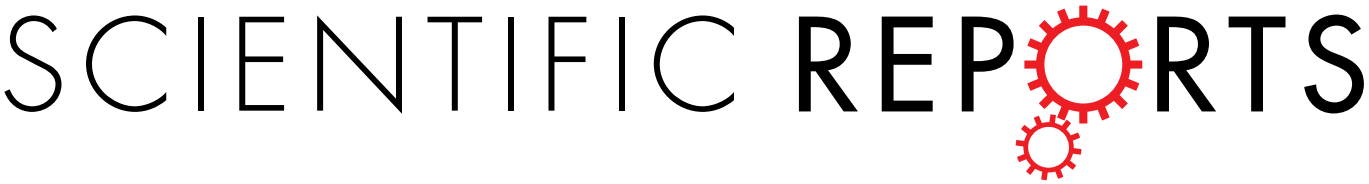

OPEN

Practical passive decoy state measurement-device-independent quantum key distribution with unstable sources

Received: 13 April 2017
Accepted: 24 July 2017
Published online: 12 September 2017

Li Liu[1,2], Fen-Zhuo Guo[1,2] & Qiao-Yan Wen[1]

Measurement-device-independent quantum key distribution (MDI-QKD) with the active decoy state method can remove all detector loopholes, and resist the imperfections of sources. But it may lead to side channel attacks and break the security of QKD system. In this paper, we apply the passive decoy state method to the MDI-QKD based on polarization encoding mode. Not only all attacks on detectors can be removed, but also the side channel attacks on sources can be overcome. We get that the MDI-QKD with our passive decoy state method can have a performance comparable to the protocol with the active decoy state method. To fit for the demand of practical application, we discuss intensity fluctuation in the security analysis of MDI-QKD protocol using passive decoy state method, and derive the key generation rate for our protocol with intensity fluctuation. It shows that intensity fluctuation has an adverse effect on the key generation rate which is non-negligible, especially in the case of small data size of total transmitting signals and long distance transmission. We give specific simulations on the relationship between intensity fluctuation and the key generation rate. Furthermore, the statistical fluctuation due to the finite length of data is also taken into account.

Quantum key distribution (QKD) has been widely studied in both theoretical and experimental aspects[1–3] since its initial proposal[4]. QKD enables two distant parties (Alice and Bob) to share a key, which is secret from any eavesdropper (Eve). It has been proved to be unconditional secure theoretically[5].

Due to the imperfections of devices, there is still a big gap between the theory and practice of QKD. Fortunately, Lo *et al*. proposed a measurement-device-independent quantum key distribution (MDI-QKD) protocol[6] to exclude all the attacks on detectors, which has been experimentally demonstrated by several groups[7–9]. Recently, the decoy state method has been widely used in MDI-QKD[9–17] to defeat the photon number splitting (PNS) attack[18,19] and guarantee the security against imperfect sources, such as weak coherent pulses sources (WCPS)[20,21]. These approaches are all related to the active decoy state selection, which is based on the assumption that Eve can not distinguish decoy and signal states. But this assumption may not stand in real active decoy state experiments, for which it may open up to side channels attacks and even break the security of the system when one actively modulates the intensities of pulses[22,23]. The passive decoy state method[24–28] can reduce the side channel information in the decoy state preparation procedure. Different from the active decoy state method, the passive one only uses one intensity signal, and Alice passively chooses the signal state and the decoy state according to the response of Alice's detector. The method in ref. 28 extended passive decoy state to practical unstable light sources, which promoted its application to practical QKD. Therefore, it is necessary to consider the MDI-QKD with a passive decoy state. This has been demonstrated with phase encoding mode in ref. 29. Due to the different advantages between phase encoding and polarization encoding in practical application, we will apply the passive decoy state in MDI-QKD with polarization encoding mode[8,9,30,31].

An important imperfect factor of photon sources is intensity fluctuation[32]. Due to unavoidable interference from environments, there should be deviation between the true value and the assumed value. The deviation rises and falls irregularly, which can be called intensity fluctuation. The intensity fluctuation in experiments will result in the irregular change of the photon number distribution, and bring a potential security loopholes to the

[1]State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China. [2]School of Science, Beijing University of Posts and Telecommunications, Beijing, 100876, China. Correspondence and requests for materials should be addressed to F.-Z.G. (email: gfenzhuo@bupt.edu.cn)

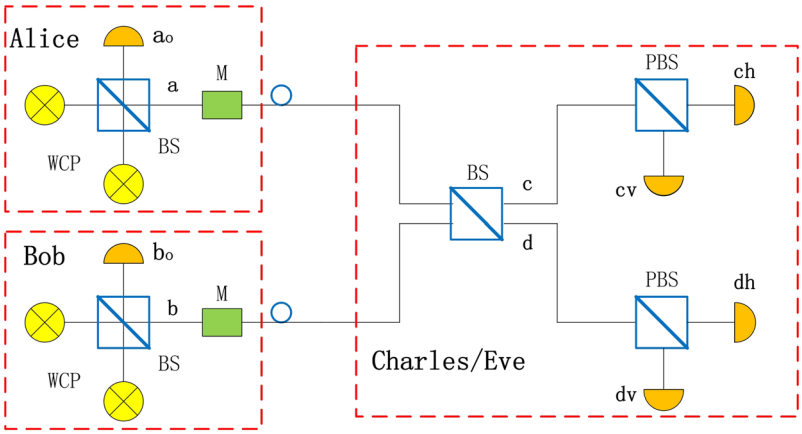

Figure 1. Passive decoy state MDI-QKD system model. WCP, weak coherent pulse; M, polarization modulators; BS, beam splitter; PBS, polarization BS; a_0, b_0, c_h, c_v, d_h and d_v, photon detector.

practical QKD[33]. The WCPs used in the passive decoy state method also has the imperfection of intensity fluctuation[34]. Therefore, how intensity fluctuations influence the performance of passive decoy state MDI-QKD protocol should also not be ignored.

In this paper, we apply the passive decoy state method to the MDI-QKD protocol with polarization encoding mode. Alice and Bob use WCPs with random phases to passively generate signal states or decoy states. Not only all the attacks on detectors can be removed, but also the side channels attacks on sources can be avoided, which may be generated by active modulation of source intensities. We analyse the security of this protocol, and show that MDI-QKD protocol with our passive decoy state method can provide a performance comparable to the active decoy state method. In order to fit for the demand of practical application, we discuss intensity fluctuation for MDI-QKD using the passive decoy state method. And based on the the formulas of yield and error rate derived in our paper, we get the key generation rate for our protocol with intensity fluctuation. According to the total gain and the overall error rate derived in our paper, we give a numerical simulations for our result. It shows that intensity fluctuation has a non-negligible effect on the key rate of the passive decoy state MDI-QKD protocol, especially in the case of small data size of total transmitting signals and long distance transmission. We give specific simulations on the relationship between intensity fluctuation and the key generation rate. Moreover, the finite-size analysis of this protocol is also taken into account in our paper.

