Quantum Inf Process (2018) 17:50
https://doi.org/10.1007/s11128-018-1818-9

Measurement-device-independent quantum key distribution with multiple crystal heralded source with post-selection

Dong Chen[1,2] · **Zhao Shang-Hong**[2] · **Deng MengYi**[3]

Received: 23 January 2017 / Accepted: 10 January 2018 / Published online: 24 January 2018

Abstract The multiple crystal heralded source with post-selection (MHPS), originally introduced to improve the single-photon character of the heralded source, has specific applications for quantum information protocols. In this paper, by combining decoy-state measurement-device-independent quantum key distribution (MDI-QKD) with spontaneous parametric downconversion process, we present a modified MDI-QKD scheme with MHPS where two architectures are proposed corresponding to symmetric scheme and asymmetric scheme. The symmetric scheme, which linked by photon switches in a log-tree structure, is adopted to overcome the limitation of the current low efficiency of m-to-1 optical switches. The asymmetric scheme, which shows a chained structure, is used to cope with the scalability issue with increase in the number of crystals suffered in symmetric scheme. The numerical simulations show that our modified scheme has apparent advances both in transmission distance and key generation rate compared to the original MDI-QKD with weak coherent source and traditional heralded source with post-selection. Furthermore, the recent advances in integrated photonics suggest that if built into a single chip, the MHPS might be a practical alternative source in quantum key distribution tasks requiring single photons to work.

Keywords Measurement-device-independent quantum key distribution · Multiple crystal heralded source with post-selection · Symmetric and asymmetric scheme

✉ Dong Chen
dongchengfkd@163.com

1 College of Information and Communication, Xi'an 710006, China

2 College of Information and Navigation, Xi'an 710077, China

3 ShanDong University, Ji'nan 250014, China

1 Introduction

Quantum key distribution [1] (QKD) has long been a promising area for application of quantum effects toward solving secure communication problems and its unconditional security can be ensured by the theory of quantum mechanics [2–4]. Despite these developments, there is still a large gap between theory and practice, in the sense that the security is based on assumptions that are not met by experimental implementations. Subtle details in implementations may introduce some laws that could potentially open side channel loopholes to attack, such as photon number splitting attack (PNS) [5], partially random phase attack [6], fake state attack [7], time shift attack [8], and blinding attack [9]. Recently, measurement-device-independent quantum key distribution (MDI-QKD) has been proposed by Lo et al. [10], which is immune to all the detector side channel attacks.

In recent MDI-QKD experiment, Refs. [11,12] implemented the proof-of-principle demonstration of time-bin encoding and polarization encoded MDI-QKD, and in Ref. [13,14] two real demonstrations with key exchange have been performed with time-bin encoding and polarization encoded for MDI-QKD. Recently, Ref. [15] reported the results of MDI-QKD over 404 km of ultralow-loss optical fiber and 311 km of standard optical fiber by employing an optimized four-intensity decoy-state method.

Weak coherence source (WCS), which has a Poisson distribution of photon number and emits n-photon state with the possibility $P_{\mathrm{WCS}} = \mathrm{e}^{-\mu}\mu^n/n!$, is usually used instead of single photon source in practical experiments. However, due to the multi-photon events of WCS, the implementations of MDI-QKD protocol usually employ decoy-state method to beat the PNS attack. Besides the WCSs, there is another easily implementable source, the heralded single-photon source (HSPS) [16–18], which seem to give the compromise between high single-photon events and low multi-photon events in QKD.

Spontaneous parametric downconversion (SPDC) process is widely used as the sources in QKD such as the trigged or heralded single-photon source. Ref. [19] derived a formula for estimating the single-photon contribution for the MDI-QKD with Poisson-distributed heralded source with post-selection (HSPS). Ref. [20] proposed MDI-QKD with thermal distributed SPDCS using polarization encoding to increase the fraction of the yield of single photon. There are some strategies for improving the single-photon character and decreasing multi-photon event of the heralded source. Ref. [21] proposed a multiple heralded source with post-selection (MHPS) scheme to suppress multi-photon events by using an m-to-1 optical switch triggered by a detector on the idler photon of each heralded source. Ref [22] proposed a symmetric scheme (SMHPS) using m heralded units linked by $m-1$ binary optical switch in a tree structure to overcome the limitation of the low efficiency of m-to-1 optical switches. Ref. [23] proposed an asymmetric scheme (AMHPS) to settle the scalability issue suffered in the symmetric scheme. Ref. [24] demonstrates the different architectures inserted in a common model of QKD implementation based on the BB84 protocol in detail.

In this paper, we present a modified decoy-state MDI-QKD scheme with multiple crystal heralded source with post-selection and analyze the two architectures of MHPS in decoy-state-modified MDI-QKD. The symmetric scheme, which linked by 2-to-1 optical switches in a log-tree structure, is adopted to overcome the limitation of the

low efficiency of m-to-1 optical switches. The asymmetric scheme, which shows a chained structure, is used to cope with the scalability issue with increase in the number of crystals suffered in the symmetric scheme. The numerical simulations show that our modified scheme has apparent advances both in distance and key generation rate compared to the original MDI-QKD with weak coherent source.

