represents the standard three-intensity decoy-state MDI-QKD using HSPS, and the dash-dotted line (W_3) corresponds to the case of using conventional three-intensity decoy-state MDI-QKD using WCS. For simplicity, we set the intensity of the decoy state as $v = 0.1$ for H_3 and W_3.

of our new scheme has drastically improved both the transmission distance and the final key generation rate. For a more vivid comparison, we also calculate the relative key generation rate between our new passive scheme and the other two three-intensity decoy-state methods, see the left and right axes in Fig. 6(b), respectively. We find that compared with the standard three-intensity decoy-state MDI-QKD using HSPSs, our new passive scheme can obtain more than five times enhancement in the key generation rate at long distances (>200 *km*). While compared with the conventional three-intensity decoy-state MDI-QKD using WCSs, it can exhibit more than 100% enhancement in the key generation rate, and achieve more than 100 *km* longer transmission distance.

Conclusion

In summary, we have introduced a new protocol for the measurement-device-independent quantum-key-distribution with heralded single-photon sources involving only one-intensity decoy state. The key features are: At the source generation part, we split the triggering signals and send into different local detectors. By recording different kinds of detection events in the local detectors, we can divide the triggered events into different species at the receiver's side. Moreover, during parameter estimations, we have implemented the newest formulae, i.e., Eqs (14) and (15) to give an upper or lower bound for the counting rate and the quantum-bit error-rate of two-single-photon pulses. Consequently, we obtain many input parameters and can do very accurate estimations for the two-single-photon pulse contributions. Furthermore, by carry out corresponding numerical calculations, we compare the new scheme with other often used three-intensity decoy-state methods, demonstrating that the new proposed approach could exhibit outstanding performance among those compared.

Besides, we should declare that if we take the source errors into consideration, the new proposed passive scheme will exhibit even predominant capability than those active decoy-state methods. Because no intensity modulator is applied in our new scheme, and thus avoids source uncertainties. These unfortunately exist in other

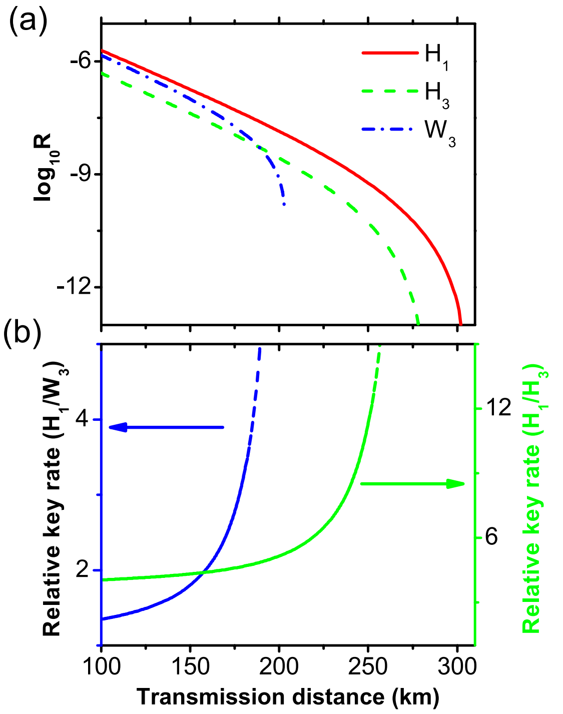

Figure 6. (**a**) Comparison of the final key generation rate R between different methods. The solid line (H_1) refers to our new scheme, the dashed line (H_3) corresponds to the standard three-intensity scheme using HSPS, and the dash-dotted line (W_3) represents a conventional three-intensity MDI-QKD using WCS. (**b**) The ratio between the key generation rates of the new proposed passive scheme and the other two, see the left and right axes respectively.

two-, three-, or four-intensity decoy-state methods. Therefore, it may be a promising candidate for the implementation of quantum key distribution in the near future.

In addition, we have noted that recently a new novel four-intensity decoy-state protocol [Phys. Rev. A 93, 042324 (2016)] have been proposed by Wang *et al.*[29], which shows excellent performance when accounting for statistical fluctuation and using biased basis. It should be interesting to implement their method into our present passive scheme which deserves further study in our future research.