Results

Passive Decoy State MDI-QKD Model. In this section, we apply the passive decoy state method to the MDI-QKD protocol, as shown in Fig. 1. The general process of this protocol is described as follows.

Alice generates phase-randomized pulses using two weak coherent sources with intensities μ_1 and μ_2, respectively. These two pulses interfere at a beam splitter (BS) with a transmittance of 50%; then there are two outcome signals which have the classically correlated photon number statistics. Alice passively generates signal or decoy states. The state Alice generated is a joint-distribution state according to the result of detector a_0. The detector a_0 with two modes c_0 and c_1. The letter c_0 indicates that the detector has no click and c_1 indicates the detector has a click. Thus corresponding to the detector's modes, the output a has two modes, c_0 and c_1, which describe the signal state and decoy state, respectively. The total probability of having n photons in the output light can be written as

$$p_{n,a}^{t} = \frac{\mu^n}{n!}\frac{1}{2\pi}\int_0^{2\pi} \alpha^n e^{-\mu\alpha} d\theta_a, \tag{1}$$

which is proven to be a non-Poissonian probability distribution[33], and the parameters $\mu = \mu_1 + \mu_2, \alpha = \frac{\frac{\mu}{2} + \xi_a \cos\theta_a}{\mu}$, $\xi_a = \sqrt{\mu_1\mu_2}$ and $\theta_a = \phi_{a_2} - \phi_{a_1}$ is the phase difference. The joint probability of having n photons in mode a and no click in the detector a_0 can be expressed by

$$p_{n,a}^{c_0} = (1-\varepsilon)\frac{\mu^n}{n!}e^{-\eta_d\mu}\frac{1}{2\pi}\int_0^{2\pi} \alpha^n e^{-(1-\eta_d)\mu\alpha} d\theta_a, \tag{2}$$

ϵ is the dark count rate of detector, and η_d is the detector efficiency. The joint probability of having n photons in mode a and producing a click in the detector a_0 has now the form

$$p_{n,a}^{c_1} = p_{n,a}^{t} - p_{n,a}^{c_0}. \tag{3}$$

Considering the normalization, the distributions of signal states and decoy states are respectively given by

$$q_{n,a}^{c_0} = p_{n,a}^{c_0}/(N_a), \quad q_{n,a}^{c_1} = p_{n,a}^{c_1}/(1 - N_a), \tag{4}$$

where

$$N_a = (1 - \epsilon)e^{-\eta_d \mu} \frac{1}{2\pi} \int_0^{2\pi} e^{\eta_d \mu \alpha} d\theta_a, \tag{5}$$

is a normalization constant.

Bob performs the same process as Alice. He generates phase-randomized pulses using two weak coherent sources with intensities υ_1 and υ_2, respectively. The distributions expressions of signal state $p_{m,b}^{c_0}$ and decoy state $p_{m,b}^{c_1}$ are just like those in Eq. (3). It can be given by

$$\begin{aligned} p_{m,b}^{t} &= \frac{\upsilon^n}{n!} \frac{1}{2\pi} \int_0^{2\pi} \beta^n e^{-\upsilon\beta} d\theta_b, \\ p_{m,b}^{c_0} &= (1 - \epsilon) \frac{\upsilon^n}{n!} e^{-\eta_d \upsilon} \frac{1}{2\pi} \int_0^{2\pi} \beta^n e^{-(1-\eta_d)\upsilon\beta} d\theta_b, \\ p_{m,b}^{c_1} &= p_{m,b}^{t} - p_{m,b}^{c_0}, \end{aligned} \tag{6}$$

where the parameters are corresponding to Alice's.

The main step of MDI-QKD based on BB84 protocol and here we adopt the polarization encoding method[6]. Each of Alice and Bob prepares phase-randomized WCP in a different BB84 polarization state which is selected by means of a polarization modulator (M), independently and at random for each signal. Then they send them to an untrusted relay Charles (or Eve), who is supposed to perform a Bell-state measurement(BSM). Inside the measurement device, signals from Alice and Bob interfere at a 50:50 beam splitter (BS) that has a polarizing beam splitter (PBS) on each end. The PBS projecting the input photons into either horizontal (H) or vertical (V) polarization states. A successful Bell state measurement corresponds to the observation of precisely two detectors (associated to orthogonal polarizations) being triggered. Charles announces the results through a public channel to Alice and Bob. According to the result that Charles announces, Alice and Bob proceed on to basis reconciliation, error correction, and privacy amplification, as in traditional QKD protocols[35]. Then both Alice and Bob can ensure they have the same bits.

Estimation of the key generation rate. We modify the Gottesman-Lo-Lutkenhaus-Preskill (GLLP) formula[36] according to the MDI-QKD security analysis. Then, we get the key generation rate formula,

$$R \geqslant P_{11}^Z Y_{11}^Z \left[1 - H(e_{11}^X)\right] - Q_{c_0c_0}^Z f_e (E_{c_0c_0}^Z) H(E_{c_0c_0}^Z), \tag{7}$$

where Y_{11}^Z and e_{11}^X are, respectively, the yield (the conditional probability that Charles declares a successful event) in the rectilinear (Z) basis and the error rate in the diagonal (X) basis, given that both Alice and Bob send single photon states; P_{11}^Z denotes the probability distribution that both Alice and Bob send single photon states in the Z basis; $f_e \geq 1$ is the efficiency of the error correction protocol; $H(x) = -x\,log_2(x) - (1-x)\,log_2(1-x))$ is the binary Shannon entropy function; $Q_{c_0c_0}^Z$ and $E_{c_0c_0}^Z$ denote, respectively, the total gain and quantum bit error rate (QBER) of signal state in the Z basis. Here we use the Z basis for key generation and the X basis for testing only.

In a MDI-QKD implementation with the model described in our paper, we can obtain the total gains and error rates in both the X basis and the Z basis,

$$Q_{c_ic_j}^{\lambda} = \sum_{n,m=0}^{\infty} q_{n,a}^{c_i} q_{m,b}^{c_j} Y_{nm}^{\lambda}, \quad Q_{c_ic_j}^{\lambda} E_{c_ic_j}^{\lambda} = \sum_{n,m=0}^{\infty} q_{n,a}^{c_i} q_{m,b}^{c_j} Y_{nm}^{\lambda} e_{nm}^{\lambda}, \tag{8}$$

where $\lambda \in \{X, Z\}$ denotes the basis choice and $i, j = 0$ or 1. Y_{nm}^{λ} and e_{nm}^{λ} are, respectively, the yield and error rate that Alice sends n photons pulse and Bob sends m photons pulse in the λ basis.