2 Model and deduction

In our modified MDI-QKD protocol, Alice and Bob generated a polarization entangled photon pair by exploiting spontaneous parametric down conversion in a β-barium borate crystal (BBO) using multiple crystal heralded unit. The two parties both adopt the two-intensity decoy state, where a variable optical attenuator and a random number generator are used to change the output statistics after HS source, to solve the multi-photon events also existed in multiple crystal heralded sources. They use single-photon detectors (D_A/D_B) to detect the more idle light and randomly prepare the signal light into a BB84 polarization state with a polarization modulator. Charlie performs a partial BSM when the signal pulses from Alice and Bob arrive at a 50:50 beam splitter. Four single-photon detectors are employed to detect the results. Based on announcement for each pulse, Alice and Bob compare the bases they used and estimate the secret key rate using the decoy state method [25]:

$$R = P_{\mu_2}(1)\, P_{\nu_2}(1)\, Y_{11}^{z}\left[1 - H_2\left(e_{11}^{x}\right)\right] - Q_{\mu_2\nu_2}^{z} f\left(E_{\mu_2\nu_2}^{z}\right) H_2\left(E_{\mu_2\nu_2}^{z}\right), \quad (1)$$

where Alice's pulse intensity is μ_i and Bob's pulse intensity is ν_j, $P_{\mu_2}(1)$ and $P_{\nu_2}(1)$ denote the single photon number distribution of signal state, f is the error correction, H_2 is the binary Shannon function, $Q_{\mu_i\nu_j}$ and $E_{\mu_i\nu_j}$ are used to denote the gain and QBER, respectively:

$$Q_{\mu_i\nu_j}^{w} = \sum_{n,m=0}^{\infty} P_{\mu_i}(n) P_{\nu_j}(m)\, Y_{nm}^{w} \quad (2)$$

$$E_{\mu_i\nu_j}^{w} Q_{\mu_i\nu_j}^{w} = \sum_{n,m=0}^{\infty} P_{\mu_i}(n) P_{\nu_j}(m)\, e_{nm}^{w} Y_{nm}^{w}, \quad (3)$$

where $w = x, z$ denotes the choice of two bases, x-base is used as test set to estimate the parameters of channel and z-base is used to distill the final secret key. $P_{\mu_i}(m)$ and $P_{\nu_j}(n)$ denote the photon number distribution, respectively. Y_{nm} is the yield and e_{nm} is the error rate, respectively, where n and m denote the number photons sent by the legitimate users.

The modified MDI-QKD scheme with MHPS, which consists of an array of m heralded source (HS) units simultaneously pumped with a laser pulse with intensity, shows the better compromise between high pair production rate and low multi-photon events. For each HS unit, the more idle photon is used as a trigger for the signal one, which is injected into an optical switch. The ideal photon number distribution of

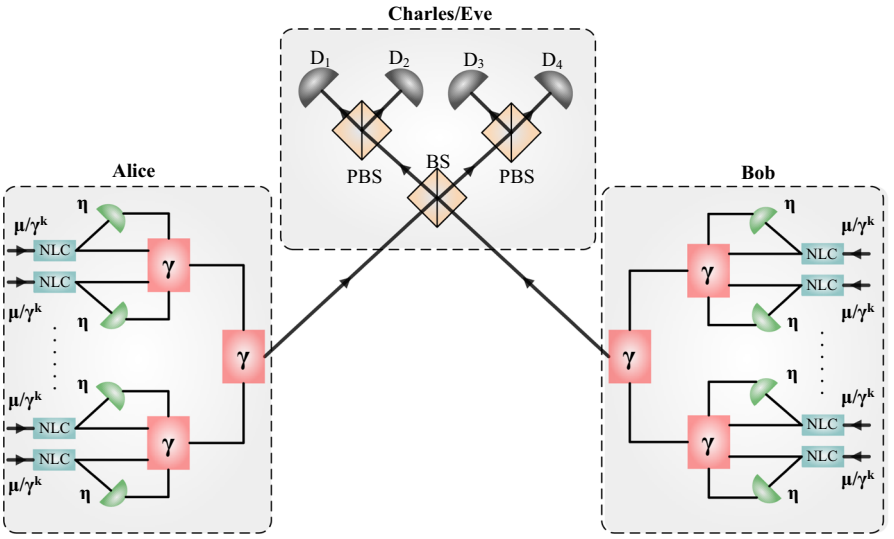

Fig. 1 Schematic of MDI-QKD with SMHPS

MHPS is given as follows:

$$P_n^{\mathrm{MHPS}}(\mu, m) = \begin{cases} \mathrm{e}^{-m\mu}, & n = 0 \\ \frac{\mu^n}{n!}\mathrm{e}^{-\mu}\frac{1-\mathrm{e}^{-m\mu}}{1-\mathrm{e}^{-\mu}}, & n \geq 1 \end{cases} \tag{4}$$

where μ is the pump intensity and m is the number of HS unit, which can be employed a parallel implementation to suppress the multi-photons events by making the intensity of the pump of each crystal low. However, an efficient implementation of m-to-1 switch is not currently available in MHPS. By employing a total of $m-1$ binary polarization switching routers, the SMHPS and AMHPS configuration are introduced in realistic scenarios. The schematic of MDI-QKD with SMHPS and AMHPS is shown in Figs. 1 and 2, respectively. Moreover, detection efficiency η and optical switch transmissivity γ are considered to make our schemes more practical with state-of-the-art technology.