Proof

In order to demonstrate inequality (10), which states that $G(i, j, k) \geqslant 0$, when $k - j \geqslant j - i \geqslant 0$, we recall that the Vandermonde determinant defined as

$$V_n := \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \gamma_1 & \gamma_2 & \cdots & \gamma_n \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_1^{n-1} & \gamma_2^{n-1} & \cdots & \gamma_n^{n-1} \end{vmatrix}$$

satisfies $V_n > 0$ for any $0 < \gamma_1 < \gamma_2 < \cdots < \gamma_n$, which follows from $V_n = \Pi_{i<j}(\gamma_j - \gamma_i)$. Now we establish the result which will be used in deriving inequality (10): The generalized Vandermonde determinant defined as

$$D_n := \begin{vmatrix} \gamma_1^{\lambda_1} & \gamma_2^{\lambda_1} & \cdots & \gamma_n^{\lambda_1} \\ \gamma_1^{\lambda_2} & \gamma_2^{\lambda_2} & \cdots & \gamma_n^{\lambda_2} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_1^{\lambda_n} & \gamma_2^{\lambda_n} & \cdots & \gamma_n^{\lambda_n} \end{vmatrix}$$

satisfies $D_n > 0$ for any $0 < \gamma_1 < \gamma_2 < \cdots < \gamma_n$ and $0 \leqslant \lambda_1 < \lambda_2 < \cdots < \lambda_n$.

To establish this, we proceed by induction method. First, it is clear that $D_1 > 0$. Now assume that $D_{n-1} > 0$, we will show that $D_n > 0$. Note that

$$D_n = \gamma_1^{\lambda_1}\gamma_2^{\lambda_1}\ldots\gamma_n^{\lambda_1} \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \gamma_1^{\lambda_2-\lambda_1} & \gamma_2^{\lambda_2-\lambda_1} & \cdots & \gamma_n^{\lambda_2-\lambda_1} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_1^{\lambda_n-\lambda_1} & \gamma_2^{\lambda_n-\lambda_1} & \cdots & \gamma_n^{\lambda_n-\lambda_1} \end{vmatrix},$$

in order to show that $D_n > 0$, we may assume without loss of generality that $\lambda_1 = 0$, and only consider D_n of the following form

$$D_n = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \gamma_1^{\lambda_2} & \gamma_2^{\lambda_2} & \cdots & \gamma_n^{\lambda_2} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_1^{\lambda_n} & \gamma_2^{\lambda_n} & \cdots & \gamma_n^{\lambda_n} \end{vmatrix}. \tag{17}$$

We will show that $D_n > 0$ for $0 \leqslant \lambda_1 < \lambda_2 < \cdots < \lambda_n$.

First, consider D_n as a function of γ_n and note that $D_n|_{\gamma_n = \gamma_{n-1}} = 0$. If we can show that $\frac{\partial D_n}{\partial \gamma_n} \geqslant 0$ for $\gamma_n > \gamma_{n-1}$, then we are done. Consider $\frac{\partial D_n}{\partial \gamma_n}$ as a function of γ_{n-1}, we have $\left.\frac{\partial D_n}{\partial \gamma_n}\right|_{\gamma_n = \gamma_{n-1}} = 0$. Thus it suffices to show that $\frac{\partial^2 D_n}{\partial \gamma_n \partial \gamma_{n-1}} \geqslant 0$ for $\gamma_{n-1} > \gamma_{n-2}$. If one proceeds similarly, it suffices to show that

$$\frac{\partial^{n-1} D_n}{\partial \gamma_n \partial \gamma_{n-1} \cdots \partial \gamma_2} \geqslant 0.$$

From Eq. (17) it is clear that

$$\begin{aligned} \frac{\partial^{n-1} D_n}{\partial \gamma_n \partial \gamma_{n-1} \cdots \partial \gamma_2} &= \lambda_n \lambda_{n-1} \cdots \lambda_2 \begin{vmatrix} 1 & 0 & \cdots & 0 \\ \gamma_1^{\lambda_2} & \gamma_2^{\lambda_2 - 1} & \cdots & \gamma_n^{\lambda_2 - 1} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_1^{\lambda_n} & \gamma_2^{\lambda_n - 1} & \cdots & \gamma_n^{\lambda_n - 1} \end{vmatrix} \\ &= \lambda_n \lambda_{n-1} \cdots \lambda_2 \begin{vmatrix} \gamma_2^{\lambda_2 - 1} & \cdots & \gamma_n^{\lambda_2 - 1} \\ \vdots & \ddots & \vdots \\ \gamma_2^{\lambda_n - 1} & \cdots & \gamma_n^{\lambda_n - 1} \end{vmatrix}, \end{aligned}$$

which is positive by assumption.