In practice, $Q_{c_0c_0}^Z$ and $E_{c_0c_0}^Z$ can be directly measured in experiments, while Alice and Bob only need to estimate the lower bound of the yield Y_{11}^Z and the upper bound of the error rate e_{11}^X using the decoy state methods. According to ref. 29, the lower bound of Y_{11}^{λ} can be given

$$\begin{aligned} Y_{11}^{\lambda} \geqslant \underline{Y_{11}^{\lambda}} &= (c_{c_1c_1} Q_{c_1c_1}^{\lambda} + c_{c_1c_0} Q_{c_1c_0}^{\lambda} + c_{c_0c_1} Q_{c_0c_1}^{\lambda} + c_{c_0c_0} Q_{c_0c_0}^{\lambda} - c_{c_10} Q_{c_10}^{\lambda} \\ &\quad - c_{c_00} Q_{c_00}^{\lambda} - c_{0c_1} Q_{0c_1}^{\lambda} - c_{0c_0} Q_{0c_0}^{\lambda} + c_{00} Q_{00}^{\lambda}) \\ &\quad \times \left[(K - A_1 B_1)\,(q_{0,a}^{c_0} q_{1,a}^{c_0} + q_{0,a}^{c_1} q_{1,a}^{c_1})\,(q_{0,b}^{c_0} q_{1,b}^{c_0} + q_{0,b}^{c_1} q_{1,b}^{c_1})\right]^{-1}, \end{aligned} \tag{9}$$

where $\lambda = X$ or Z and the coefficients of the total gain in each mode are

$$
\begin{aligned}
c_{c_1c_1} &= Kq_{0,a}^{c_1}q_{0,b}^{c_1} - q_{0,a}^{c_0}q_{0,b}^{c_0}, & c_{c_1c_0} &= Kq_{0,a}^{c_1}q_{0,b}^{c_0} + q_{0,a}^{c_0}q_{0,b}^{c_1},\\
c_{c_0c_1} &= Kq_{0,a}^{c_0}q_{0,b}^{c_1} + q_{0,a}^{c_1}q_{0,b}^{c_0}, & c_{c_0c_0} &= Kq_{0,a}^{c_0}q_{0,b}^{c_0} - q_{0,a}^{c_1}q_{0,b}^{c_1},\\
c_{c_10} &= Kq_{0,a}^{c_1}\left[(q_{0,b}^{c_1})^2 + (q_{0,b}^{c_0})^2\right], & c_{c_00} &= Kq_{0,a}^{c_0}\left[(q_{0,b}^{c_1})^2 + (q_{0,b}^{c_0})^2\right],\\
c_{0c_1} &= Kq_{0,b}^{c_1}\left[(q_{0,a}^{c_1})^2 + (q_{0,a}^{c_0})^2\right], & c_{0c_0} &= Kq_{0,b}^{c_0}\left[(q_{0,a}^{c_1})^2 + (q_{0,a}^{c_0})^2\right],\\
c_{00} &= K\left[(q_{0,a}^{c_1})^2 + (q_{0,a}^{c_0})^2\right]\left[(q_{0,b}^{c_1})^2 + (q_{0,b}^{c_0})^2\right],\\
K &= min\{A_1B_2, A_2B_1, A_2B_2\}
\end{aligned}
\tag{10}
$$

and

$$
\begin{aligned}
A_1 &= \frac{q_{0,a}^{c_1}q_{1,a}^{c_0} - q_{0,a}^{c_0}q_{1,a}^{c_1}}{q_{0,a}^{c_0}q_{1,a}^{c_0} + q_{0,a}^{c_1}q_{1,a}^{c_1}}, A_2 = \frac{q_{0,a}^{c_1}q_{2,a}^{c_0} - q_{0,a}^{c_0}q_{2,a}^{c_1}}{q_{0,a}^{c_0}q_{2,a}^{c_0} + q_{0,a}^{c_1}q_{2,a}^{c_1}},\\
B_1 &= \frac{q_{0,b}^{c_1}q_{1,b}^{c_0} - q_{0,b}^{c_0}q_{1,b}^{c_1}}{q_{0,b}^{c_0}q_{1,b}^{c_0} + q_{0,b}^{c_1}q_{1,b}^{c_1}}, B_2 = \frac{q_{0,b}^{c_1}q_{2,b}^{c_0} - q_{0,b}^{c_0}q_{2,b}^{c_1}}{q_{0,b}^{c_0}q_{2,b}^{c_0} + q_{0,b}^{c_1}q_{2,b}^{c_1}}.
\end{aligned}
\tag{11}
$$

The upper bound of e_{11}^{λ} can be obtained with

$$
e_{11}^{\lambda} \leqslant \overline{e_{11}^{\lambda}} = (Q_{c_1c_1}^{\lambda}E_{c_1c_1}^{\lambda} - q_{0,a}^{c_1}Q_{0c_1}^{\lambda}E_{0c_1}^{\lambda} - q_{0,b}^{c_1}Q_{c_10}^{\lambda}E_{c_10}^{\lambda} - q_{0,a}^{c_1}q_{0,b}^{c_1}Q_{00}^{\lambda}E_{00}^{\lambda})/(q_{1,a}^{c_1}q_{1,b}^{c_1}\underline{Y_1^{\lambda}}).
\tag{12}
$$

The subscripts c_0 and c_1 denote Alice or Bob prepare a signal state and a decoy state, respectively. If a subscript 0 appears, then Alice or Bob prepares a vacuum state.

To analyse the security and performance of our passive decoy state MDI-QKD, we still need to know the total gains and the overall error rates in both the X basis and the Z basis. Supplementary Material shows the calculating process that how to get the total gain and overall error rate theoretically.

Passive Decoy State MDI-QKD With Intensity Fluctuation. We discuss an unavoidable imperfect factor, intensity fluctuation, in practice QKD protocol. We introduce parameter δ to denote the degree of intensity fluctuation. Here we take Alice as an example to describe the general process. The fluctuation ranges of the two intensities of Alice's WCP sources are characterized by

$$
\mu_1(1 - \delta_{\mu_1}) \leqslant \mu_1^{real} \leqslant \mu_1(1 + \delta_{\mu_1}), \quad \mu_1(1 - \delta_{\mu_2}) \leqslant \mu_1^{real} \leqslant \mu_1(1 + \delta_{\mu_2}),
\tag{13}
$$

where δ_{μ_1} and δ_{μ_2} are the variation ranges of μ_1 and μ_2, respectively. μ_1^{real} and μ_2^{real} are the real intensities of Alice's WCP sources. We assume that the range of the intensity fluctuation parameters δ_{μ_1} and δ_{μ_2} is $[0,\ 0.1]$[34].

Similarly, we can get

$$
q_{n,a}^{t,L} \leqslant q_{n,a}^{t,real} \leqslant q_{n,a}^{t,U}, \quad q_{n,a}^{c_0,L} \leqslant q_{n,a}^{c_0,real} \leqslant q_{n,a}^{c_0,U}, \quad q_{n,a}^{c_1,L} \leqslant q_{n,a}^{c_1,real} \leqslant q_{n,a}^{c_1,U},
\tag{14}
$$

where $q_{n,a}^{t,real}$ is the real total probability of having n photons in Alice's output light, $q_{n,a}^{c_0,real}$ and $q_{n,a}^{c_1,real}$ are the joint probability of having n photons in mode a and no click or a click in the detector a_0, respectively. The capital letter L and U represent the lower and the upper bounds.