In the schematic of MDI-QKD with SMHPS, Alice (Bob) use parallel nonlinear crystals (NLC) which are pumped with intensity μ/γ^k. The photon number distribution of SMHPS is given by:

$$\begin{aligned} P_n^{\mathrm{SMHPS}}(\mu, m, \eta, \gamma) = & \frac{(1-\eta)\,\mu\mathrm{e}^{-(1-\eta)\mu}}{n!}\mathrm{e}^{-\eta\mu(2^k/\gamma^k)} \\ & + \frac{\mu^n\mathrm{e}^{-\mu}}{n!}\frac{1-(1-\eta)^n\mathrm{e}^{-\eta(1/\gamma^k-1)\mu}}{1-\mathrm{e}^{-\eta(\mu/\gamma^k)}}\left(1-\mathrm{e}^{-\eta\mu(2^k/\gamma^k)}\right) \end{aligned} \tag{5}$$

Different with MDI-QKD with SMHPS using same intensity to pump the NLC, MDI-QKD with AMHPS adopted a different intensity to compensate the different number of traversed 2-to-1 optical switches. The photon number distribution of AMHPS is:

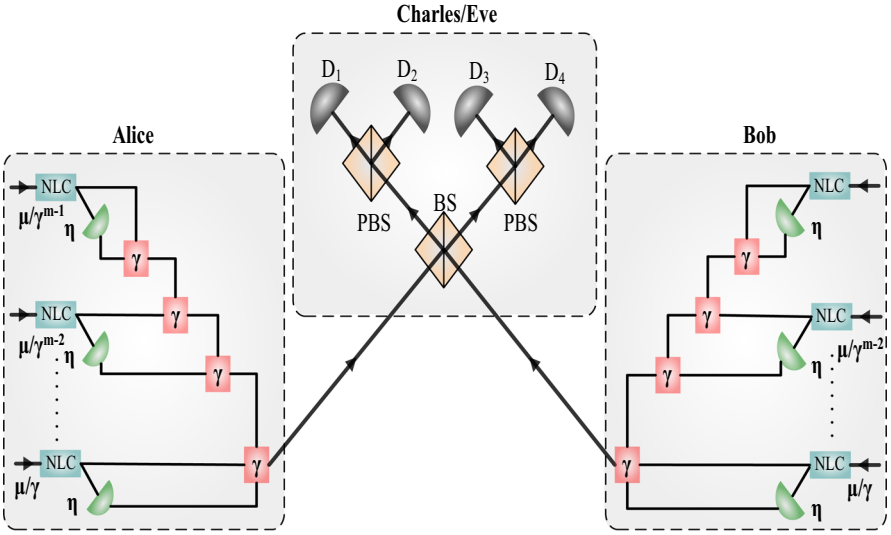

Fig. 2 Schematic of MDI-QKD with AMHPS

Table 1 Multi-photon probabilities, single-photon probabilities, and vacuum events of different sources

Source	Vacuum event	Single photon	Multi-photon
WCS	0.7408	0.2222	0.0369
MHPS ($m = 2$)	0.4493	0.4479	0.1028
MHPS ($m = 4$)	0.2019	0.6491	0.1490
MHPS ($m = 8$)	0.0408	0.7801	0.1791
MHPS ($m = 16$)	0.0083	0.8504	0.1413
MHPS ($m = 32$)	6.77×10^{-5}	0.8574	0.1425

The mean photon number of the source is $\mu = 0.3$. The transmittance of 2-to-1 optical switches $\gamma = 0.5$. The detector efficiency $\eta = 0.7$

$$
\begin{aligned}
P_n^{\mathrm{AMHPS}}(\mu, m, \eta, \gamma) = & \frac{(1-\eta)\,\mu \mathrm{e}^{-(1-\eta)\mu}}{n!} \mathrm{e}^{-\eta\mu\{[(2-\gamma)\gamma^{1-m}-1]/(1-\gamma)\}} \\
& + \frac{\mu^n \mathrm{e}^{-\mu}}{n!} \sum_{i=1}^{m} \mathrm{e}^{-\eta\mu[(\gamma^{1-i}-1)/(1-\gamma)]} \\
& \times \left[1-(1-\eta)^n \mathrm{e}^{-\eta\mu} \mathrm{e}^{-\eta\mu/\gamma^{k_i}}\right]
\end{aligned} \tag{6}
$$

where $k_i = \begin{cases} i, & i \le m-1 \\ m-1, & i = m \end{cases}$.

Table 1 shows the comparison of multi-photon probabilities, single-photon probabilities and vacuum events between WCS and MHPS. Multiple crystal heralded source with post-selection seems to give the best compromise between high single-photon events and low multi-photon events.

In the following, we give two tight formulas to estimate these parameters. For simplicity, we assume that the detection efficiency and dark count rate of the trigger detector of Alice's and Bob's are same, that is $\eta^A = \eta^B = \eta$, $P_d^A = P_d^B = P_d$.