With the above preparation, we proceed to prove inequality (10). As introduced above, in the new passive decoy-state scheme, Bob's counting events can be divided into four species by conditioning them on Alice's heralding events X_i, ($i = 1, 2, 3$ and 4). The first three have been denoted as states x, y and z respectively, and their photon-number distribution can be written as in Eq. (6). By substituting Eq. (6) into condition (10), we obtain

$$\begin{aligned} &G(i, j, k) \\ &= \left[\frac{1}{\left(\frac{1 - t\eta_A}{1 - \eta_A}\right)^i - 1} - \frac{1}{\left(\frac{1 - t\eta_A}{1 - \eta_A}\right)^j - 1}\right]\left[\frac{\left(1 + \frac{t\eta_A}{1 - \eta_A}\right)^j - 1}{\left(\frac{1 - t\eta_A}{1 - \eta_A}\right)^j - 1} - \frac{\left(1 + \frac{t\eta_A}{1 - \eta_A}\right)^k - 1}{\left(\frac{1 - t\eta_A}{1 - \eta_A}\right)^k - 1}\right] \\ &\quad - \left[\frac{\left(1 + \frac{t\eta_A}{1 - \eta_A}\right)^i - 1}{\left(\frac{1 - t\eta_A}{1 - \eta_A}\right)^i - 1} - \frac{\left(1 + \frac{t\eta_A}{1 - \eta_A}\right)^j - 1}{\left(\frac{1 - t\eta_A}{1 - \eta_A}\right)^j - 1}\right]\left[\frac{1}{\left(\frac{1 - t\eta_A}{1 - \eta_A}\right)^j - 1} - \frac{1}{\left(\frac{1 - t\eta_A}{1 - \eta_A}\right)^k - 1}\right] \\ &= (b_i - b_j)(a_j b_j - a_k b_k) - (a_i b_i - a_j b_j)(b_j - b_k) \\ &= -\left[a_k b_k (b_i - b_j) - a_j b_j (b_i - b_k) + a_i b_i (b_j - b_k)\right] \\ &= -\begin{vmatrix} a_i b_i & a_j b_j & a_k b_k \\ a_i & a_j & a_k \\ 1 & 1 & 1 \end{vmatrix}, \end{aligned}$$

where $a_n = \left(1 + \frac{t\eta_A}{1 - \eta_A}\right)^n - 1$, $b_n = \frac{1}{\left(\frac{1 - t\eta_A}{1 - \eta_A}\right)^n - 1}$. In order to show $G(i, j, k) \geqslant 0$, it suffices to show that

$$D = \begin{vmatrix} a_i b_i & a_j b_j & a_k b_k \\ b_i & b_j & b_k \\ 1 & 1 & 1 \end{vmatrix} \leq 0.$$

We denote $c = \frac{1 - \eta_A}{1 - t\eta_A}$, $d = \frac{1 - \eta_A}{1 - \eta_A + t\eta_A}$, so $a_n = \frac{1}{d^n} - 1, b_n = \frac{1}{\frac{1}{c^n} - 1} = \frac{c^n}{1 - c^n}$.

Note that

$$\begin{aligned} D &= \begin{vmatrix} \left(\frac{1}{d^i} - 1\right)\frac{c^i}{1 - c^i} & \left(\frac{1}{d^j} - 1\right)\frac{c^j}{1 - c^j} & \left(\frac{1}{d^k} - 1\right)\frac{c^k}{1 - c^k} \\ \frac{c^i}{1 - c^i} & \frac{c^j}{1 - c^j} & \frac{c^k}{1 - c^k} \\ 1 & 1 & 1 \end{vmatrix} \\ &= \frac{1}{(1 - c^i)(1 - c^j)(1 - c^k)} \begin{vmatrix} \left(\frac{1}{d^i} - 1\right)c^i & \left(\frac{1}{d^j} - 1\right)c^j & \left(\frac{1}{d^k} - 1\right)c^k \\ c^i & c^j & c^k \\ 1 - c^i & 1 - c^j & 1 - c^k \end{vmatrix} \\ &= \frac{1}{(1 - c^i)(1 - c^j)(1 - c^k)} \begin{vmatrix} \left(\frac{c}{d}\right)^i & \left(\frac{c}{d}\right)^j & \left(\frac{c}{d}\right)^k \\ c^i & c^j & c^k \\ 1^i & 1^j & 1^k \end{vmatrix}. \end{aligned}$$

Due to the $t \in \left[0, \frac{1}{2}\right]$, we can get $0 < c < d$, and $c < \frac{c}{d} < 1$. Thus,

$$G(i, j, k) = \frac{1}{(1 - c^i)(1 - c^j)(1 - c^k)} \begin{vmatrix} c^i & c^j & c^k \\ \left(\frac{c}{d}\right)^i & \left(\frac{c}{d}\right)^j & \left(\frac{c}{d}\right)^k \\ 1^i & 1^j & 1^k \end{vmatrix}.$$

By the property of the generalized Vandermonde determinant inequality, the above expression is non-positive. It completes the proof of inequality (10).