Due to the intensity fluctuation, we can derive the following expressions:

$$
\begin{aligned}
&q_{0,a}^{t,L} = I_{0,\xi_a^U}e^{-\omega_a^U},\ q_{1,a}^{t,L} = (\omega_a^L I_{0,\xi_a^L} - \xi_a^L I_{1,\xi_a^L})e^{-\omega_a^L},\\
&q_{1,a}^{t,U} = (\omega_a^U I_{0,\xi_a^U} - \xi_a^U I_{1,\xi_a^U})e^{-\omega_a^U},\ q_{0,a}^{t,U} = I_{0,\xi_a^L}e^{-\omega_a^L},\\
&q_{0,a}^{c_0,L} = \tau_a^U I_{0,(1-\eta_d)\xi_a^U},\ q_{0,a}^{c_0,U} = \tau_a^L I_{0,(1-\eta_d)\xi_a^L},\\
&q_{1,a}^{c_0,L} = \tau_a^L(\omega_a^L I_{0,(1-\eta_d)\xi_a^L} - \xi_a^L I_{1,(1-\eta_d)\xi_a^L}),\\
&q_{1,a}^{c_0,U} = \tau_a^U(\omega_a^U I_{0,(1-\eta_d)\xi_a^U} - \xi_a^U I_{1,(1-\eta_d)\xi_a^U}).
\end{aligned}
\tag{15}
$$

Then, we have

$$
\begin{aligned}
q_{0,a}^{c_1,L} &= q_{0,a}^{t,L} - q_{0,a}^{c_0,L}, \quad q_{0,a}^{c_1,U}\\
&= q_{0,a}^{t,U} - q_{0,a}^{c_0,U}, \quad q_{1,a}^{c_1,L}\\
&= q_{1,a}^{t,L} - q_{1,a}^{c_0,L}, \quad q_{1,a}^{c_1,U}\\
&= q_{1,a}^{t,U} - q_{1,a}^{c_0,U},
\end{aligned}
\tag{16}
$$

where

$$\begin{aligned}
\omega_a^L &= \frac{1}{2}\left[\mu_1(1-\delta_{\mu_1})+\mu_2(1-\delta_{\mu_2})\right], & \omega_a^U &= \frac{1}{2}\left[\mu_1(1+\delta_{\mu_1})+\mu_2(1+\delta_{\mu_2})\right],\\
\xi_a^L &= \sqrt{\mu_1(1-\delta_{\mu_1})\mu_2(1-\delta_{\mu_2})}, & \xi_a^U &= \sqrt{\mu_1(1+\delta_{\mu_1})\mu_2(1+\delta_{\mu_2})},\\
\tau_a^L &= (1-\epsilon)e^{-\left[\eta_d\mu^L+(1-\eta_d)\omega_a^L\right]}, & \tau_a^U &= (1-\epsilon)e^{-\left[\eta_d\mu^U+(1-\eta_d)\omega_a^U\right]},\\
\mu^L &= \mu_1(1-\delta_{\mu_1})+\mu_2(1-\delta_{\mu_2}), & \mu^U &= \mu_1(1+\delta_{\mu_1})+\mu_2(1+\delta_{\mu_2}).
\end{aligned} \tag{17}$$

Bob has the same process as Alice. Next, we will calculate the lower bound of $Q_{11}^{c_0c_0}$ and $Q_{11}^{c_1c_1}$, i.e., $Q_{11}^{c_0c_0,L}$ and $Q_{11}^{c_1c_1,L}$, the upper bound of e_{11}, i.e., e_{11}^U, when we consider the intensity fluctuation.

The overall gain of Alice's and Bob's detector both producing a click is $Q_{c_1c_1}$ and no click is $Q_{c_0c_0}$. They can be expressed as

$$\begin{aligned}
Q_{c_0c_0} = \sum_{n=0}^{\infty}\sum_{m=0}^{\infty} Q_{nm}^{c_0c_0} &= Q_{00}^{c_0c_0}+Q_{11}^{c_0c_0}+\sum_{m=1}^{\infty}Q_{0m}^{c_0c_0}+\sum_{n=1}^{\infty}Q_{n0}^{c_0c_0}\\
&\quad+\sum_{m=2}^{\infty}Q_{1m}^{c_0c_0}+\sum_{n=2}^{\infty}Q_{n1}^{c_0c_0}+\sum_{n=2}^{\infty}\sum_{m=2}^{\infty}Q_{nm}^{c_0c_0},\\
Q_{c_1c_1} = \sum_{n=0}^{\infty}\sum_{m=0}^{\infty} Q_{nm}^{c_1c_1} &= Q_{00}^{c_1c_1}+Q_{11}^{c_1c_1}+\sum_{m=1}^{\infty}Q_{0m}^{c_1c_1}+\sum_{n=1}^{\infty}Q_{n0}^{c_1c_1}\\
&\quad+\sum_{m=2}^{\infty}Q_{1m}^{c_1c_1}+\sum_{n=2}^{\infty}Q_{n1}^{c_1c_1}+\sum_{n=2}^{\infty}\sum_{m=2}^{\infty}Q_{nm}^{c_1c_1},
\end{aligned} \tag{18}$$

where the parameters are in the condition of using μ_1^{real}, μ_2^{real}, υ_1^{real} and υ_1^{real}.

Then, applying $Q_{c_1c_1}-Q_{c_0c_0}$, we can get

$$\begin{aligned}
Q_{11}^{c_0c_0}-Q_{11}^{c_1c_1} &= Q_{c_0c_0}-Q_{c_1c_1}+Q_{00}^{c_1c_1}-Q_{00}^{c_0c_0}+\sum_{m=1}^{\infty}Q_{0m}^{c_1c_1}\\
&\quad-\sum_{m=1}^{\infty}Q_{0m}^{c_0c_0}+\sum_{n=1}^{\infty}Q_{n0}^{c_1c_1}-\sum_{n=1}^{\infty}Q_{n0}^{c_0c_0}\\
&\quad+\sum_{m=2}^{\infty}Q_{1m}^{c_1c_1}-\sum_{m=2}^{\infty}Q_{1m}^{c_0c_0}+\sum_{n=2}^{\infty}Q_{n1}^{c_1c_1}\\
&\quad-\sum_{n=2}^{\infty}Q_{n1}^{c_0c_0}+\sum_{n=2}^{\infty}\sum_{m=2}^{\infty}Q_{nm}^{c_1c_1}-\sum_{n=2}^{\infty}\sum_{m=2}^{\infty}Q_{nm}^{c_0c_0}.
\end{aligned} \tag{19}$$