The lower bound of Y_{11}^w—note that the expression of Eq. (2) is independent on w, and thus we neglect the superscript w for simplicity in the following of the paper.Then the total gain $Q_{\mu_i \nu_j}$ for the signal state (μ_2, ν_2) and the decoy state (μ_1, ν_1) are:

$$\begin{aligned}
&\frac{1-\mathrm{e}^{-\mu_i}}{1-\mathrm{e}^{-m_A\mu_i}}\frac{1-\mathrm{e}^{-\nu_j}}{1-\mathrm{e}^{-m_B\nu_j}}\mathrm{e}^{\mu_i+\nu_j}Q_{\mu_i\nu_j} \\
&= \frac{1-\mathrm{e}^{-\nu_j}}{1-\mathrm{e}^{-m_B\nu_j}}\nu_j Q_{0\nu_j} + \frac{1-\mathrm{e}^{-\mu_i}}{1-\mathrm{e}^{-m_A\mu_i}}\mu_i Q_{\mu_i 0} - Q_{00} + \mu_i\nu_j Y_{11} + h\left(\mu_i, \nu_j\right) \qquad (7) \\
&h\left(\mu_i, \nu_j\right) = \sum_{m=2}^{\infty}\frac{\mu_i\nu_j^m}{m!}Y_{1m} + \sum_{m=2}^{\infty}\frac{\mu_i^n\nu_j}{n!}Y_{n1} + \sum_{m=2}^{\infty}\frac{\mu_i^n\nu_j^m}{n!m!}Y_{nm} \qquad (8)
\end{aligned}$$

Thus we will have:

$$\begin{aligned}
&\frac{1-\mathrm{e}^{-\mu_2}}{1-\mathrm{e}^{-m_A\mu_2}}\frac{1-\mathrm{e}^{-\nu_2}}{1-\mathrm{e}^{-m_B\nu_2}}\mathrm{e}^{\mu_2+\nu_2}Q_{\mu_2\nu_2} - \frac{1-\mathrm{e}^{-\mu_1}}{1-\mathrm{e}^{-m_A\mu_1}}\frac{1-\mathrm{e}^{-\nu_1}}{1-\mathrm{e}^{-m_B\nu_1}}\mathrm{e}^{\mu_1+\nu_1}Q_{\mu_1\nu_1} \\
&= g_1 + (\mu_2\nu_2 - \mu_1\nu_1)Y_{11} + \sum_{m=2}^{\infty}\frac{\mu_2\nu_2^m - \mu_1\nu_1^m}{m!}Y_{1m} \\
&\quad + \sum_{n=2}^{\infty}\frac{\mu_2^n\nu_2 - \mu_1^n\nu_1}{n!}Y_{n1} + \sum_{n,m=2}^{\infty}\frac{\mu_2^n\nu_2^m - \mu_1^n\nu_1^m}{n!m!}Y_{nm} \\
&\geq g_1 + g_2 + g_3 - (\mu_2\nu_2 - \mu_1\nu_1 + \alpha\mu_2\nu_1 + \alpha\mu_1\nu_2)Y_{11} \qquad (9)
\end{aligned}$$

where we use the fact that for any $n, m \geq 2$, the following inequalities always hold, which are given by [26]:

$$\begin{aligned}
\frac{\mu_2\nu_2^m - \mu_1\nu_1^m}{\mu_2\nu_1^m + \mu_1\nu_2^m} &\geq \frac{\mu_2\nu_2^2 - \mu_1\nu_1^2}{\mu_2\nu_1^+\mu_1\nu_2^2} \equiv a > 0 \\
\frac{\mu_2^n\nu_2 - \mu_1^n\nu_1}{\mu_2^n\nu_1 + \mu_1^n\nu_2} &\geq \frac{\mu_2^2\nu_2 - \mu_1^2\nu_1}{\mu_2^2\nu_1^+\mu_1^2\nu_2} \equiv b > 0 \\
\frac{\mu_2^n\nu_2^m - \mu_1^n\nu_1^m}{\mu_2^n\nu_1^m + \mu_1^n\nu_2^m} &\geq \frac{\mu_2^2\nu_2^2 - \mu_1^2\nu_1^2}{\mu_2^2\nu_1^2 + \mu_1^2\nu_2^2} \equiv c > 0 \qquad (10)
\end{aligned}$$

And $\alpha = \min\{a, b, c\}$

Here g_0, g_1, g_2 are defined as:

$$\begin{aligned}
g_1 = &\frac{1-\mathrm{e}^{-\nu_2}}{1-\mathrm{e}^{-m_B\nu_2}}\mathrm{e}^{\nu_2}Q_{0\nu_2} + \frac{1-\mathrm{e}^{-\mu_2}}{1-\mathrm{e}^{-m_A\mu_2}}\mathrm{e}^{\mu_2}Q_{\mu_2 0} \\
&- \frac{1-\mathrm{e}^{-\nu_1}}{1-\mathrm{e}^{-m_B\nu_1}}\mathrm{e}^{\nu_1}Q_{0\nu_1} - \frac{1-\mathrm{e}^{-\mu_1}}{1-\mathrm{e}^{-m_A\mu_1}}\mathrm{e}^{\mu_1}Q_{\mu_1 0}
\end{aligned}$$