References

1. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Proc. of IEEE Int. Conf. on Computers, Systems, and Signal Processing* [175–179] (IEEE, New York, 1984).
2. Lo, H. K. & Chau, H. F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **283,** 2050–2056 (1999).
3. Shor, P. W. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85,** 441–444 (2000).
4. Mayers D. Unconditional security in quantum cryptography. *J. ACM* **48,** 351–406 (2001).
5. Brassard, G., Lütkenhaus, N., Mor, T. & Sanders, B. C. Limitations on practical quantum cryptography. *Phys. Rev. Lett.* **85,** 1330–1333 (2000).
6. Lütkenhaus, N. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A* **61,** 052304 (2000).
7. Lütkenhaus, N. & Jahma, M. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. *New J. Phys.* **4,** 44.1–44.9 (2002).
8. Hwang, W. Y. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.* **91,** 057901 (2003).
9. Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94,** 230503 (2005).
10. Lo, H.-K., Ma, X. F. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94,** 230504 (2005).
11. 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).
12. Wang, Q. & Karlsson, A. Performance enhancement of a decoy-state quantum key distribution using a conditionally prepared down-conversion source in the Poisson distribution. *Phys. Rev. A* **76,** 014309 (2007).
13. Wang, Q., Wang, X.-B., Bjork, G. & Karlsson, A. Improved practical decoy state method in quantum key distribution with parametric down-conversion source. *Europhysics Letters* **79,** 4 (2007).
14. Wang, Q. *et al.* Experimental decoy-state quantum key distribution with a sub-Poissionian heralded single-photon source. *Phys. Rev. Lett.* **100,** 090501 (2008).
15. Braunstein, S. L. & Pirandola, S. Side-Channel-Free Quantum Key Distribution. *Phys. Rev. Lett.* **108,** 130502 (2012).
16. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108,** 130503 (2012).
17. Wang, X.-B. Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors. *Phys. Rev. A* **87,** 012320 (2013).
18. Wang, Q. & Wang, X.-B. Efficient implementation of the decoy-state measurement-device-independent quantum key distribution with heralded single-photon sources. *Phys. Rev. A* **88,** 052332 (2013).
19. Wang, Q. & Wang, X.-B. Simulating of the measurement-device-independent quantum key distribution with phase randomized general sources. *Sci. Rep.* **4,** 04612 (2014).
20. Wang, D. *et al.* Quantum key distribution with the single-photon-added coherent source. *Phys. Rev. A* **90,** 062315 (2014).
21. Wang, D., Li, M., Guo, G.-C. & Wang, Q. An improved scheme on decoy-state method for measurementdevice-independent quantum key distribution. *Sci. Rep.* **5,** 15130 (2015).
22. Zhu, F. & Wang, Q. The quantum key distribution based on heralded single photon source. *Acta Optica Sinica* **34,** 0627002 (2014).
23. Ma, X., Fung, C.-H. F. & Razavi, M. Statistical fluctuation analysis for measurement-device-independent quantum key distribution. *Phys. Rev. A* **86,** 052305 (2012).
24. Yu, Z.-W., Zhou, Y.-H. & Wang, X.-B. Three-intensity decoy-state method for measurement-device-independent quantum key distribution. *Phys. Rev. A* **88,** 062339 (2013).
25. 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).
26. Tang, Y.-L. *et al.* Measurement-Device-Independent Quantum Key Distribution over Untrustful Metropolitan Network. *Phys. Rev. X* **6,** 011024 (2016).
27. Pirandola, S. *et al.* High-rate measurement-device-independent quantum cryptography. *Nature Photonics* **9,** 397 (2015).

28. Shan, Y.-Z. *et al.* Measurement-device-independent quantum key distribution with a passive decoy-state method. *Phys. Rev. A* **90,** 042334 (2014).
29. Zhou, Y.-H., Yu, Z.-W. & Wang, X.-B. Making the decoy-state measurement-device-independent quantum key distribution practically useful. *Phys. Rev. A* **93,** 042324 (2016).

Acknowledgements

Q.W. thanks Prof. G.B. for enlighten discussion, and thank Prof. S.L.L. for help in mathematical analysis. We also acknowledge the financial support from the National Natural Science Foundation of China through Grants No. 11274178, No. 61475197 and No. 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.

Author Contributions

Q.W. proposed the idea, wrote the source code, analyzed the numerical results and did changes on the manuscript, X.-Y.Z. did numerical simulation and wrote the manuscript, G.-C.G. commented and made changes to the manuscript.

Additional Information

Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Wang, Q. *et al.* Realizing the measure-device-independent quantum-key-distribution with passive heralded-single photon sources. *Sci. Rep.* **6**, 35394; doi: 10.1038/srep35394 (2016).