The common point between the passive decoy state and the active decoy state is that the counting rates and the error rates of pulse of the same photon number states from the signal states and the decoy states shall be equal to each other[37]. Thus, in our study, we assume they are still equal to each other in the case of intensity fluctuation. Then, we use the following inequalities to substitute the elements in Eq. (19):

$$Q_{00}^{c_0c_0}\leqslant\frac{q_{0,a}^{c_0,U}q_{0,b}^{c_0,U}Q_{00}^{c_1c_1}}{q_{0,a}^{c_1,L}q_{0,b}^{c_0,L}},\quad Q_{nm}^{c_0c_0}\leqslant\frac{q_{n,a}^{c_0,U}q_{m,b}^{c_0,U}Q_{nm}^{c_1c_1}}{q_{n,a}^{c_1,L}q_{m,b}^{c_1,L}},\quad 0\leq Q_{00}^{c_1c_1}\leqslant\frac{E_{c_1c_1}Q_{c_1c_1}}{e_{00}}. \tag{20}$$

And note that $n\geqslant 1$, we have $q_{n,a}^{c_1,L}/q_{n,a}^{c_0,U}\leqslant q_{1,a}^{c_1,L}/q_{1,a}^{c_0,U}$ and $q_{m,b}^{c_1,U}/q_{m,b}^{c_0,L}\leqslant q_{1,b}^{c_1,U}/q_{1,b}^{c_0,L}$. By using this inequalities, the elements in Eq. (19) can be substituted as:

$$\begin{aligned}
&Q_{11}^{c_0c_0}-Q_{11}^{c_1c_1}\leqslant Q_{11}^{c_1c_1}\left(\frac{q_{1,a}^{c_0,U}q_{1,b}^{c_0,U}}{q_{1,a}^{c_1,L}q_{1,b}^{c_1,L}}-1\right),\\
&Q_{00}^{c_1c_1}-Q_{00}^{c_0c_0}\geqslant-\frac{E_{c_1c_1}Q_{c_1c_1}}{e_{00}}\left(\frac{q_{0,a}^{c_0,U}q_{0,b}^{c_0,U}}{q_{0,a}^{c_1,L}q_{0,b}^{c_1,L}}-1\right),\\
&\sum_{m=1}^{\infty}Q_{0m}^{c_1c_1}-\sum_{m=1}^{\infty}Q_{0m}^{c_0c_0}\geqslant\sum_{m=1}^{\infty}-Q_{0m}^{c_1c_1}\left(\frac{q_{0,a}^{c_0,U}q_{1,b}^{c_0,U}}{q_{0,a}^{c_1,L}q_{1,b}^{c_1,L}}-1\right),\\
&\sum_{n=1}^{\infty}Q_{n0}^{c_1c_1}-\sum_{n=1}^{\infty}Q_{n0}^{c_0c_0}\geqslant\sum_{n=1}^{\infty}-Q_{n0}^{c_1c_1}\left(\frac{q_{1,a}^{c_0,U}q_{0,b}^{c_0,U}}{q_{1,a}^{c_1,L}q_{0,b}^{c_1,L}}-1\right),\\
&\sum_{m=2}^{\infty}Q_{1m}^{c_1c_0}-\sum_{m=2}^{\infty}Q_{1m}^{c_0c_0}\geqslant\sum_{m=2}^{\infty}-Q_{1m}^{c_1c_1}\left(\frac{q_{1,a}^{c_0,U}q_{1,b}^{c_0,U}}{q_{1,a}^{c_1,L}q_{1,b}^{c_1,L}}-1\right),\\
&\sum_{n=2}^{\infty}Q_{n1}^{c_1c_1}-\sum_{n=2}^{\infty}Q_{n1}^{c_0c_0}\geqslant\sum_{n=2}^{\infty}-Q_{n1}^{c_1c_1}\left(\frac{q_{1,a}^{c_0,U}q_{1,b}^{c_0,U}}{q_{1,a}^{c_1,L}q_{1,b}^{c_1,L}}-1\right),\\
&\sum_{n=2}^{\infty}\sum_{m=2}^{\infty}Q_{nm}^{c_1c_1}-\sum_{n=2}^{\infty}\sum_{m=2}^{\infty}Q_{nm}^{c_0c_0}\geqslant\sum_{n=2}^{\infty}\sum_{m=2}^{\infty}-Q_{nm}^{c_1c_1}\left(\frac{q_{1,a}^{c_0,U}q_{1,b}^{c_0,U}}{q_{1,a}^{c_1,L}q_{1,b}^{c_1,L}}-1\right).
\end{aligned} \tag{21}$$

Finally, we obtain the lower bound of $Q_{11}^{c_1c_1}$,

$$Q_{11}^{c_1c_1} \geq Q_{11}^{c_1c_1,L} = \frac{Q_{c_0c_0} - Q_{c_1c_1} - \left(\frac{q_{0,a}^{c_0,U} q_{0,b}^{c_0,U}}{q_{0,a}^{c_1,L} q_{0,b}^{c_1,L}} - 1\right)\frac{E_{c_1c_1}Q_{c_1c_1}}{e_{00}}}{\frac{q_{1,a}^{c_0,U} q_{1,b}^{c_0,U}}{q_{1,a}^{c_1,L} q_{1,b}^{c_1,L}} - 1}. \tag{22}$$

We can get

$$\frac{Q_{11}^{c_1c_1}}{q_{1,a}^{c_1} q_{1,b}^{c_1}} = Y_{11}^{c_0c_0} = Y_{11}^{c_0c_0} = \frac{Q_{11}^{c_0c_0}}{q_{1,a}^{c_0} q_{1,b}^{c_0}}, \quad Q_{11}^{c_0c_0,L} = \frac{Q_{11}^{c_1c_1,L} q_{1,a}^{c_0,L} q_{1,b}^{c_0,L}}{q_{1,a}^{c_0,U} q_{1,b}^{c_1,U}}. \tag{23}$$

Then, we will calculate the upper bound of e_{11}. The overall quantum bit error rate (QBER) is

$$\begin{aligned} E_{c_1c_1}Q_{c_1c_1} &= q_{0,a}^{c_1} q_{0,b}^{c_1} e_{00} Y_{00} + q_{1,a}^{c_1} q_{1,b}^{c_1} e_{11} Y_{11} + q_{0,a}^{c_1} \sum_{m=1}^{\infty} q_{m,b}^{c_1} e_{0m} Y_{0m} + q_{0,b}^{c_1} \sum_{n=1}^{\infty} q_{n,a}^{c_1} e_{n0} Y_{n0} \\ &\quad + q_{1,a}^{c_1} \sum_{m=2}^{\infty} q_{m,b}^{c_1} e_{1m} Y_{1m} + q_{1,b}^{c_1} \sum_{n=2}^{\infty} q_{n,a}^{c_1} e_{n1} Y_{n1} + \sum_{n,m=2}^{\infty} q_{n,a}^{c_1} q_{n,b}^{c_1} e_{nm} Y_{nm} \\ &\geq q_{0,a}^{c_1} Q_{0c_1} E_{0c_1} + q_{0,a}^{c_1} q_{0,b}^{c_1} e_{11} Y_{11} + q_{0,b}^{c_1} Q_{c_10} E_{c_10} + q_{0,a}^{c_1} q_{0,b}^{c_1} Q_{00} E_{00}. \end{aligned} \tag{24}$$

we can obtain the upper bound of e_{11}

$$e_{11} \leq e_{11}^U = \frac{1}{Q_{11}^{c_1c_1,L}} (Q_{c_1c_1}E_{c_1c_1} - q_{0,a}^{c_1} Q_{0c_1} E_{0c_1} - q_{0,b}^{c_1} Q_{c_10} E_{c_10} - q_{0,a}^{c_1} q_{0,b}^{c_1} Q_{00} E_{00}). \tag{25}$$

The key generation rate with intensity fluctuation is

$$R \geq (Q_{11}^{c_1c_1,L} + Q_{11}^{c_0c_0,L}) \left[1 - H(e_{11}^U)\right] - Q_{c_0c_0} f_e \left(E_{c_0c_0}\right) H\left(E_{c_0c_0}\right). \tag{26}$$

Statistical Fluctuation. In practical, the number of key distribution is finite, which will bring some statistical fluctuation into the parameter estimation. In this section, we will discuss the effect of the finite size on the security of MDI-QKD with our passive decoy state method based on the standard statistical analysis[38,39].