$$
\begin{aligned}
g_2 = \alpha \Bigg(& \frac{1-\mathrm{e}^{-\mu_2}}{1-\mathrm{e}^{-m_A\mu_2}} \frac{1-\mathrm{e}^{-\nu_1}}{1-\mathrm{e}^{-m_B\nu_1}} \mathrm{e}^{\mu_2}\mathrm{e}^{\nu_1} Q_{\mu_2\nu_1} - \frac{1-\mathrm{e}^{-\mu_2}}{1-\mathrm{e}^{-m_A\mu_2}} \mathrm{e}^{\mu_2} Q_{\mu_2 0} \\
& - \frac{1-\mathrm{e}^{-\nu_1}}{1-\mathrm{e}^{-m_B\nu_1}} \mathrm{e}^{\nu_1} Q_{0\nu_1} + Q_{00} \Bigg) \\
g_3 = \alpha \Bigg(& \frac{1-\mathrm{e}^{-\mu_1}}{1-\mathrm{e}^{-m_A\mu_1}} \frac{1-\mathrm{e}^{-\nu_2}}{1-\mathrm{e}^{-m_B\nu_2}} \mathrm{e}^{\mu_1}\mathrm{e}^{\nu_2} Q_{\mu_1\nu_2} - \frac{1-\mathrm{e}^{-\mu_1}}{1-\mathrm{e}^{-m_A\mu_1}} \mathrm{e}^{\mu_1} Q_{\mu_1 0} \\
& - \frac{1-\mathrm{e}^{-\nu_2}}{1-\mathrm{e}^{-m_B\nu_2}} \mathrm{e}^{\nu_2} Q_{0\nu_2} + Q_{00} \Bigg)
\end{aligned} \tag{11}
$$

Thus the lower bound of Y_{11} is given by:

$$
\begin{aligned}
Y_{11} \geq \underline{Y_{11}} & \\
\equiv & \frac{g_0 + g_1 + g_2 - \frac{1-\mathrm{e}^{-\mu_2}}{1-\mathrm{e}^{-m_A\mu_2}} \frac{1-\mathrm{e}^{-\nu_2}}{1-\mathrm{e}^{-m_B\nu_2}} \mathrm{e}^{\mu_2}\mathrm{e}^{\nu_2} Q_{\mu_2\nu_2}}{(\mu_1\nu_1 - \mu_2\nu_2 + \alpha\mu_2\nu_2 + \alpha\mu_1\nu_1)} \\
& + \frac{\frac{1-\mathrm{e}^{-\mu_1}}{1-\mathrm{e}^{-m_A\mu_1}} \frac{1-\mathrm{e}^{-\nu_1}}{1-\mathrm{e}^{-m_B\nu_1}} \mathrm{e}^{\mu_1}\mathrm{e}^{\nu_1} Q_{\mu_1\nu_1}}{(\mu_1\nu_1 - \mu_2\nu_2 + \alpha\mu_2\nu_2 + \alpha\mu_1\nu_1)}
\end{aligned} \tag{12}
$$

The upper bound of e_{11}^{w}—according to Eqs. (3) and (10), we can calculate the upper bound of single-photon error rate:

$$
\begin{aligned}
e_{11} \leq \overline{e_{11}} \equiv & \frac{\frac{1-\mathrm{e}^{-\mu_1}}{1-\mathrm{e}^{-m_A\mu_1}} \frac{1-\mathrm{e}^{-\nu_1}}{1-\mathrm{e}^{-m_B\nu_1}} \mathrm{e}^{\mu_1}\mathrm{e}^{\nu_1} Q_{\mu_1\nu_1} E_{\mu_1\nu_1} - \frac{1-\mathrm{e}^{-\mu_1}}{1-\mathrm{e}^{-m_A\mu_1}} \mathrm{e}^{\mu_1} Q_{\mu_1 0} E_{\mu_1 0}}{\mu_1\underline{\nu_1 Y_{11}}} \\
& - \frac{\frac{1-\mathrm{e}^{-\nu_1}}{1-\mathrm{e}^{-m_B\nu_1}} \mathrm{e}^{\nu_1} Q_{0\nu_1} E_{0\nu_1} + Q_{00} E_{00}}{\mu_1\underline{\nu_1 Y_{11}}}
\end{aligned} \tag{13}
$$

Compared with the original MDI-QKD formulas, we found that MHPS bring at least one advantage: It is possible to obtain a higher value of the one-photon probability with MHPS owing to the post-selection procedure, which turns multi-detectors trigger event into one-photon output event by blocking the output of all the HS units but one with a certain probability.

3 Simulations

In the present section, we compare the performances of the SMHPS and AMHPS sources for different values of the number of HS units. The parameter μ, related to the number of generated pairs per pulse, is the free parameter used to numerically maximize the rate.

The measurement apparatus is characterized by detectors with quantum efficiency $\eta_c = 14.5\%$ and dark count probability $d_c = 3 \times 10^{-6}$, corresponding to the state-of-the-art semiconductor single-photon detectors. The optimal intensity of signal state with WCS is 0.5∼0.6, and the optimal intensity of signal state with MHPS is 0.2∼0.3. The efficiency of the error correction code is $f = 1.16$ and (a) $m = 2$ (b) $m = 8$

Table 2 List of experimental parameters for the measurement part

Ref. [27]	η_c	d_c	f	α
	14.5%	3×10^{-6}	1.16	0.21

Table 3 List of experimental parameters for Alice (Bob)

Ref. [24]	η	γ
	0.7	0.5

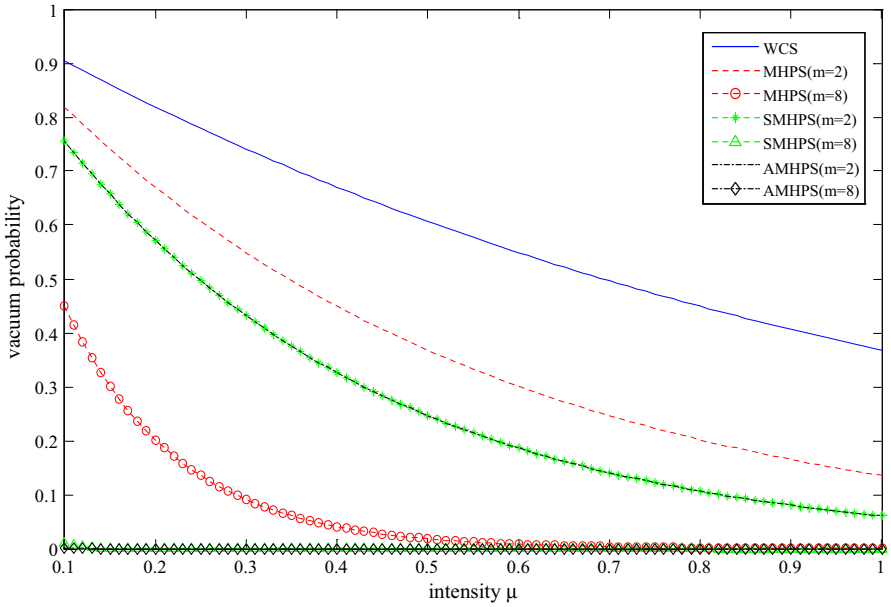

Fig. 3 A comparison for the probability of vacuum events between WCS, MHPS, SMHPS, and AMHPS

to illustrate the performance of different sources with different value m. The main parameters are listed in Tables 2 and 3:

The probability of vacuum events and single photon number distribution of the MHPS, SMHPS, and AMHPS are shown in Figs. 3 and 4, respectively. As shown in Fig. 3, the vacuum events of all three sources are decreasing rapidly when increasing the number m of the crystals. As shown in Fig. 4, when the detection efficiency and the transmissivity are fixed ($\eta = 0.7, \gamma = 0.5$), the single-photon performance does not always improve for SMHPS, while the AMHPS offers a better performance when the number of crystals is increased.

In Figs. 5 and 6, we compared the key generation rates of SMHPS and AMHPS with single-photon source and weak coherent source. The performance of the SMHPS and AMHPS are also compared for different values m. Both the key rate and the maximum secure transmittance distance of SMHPS and AMHPS are better than MDI-QKD with WCS owing to the use of parallel HS strategies, which not only suppresses the multi-

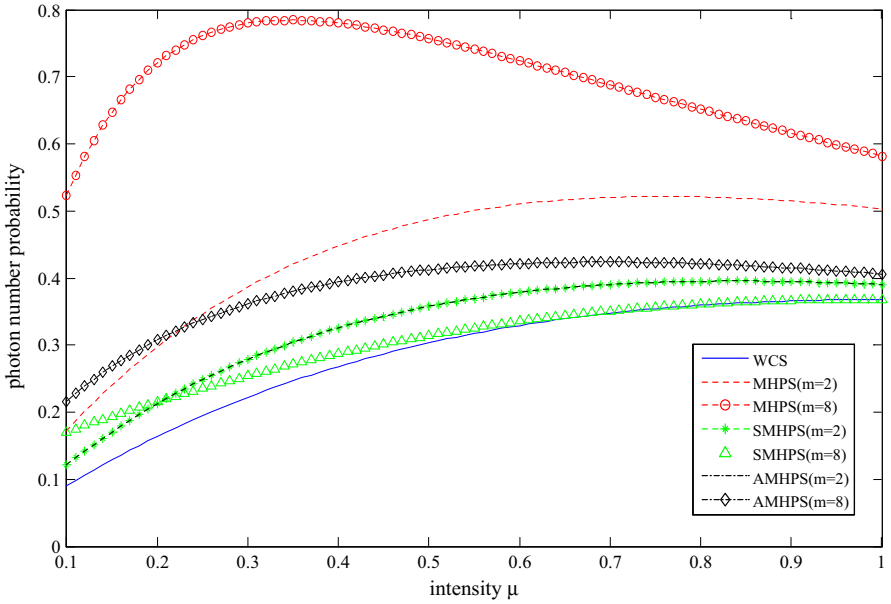

Fig. 4 A comparison for the probability of single-photon events between WCS, MHPS, SMHPS, and AMHPS