When consider the statistical fluctuation, the total gain $Q_{c_ic_j}^{\lambda}$ and the overall error rate $E_{c_ic_j}^{\lambda}$ are turned from determined values into intervals, which can be written as

$$\underline{Q_{c_ic_j}^{\lambda}} \leq Q_{c_ic_j}^{\lambda} \leq \overline{Q_{c_ic_j}^{\lambda}}, \quad \underline{Q_{c_ic_j}^{\lambda} E_{c_ic_j}^{\lambda}} \leq Q_{c_ic_j}^{\lambda} E_{c_ic_j}^{\lambda} \leq \overline{Q_{c_ic_j}^{\lambda} E_{c_ic_j}^{\lambda}}, \tag{27}$$

where

$$\begin{aligned} \underline{Q_{c_ic_j}^{\lambda}} &= Q_{c_ic_j}^{\lambda}(1 - \gamma_1), \ \overline{Q_{c_ic_j}^{\lambda}} = Q_{c_ic_j}^{\lambda}(1 + \gamma_1), \\ \gamma_1 &= \sigma_\alpha / \sqrt{N_{c_ic_j}^{\lambda} Q_{c_ic_j}^{\lambda}}, \ \gamma_2 = \sigma_\alpha / \sqrt{N_{c_ic_j}^{\lambda} Q_{c_ic_j}^{\lambda} E_{c_ic_j}^{\lambda}}, \\ \underline{Q_{c_ic_j}^{\lambda} E_{c_ic_j}^{\lambda}} &= Q_{c_ic_j}^{\lambda} E_{c_ic_j}^{\lambda}(1 - \gamma_2), \ \overline{Q_{c_ic_j}^{\lambda} E_{c_ic_j}^{\lambda}} = Q_{c_ic_j}^{\lambda} E_{c_ic_j}^{\lambda}(1 + \gamma_2). \end{aligned} \tag{28}$$

Here σ_α is the number of standard deviations, which is related to the failure probability of the security analysis. we choose $\sigma_\alpha = 5$, which means the failure probability is 5.73×10^{7}. These parameters used in our method are the same as those in the refs 12 and 29. $N_{c_ic_j}^{\lambda}$ is the length of data in the situation that Alice has the c_i mode and Bob has the c_j mode, where $i,j = 0$ or 1. Thus, the lower bound of Y_{11}^{λ} and the upper bound of e_{11}^{λ} given by Eqs (9) and (12), respectively, can be modified to ref. 29

$$\begin{aligned} Y_{11}^{\lambda} \geq \underline{Y_{11}^{\lambda}} &= \Big(c_{c_1c_1} \overline{Q_{c_1c_1}^{\lambda}} + c_{c_1c_0} \underline{Q_{c_1c_0}^{\lambda}} + c_{c_0c_1} \underline{Q_{c_0c_1}^{\lambda}} + c_{c_0c_0} \overline{Q_{c_0c_0}^{\lambda}} \\ &\quad - c_{c_10} \overline{Q_{c_10}^{\lambda}} - c_{c_0c_0} \overline{Q_{c_0c_0}^{\lambda}} - c_{0c_1} \overline{Q_{0c_1}^{\lambda}} - c_{0c_0} \overline{Q_{0c_0}^{\lambda}} + c_{00} \underline{Q_{00}^{\lambda}}\Big) \\ &\quad \times \left[(K - A_1B_1)\left(q_{0,a}^{c_0} q_{1,a}^{c_0} + q_{0,a}^{c_1} q_{1,a}^{c_1}\right)\left(q_{0,b}^{c_0} q_{1,b}^{c_0} + q_{0,b}^{c_1} q_{1,b}^{c_1}\right)\right]^{-1}, \end{aligned} \tag{29}$$

$$e_{11}^{\lambda} \leq \overline{e_{11}^{\lambda}} = \left(\overline{Q_{c_1c_1}^{\lambda} E_{c_1c_1}^{\lambda}} - q_{0,a}^{c_1} \underline{Q_{0c_1}^{\lambda} E_{0c_1}^{\lambda}} - q_{0,b}^{c_1} \underline{Q_{c_10}^{\lambda} E_{c_10}^{\lambda}} - q_{0,a}^{c_1} q_{0,b}^{c_1} \underline{Q_{00}^{\lambda} E_{00}^{\lambda}}\right) / \left(q_{1,a}^{c_1} q_{1,b}^{c_1} \underline{Y_{11}^{\lambda}}\right). \tag{30}$$

We can also modify the lower bound of $Q_{11}^{c_1c_1}$ and the upper bound of e_{11}^{λ} given by Eqs (22) and (25), respectively, as follows

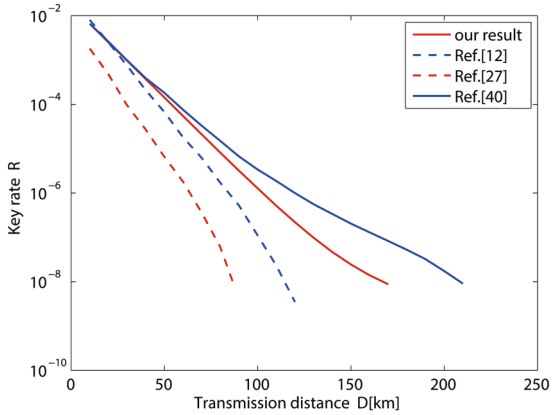

Figure 2. Key generation rate versus the total transmission distance with the passive decoy state method based on polarization encoding mode (red solid line) compared to the passive decoy state method based on phase encoding mode (red dot-dashed line; ref. 29), the active decoy state method using two decoy states (blue dot-dashed line; ref. 12), and recently optimal active decoy state method (blue solid line; ref. 17).