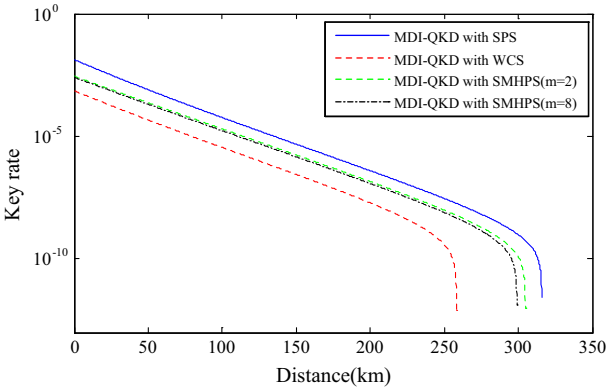

Fig. 5 Key rate R versus the maximal secure transmittance distance L with different sources. Blue solid line: MDI-QKD protocol using single-photon source. Red dash line: asymptotic MDI-QKD protocol with weak coherent source. Green dot line: our modified MDI-QKD protocol using SMHPS ($m = 2$) beams. Black dot-dashed line: our modified MDI-QKD protocol using SMHPS ($m = 8$) (Color figure online)

photons events, but also keeps an acceptable production rate of single photons. For $m = 2$, the performance of SMHPS and AMHPS are identical because the architecture of SMHPS and AMHPS are equivalent. When the number of crystals increases to $m = 8$, the maximal secure transmittance distance of SMHPS decreases owing to the effect of the increased absorption in optical switches. On the contrary, the AMHPS, which employs the same kind of binary switches but the different multiplex way,

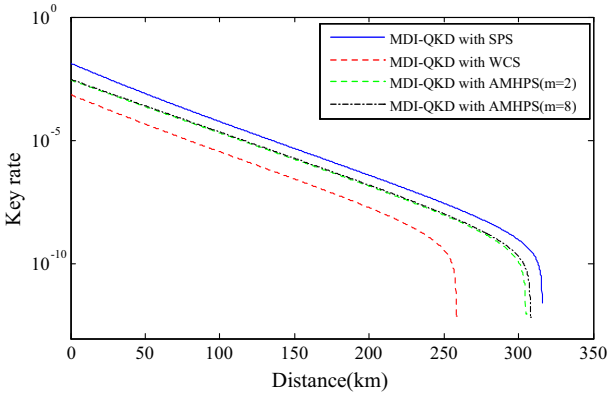

Fig. 6 Key rate R versus the maximal secure transmittance distance L with different sources. Blue solid line: MDI-QKD protocol using single-photon source. Red dash line: asymptotic MDI-QKD protocol with weak coherent source. Green dot line: our modified MDI-QKD protocol using AMHPS ($m = 2$) beams. Black dot-dashed line: our modified MDI-QKD protocol using AMHPS ($m = 8$) (Color figure online)

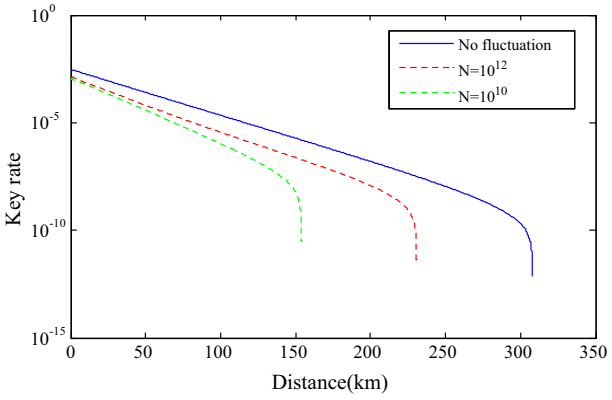

Fig. 7 Key rate R versus the maximal secure transmittance distance L with different key size for fixed m in MDI-QKD with SMHPS

shows improvement with eight HS units. The AMHPS shows better scalability than the SMHPS because the addition of HS units in SMHPS degrades the performance.

From Figs. 7 and 8, the performance varies heavily with different pulse numbers in MDI-QKD protocol with SMHPS and AMHPS, respectively. However, in the linear regime before the cutting-off, the scheme can work at the level close to the situation with no fluctuation. We should mention that, not as Curty et al.'s work, the statistical fluctuation analysis done in the manuscript is by far not a composable security proof, but it shows the overall trend of the behavior for different sources in the finite size regime.

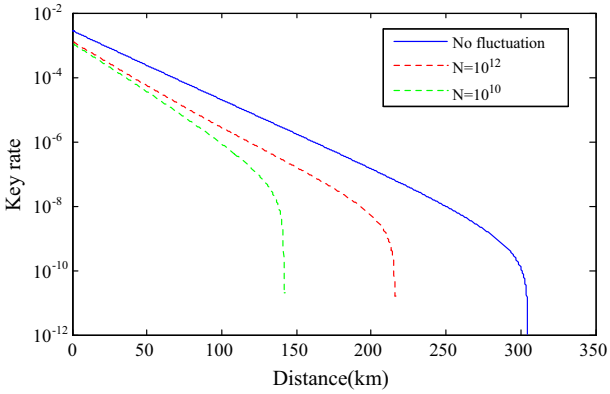

Fig. 8 Key rate R versus the maximal secure transmittance distance L with different key size for fixed $m = 4$ in MDI-QKD with AMHPS

4 Conclusion

In conclusion, we present a modified MDI-QKD with multiple crystal heralded single-photon sources. The symmetric scheme and asymmetric architectures are proposed to improve the single-photon character of the heralded source in MDI-QKD. The symmetric scheme is adopted to overcome the limitation of the current low efficiency of m-to-1 optical switches, while the asymmetric scheme is used to cope with the scalability issue with increasing the number of crystals suffered in symmetric scheme. MDI-QKD with multiple crystal heralded sources with post-selection has shown better performance than the original MDI-QKD protocol owing to the use of parallel HS strategies, which not only suppresses the multi-photons events, but also keeps an acceptable production rate of single photons. Furthermore, integrated devices represent the best resource to achieve high efficiency of the SPDC process and ensure good coupling into single mode fibers. [28] The recent advances in integrated photonics suggest an increasing role of multiple crystal heralded sources. If built into a single chip, they might be a valid alternative to lasers in quantum key distribution and other quantum information tasks requiring single photons to work properly.

Acknowledgements This work is supported by the National Natural Science Foundation of China (Grant No. 11704412).

References

1. Bennett, C.H., Brassard, G.; Quantum cryptography. In: Proceedings of the IEEE International Conference Computers, Systems and Signal Processing, pp. 175–179. IEEE, New York (1984)
2. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. **85**, 441–444 (2000)
3. Mayers, D.: Unconditional security in quantum cryptography. J. ACM **48**, 351–406 (2001)
4. Gottesman, D., Lo, H.K., Lutkenhaus, N., Preskill, J.: Security of quantum key distribution with imperfect devices. Quantum Inf. Comput. **4**, 325–360 (2004)

5. Brassard, G., Lutkenhaus, N., Mor, T., Sanders, B.C.: Limitations on practical quantum cryptography. Phys. Rev. Lett. **85**, 1330–1333 (2000)
6. Sun, S.H., Liang, L.M.: Experimental demonstration of an active phase randomization and monitor module for quantum key distribution. Appl. Phys. Lett. **101**, 071107 (2012)
7. Makarov, V., Skaar, J.: Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols. Quantum Inf. Comput. **86**, 0622–0635 (2008)
8. Qi, B., Zhao, Y., Ma, X.F., Lo, H.K., Qian, L.: Quantum key distribution with dual detectors. Phys. Rev. A: At. Mol. Opt. Phys. **75**, 052304 (2007)
9. Makarov, V.: Controlling passively-quenched single photon detectors by bright light. New J. Phys. **11**, 065003 (2009)
10. Lo, H.K., Curty, M., Qi, B.: Measurement-device-independent quantum key distribution. Phys. Rev. Lett. **108**, 130503 (2012)
11. 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 (2014)
12. Ferreira da Silva, T., Vitoreti, D., Xavier, G.B., do Amaral, G.C., Temporao, G.P., vonder Weid, J.P.: Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. Phys. Rev. A **88**, 052303 (2013)
13. Liu, Y., Chen, T.Y., Wang, L.J., Liang, H., Shentu, G.L., Wang, J., Cui, K., Yin, H.L., Liu, N.L., Li, L., et al.: Experimental measurement-device-independent quantum key distribution. Phys. Rev. Lett. **111**, 130502 (2013)
14. Tang, Z., Liao, Z., Xu, F., Qi, B., Qian, L., Lo, H.K.: Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. Phys. Rev. Lett. **112**, 190503 (2013)
15. Yin, H.L., et al.: Measurement-device-independent quantum key distribution over a 404 km optical fiber. Phys. Rev. Lett. **117**, 190501 (2016)
16. Adachi, Y., Yamamoto, T., Koashi, M., Imoto, N.: Simple and efficient quantum key distribution with parametric down-conversion. Phys. Rev. Lett. **99**, 180503 (2007)
17. Ma, X.F., Lo, H.K.: Quantum key distribution with triggering parametric down conversion sources. New J. Phys. **10**, 073018 (2008)
18. Brida, G., Degiovanni, I.P., Genovese, M., Piacentini, F., Traina, P., Della Frera, A., et al.:]An extremely low-noise heralded single-photon source: a breakthrough for quantum technologies. Appl. Phys. Lett. **101**, 221112 (2012)
19. 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)
20. Zhou, C., Bao, W.S., Chen, W., Li, H.W., Yin, Z.-Q., Wang, Y., Han, Z.F.: Phase-encoded measurement device independent quantum key distribution with practical spontaneous parametric-down-conversion sources. Phys. Rev. A **88**, 052333 (2013)
21. Migdall, A.L., Branning, D., Castelletto, S.: Tailoring single-photon and multiphoton probabilities of a single-photon on-demand source. Phys. Rev. A **66**, 053805 (2002)
22. Shapiro, J.H., Wong, F.N.: On-demand single-photon generation using a modular array of parametric downconverters with electro-optic polarization controls. Opt. Lett. **32**, 2698 (2007)
23. Mazzarella, L., Ticozzi, F., Sergienko, A.V., Vallone, G., Villoresi, P.: Asymmetric architecture for heralded single photon sources. Phys. Rev. A **88**, 023848 (2013)
24. Schiavon, M., Vallone, G., Ticozzi, F., Villoresi, P.: Heralded single-photon sources for quantum key distribution applications. Phys. Rev. A **93**, 012331 (2016)
25. Ma, X.F., Razavi, M.: Alternative schemes for measurement-device-independent quantum key distribution. Phys. Rev. A **86**, 062319 (2012)
26. 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)
27. Curty, M., Xu, F., Cui, W., Lim, C.C.W., Tamaki, K., Lo, H.-K.: Finite-key analysis for measurement-device-independent quantum key distribution. Nat. Commun. **5**, 3732 (2014)
28. Francis-Jones, R.J.A., Hoggarth, R.A., Mosley, P.J.: All-fibre multiplexed source of high-purity single photons. Optica **4**, 90–96 (2017)