$$Q_{11}^{c_1c_1} \geq \underline{Q_{11}^{c_1c_1,L}} = \frac{\underline{Q_{c_0c_0}} - \overline{Q_{c_1c_1}} - \left(\frac{q_{0,a}^{c_0,U} q_{0,b}^{c_0,U}}{q_{0,a}^{c_1,L} q_{0,b}^{c_1,L}} - 1\right)\frac{E_{c_1c_1}Q_{c_1c_1}}{e_{00}}}{\frac{q_{1,a}^{c_0,U} p_{1,b}^{c_0,U}}{q_{1,a}^{c_1,L} q_{1,b}^{c_1,L}} - 1}, \tag{31}$$

$$e_{11} \leq \overline{e_{11}^{U}} = \frac{1}{\underline{Q_{11}^{c_1c_1,L}}}\left(\overline{Q_{c_1c_1}E_{c_1c_1}} - q_{0,a}^{c_1}\underline{Q_{0c_1}E_{0c_1}} - q_{0,b}^{c_1}\underline{Q_{c_10}E_{c_10}} - q_{0,a}^{c_1}q_{0,b}^{c_1}\underline{Q_{00}E_{00}}\right). \tag{32}$$

Substituting Eqs (29) and (30) into Eqs (7), (31) and (32) into Eq. (26), we can respectively estimate the key generation rate with or without intensity fluctuation in the case of finite resource in different data length. In our method, we assume that Alice's and Bob's data length are the same for each pair of intensities.

Numerical Simulation. From our security analysis, we can obtain the yield Y_{11}^{Z} and the error rate e_{11}^{X}, respectively, when Alice and Bob send single-photon pulses to Charles, as well as the total gains and the overall error rates in both the X basis and the Z basis. Then, we can get the key generation rate plotted in Fig. 2. The practical parameters for numerical simulations used in our method are $\eta_d = 14.5\%$, $e_d = 1.5\%$, $Y_0 = 3 \times 10^{-6}$, $f_e = 1.16$ and $\alpha = 0.2\,dB/km$. These experimental parameters, including the detection efficiency η_d, the total misalignment error e_d and the background rate Y_0, are from the 144 km QKD experiment reported in ref. 40. Since two PDs (Photon Detectors) are used in ref. 40, the background rate of each PD here is roughly a quarter of the value there. We assume our model that the six PDs in MDI-QKD (see Fig. 1) have identical η_d and Y_0.

In Fig. 2, we compare the key generation rate of MDI-QKD given by our passive decoy state method with that given by an active decoy state method with two decoy states in ref. 12 and recently optimal active decoy state method in ref. 17. The key generation rate is maximized by optimizing the intensity of sources. It can clearly be seen that the passive decoy state method can provide a performance comparable to the active one. We also compare the key generation rate of MDI-QKD given by our passive decoy state method which based on polarization encoding mode with that based on phase encoding mode in ref. 29, due to these two encoding modes are both applied in practical systems.

In addition, we will characterize the relationship between the key generation rate and the intensity fluctuation when transmission distance d is fixed. The result is shown in Fig. 3. Define $R(\delta)/R(0)$ as the fidelity of the the key generation rate with passive decoy state method, where $R(\delta)$ denotes the the key generation rate R with intensity fluctuation and $R(0)$ denotes the the key generation rate R with no intensity fluctuation. From Fig. 3, we can see that the $R(\delta)/R(0)$ is getting to 0 with δ getting to 0.1. It indicates that when intensity fluctuation increases, the fidelity decreases, so does the key generation rate. Furthermore, we can also get that the effect of intensity fluctuation on the key generation rate monotonously increases with the increase of the transmission distance. So when we analyse the performance of MDI-QKD, the influence of intensity fluctuation can not be neglected, especially over long-distance communications.

Figure 4 shows the key generation rate of MDI-QKD given by our passive-decoy-state method with different intensity fluctuation. We can find that intensity fluctuation obviously limit the secret key rate. In order to further study the effect of intensity fluctuation for different total numbers of transmitting signals N, we show the relations between $R(\delta)/R(0)$ and the secure transmission distance given that the intensity fluctuation is fixed to be 0.05 in Fig. 5. We can find that the smaller the data size of total transmitting signals is, more obvious the effect of intensity fluctuation is.

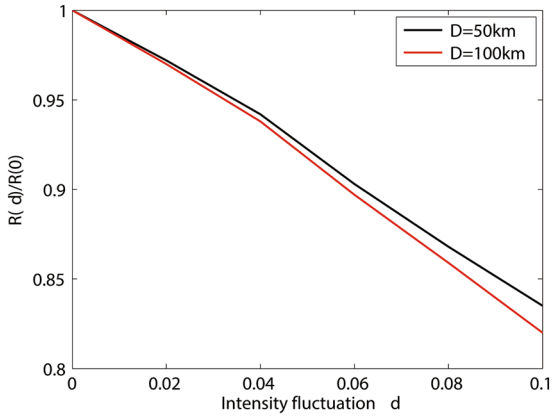

Figure 3. The fidelity of the the key generation rate $R(\delta)/R(0)$ versus intensity fluctuation δ.

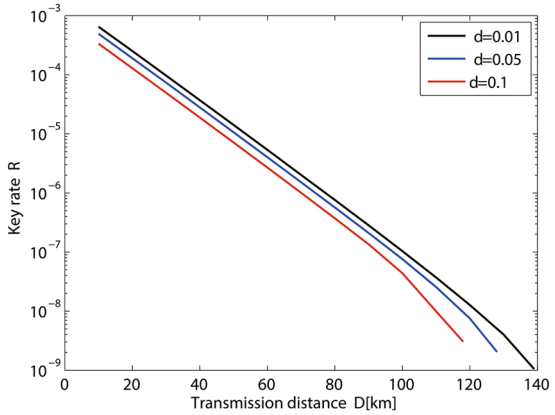

Figure 4. Secret key rate R versus the transmission distance with $\delta = 0.01,0.05,0.09,0.1$ (curves from right to left).

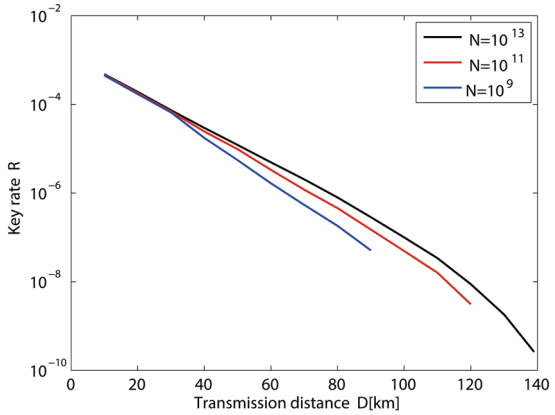

Figure 5. Secret key rate R versus the transmission distance for $\delta = 0.05$ and $N = 1 \times 10^x$ with $x = 9,10,11,12,13$ (curves from left to right).

Discussion

In conclusion, we applied the passive decoy state method in the MDI-QKD based on polarization encoding mode, and gave a security analysis of this protocol. Using the passive decoy state method, not only all detector side channel attacks can be removed, but also side channel attacks on the sources can be overcome, which the active source modulation method may bring. We analysed the security of this protocol, and found that the MDI-QKD with our passive decoy state method can have a performance comparable to the protocol with the active decoy state method and the passive decoy state method based on phase encoding mode. To fit for the demand of practical

application, we discuss intensity fluctuation in the security analysis of passive decoy state MDI-QKD protocol. In this case, we got the key generation rate through the formulas of yield and error rate derived in our paper. Based on the total gain and the overall error rate derived in our paper, we gave numerical simulations for our protocol. We showed that intensity fluctuation has a non-negligible effect on the secret key rate of the passive decoy state MDI-QKD protocol, especially in the case of small data size of total transmitting signals and long distance transmission. In addition, our analysis of statistical fluctuation shows that the finite-size effect also limits the key generation rate of MDI-QKD with passive decoy state method.

References

1. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145–195 (2002).
2. Lo, H. K. & Chau, H. F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **283**, 2050 (1999).
3. Scarani, V., Acin, A., Ribordy, G. & Gisin, N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.* **92**, 057901 (2004).
4. Bennett, C. H. & Brassard. G. Quantum cryptography: public-key distribution and coin tossing. *In Proceedings of IEEE International Conference on Computers Systems and Signal Processing* 175–179 (1984).
5. Shor, P. W. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**, 441 (2000).
6. Lo, H. K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
7. Liu, Y. *et al*. Experimental Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **111**, 130502 (2013).
8. Tang, Z. Y. *et al*. Experimental Demonstration of Polarization Encoding Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **112**, 190503 (2014).
9. Rubenok, A., Slater, J. A., Chan, P., Lucio-Martinez, I. & Tittel, W. Real-World Two-Photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attacks. *Phys. Rev. Lett.* **111**, 130501 (2013).
10. Ma, X. F. & Razavi, M. Alternative schemes for measurement-device-independent quantum key distribution. *Phys. Rev. A* **86**, 062319 (2012).
11. Song, T. T., Wen, Q. Y., Guo, F. Z. & Tan, X. Q. Finite-key analysis for measurement-device-independent quantum key distribution. *Phys. Rev. A* **86**, 022332 (2012).
12. Sun, S. H., Gao, M., Li, C. Y. & Liang, L. M. Practical decoy-state measurement-device-independent quantum key distribution. *Phys. Rev. A* **87**, 052329 (2013).
13. Xu, F., Xu, H. & Lo, H. K. Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution. *Phys. Rev. A* **89**, 052333 (2014).
14. Zhou, C. *et al*. Biased decoy-state measurement-device-independent quantum key distribution with finite resources. *Phys. Rev. A* **91**, 022313 (2015).
15. Wang, X. B. Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors. *Phys. Rev. A* **87**, 012320 (2013).
16. 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).
17. 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).
18. Lin, S., Wen, Q. Y., Gao, F. & Zhu, F. C. Eavesdropping on secure deterministic communication with qubits through photon-number-splitting attacks. *Phys. Rev. A* **79**, 054303 (2009).
19. Brassard, G., Lütkenhaus, N., Mor, T. & Sanders, B. C. Limitations on practical quantum cryptography. *Phys. Rev. Lett.* **85**, 1330 (2000).
20. Wang, X. B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94**, 230503 (2005).
21. Song, T. T., Zhang, J., Qin, S. J., Gao, F. & Wen, Q. Y. Finite-key analyses for quantum key distribution with decoy-states. *Quant. Inf. Comp.* **11**, 374–389 (2011).
22. Jiang, M. S., Sun, S. H., Li, C. Y. & Liang, L. M. Wavelength-selected photon-number-splitting attack against plug-and-play quantum key distribution systems with decoy states. *Phys. Rev. A* **86**, 032310 (2012).
23. Ma, X. F. & Lo, H. K. Quantum key distribution with triggering parametric down-conversion sources. *New J. Phys.* **10**, 073018 (2008).
24. Curty, M., Moroder, T., Ma, X. & Lütkenhaus, N. Non-Poissonian statistics from Poissonian light sources with application to passive decoy state quantum key distribution. *Opt. Lett.* **34**, 3238 (2009).
25. Curty, M., Ma, X. F., Qi, B. & Moroder, T. Passive decoy-state quantum key distribution with practical light sources. *Phys. Rev. A* **81**, 022310 (2010).
26. Mauerer, W. & Silberhorn, C. Quantum key distribution with passive decoy state selection. *Phys. Rev. A* **75**, 050305(R) (2007).
27. Adachi, Y., Yamamoto, T., Koashi, M. & Imoto, N. Simple and efficient quantum key distribution with parametric down-conversion. *Phys. Rev. Lett.* **99**, 180503 (2007).
28. Song, T. T., Qin, S. J., Wen, Q. Y., Wang, Y. K. & Jia, H. Y. Finite-key security analyses on passive decoy-state QKD protocols with different unstable sources. *Scientific Reports* **5**, 15276 (2015).
29. Shan, Y. Z. *et al*. Measurement-device-independent quantum key distribution with a passive decoy-state method. *Phys. Rev. A* **90**, 042334 (2014).
30. FerreiradaSilva, T. *et al*. Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. *Phys. Rev. A* **88**, 052303 (2013).
31. Xu, F., Curty, M., Qi, B. & Lo, H. K. Practical aspects of measurement-device-independent quantum key distribution. *New J. Phys.* **15**, 113007 (2013).
32. Wang, S. *et al*. Decoy-state theory for the heralded single-photon source with intensity fluctuations. *Phys. Rev. A* **79**, 062309 (2009).
33. Hu, J. Z. & Wang, X. B. Reexamination of the decoy-state quantum key distribution with an unstable source. *Phys. Rev. A* **82**, 012331 (2010).
34. Li, Y., Bao, W. S., Li, H. W., Zhou, C. & Wang, Y. Passive decoy-state quantum key distribution using weak coherent pulses with intensity fluctuations. *Phys. Rev. A* **89**, 032329 (2014).
35. Stucki, D., Gisin, N., Guinnard, O., Ribordy, G. & Zbinden, H. Quantum key distribution over 67 km with a plug & play system. *New J. Phys.* **4**, 41 (2002).
36. Gottesman, D., Lo, H. K., Lütkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. *Quantum Inf. Comput.* **4**, 325 (2004).
37. Lo, H. K., Ma, X. F. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
38. Ma, X. F., Qi, B., Zhao, Y. & Lo, H. K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **72**, 012326 (2005).
39. Ma, X. F., Fung, C. & Razavi, M. Statistical fluctuation analysis for measurement-device-independent quantum key distribution. *Phys. Rev. A* **86**, 052305 (2012).
40. Ursin, R. *et al*. Entanglement-based quantum communication over 144 km. *Nat. Phys.* **3**, 481 (2007).

Acknowledgements
This work was supported by the National Natural Science Foundation of China, Grants No. 61572081, No. 61672110 and No. 61671082.

Author Contributions
L.L. proposed the theoretical method. L.L. and F.Z.G. wrote the main manuscript text. F.Z.G. and Q.Y.W. reviewed the manuscript.

Additional Information
Supplementary information accompanies this paper at doi:10.1038/s41598-017-09367-y

Competing Interests: The authors declare that they have no competing interests.

Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.