


## Passive round-robin differential-quadrature-phase-shift quantum key distribution scheme with untrusted detectors

Hongwei Liu(刘宏伟), Wenxiu Qu(屈文秀), Tianqi Dou(窦天琦), Jipeng Wang(王吉鹏), Yong Zhang(张勇), Haiqiang Ma(马海强)

**Citation:**Chin. Phys. B . 2018, 27(10): 100309. **doi:** 10.1088/1674-1056/27/10/100309

Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

**What follows is a list of articles you may be interested in**

---

## Finite-size analysis of eight-state continuous-variable quantum key distribution with the linear optics cloning machine

Hang Zhang(张航), Yu Mao(毛宇), Duan Huang(黄端), Ying Guo(郭迎), Xiaodong Wu(吴晓东), Ling Zhang(张玲)

Chin. Phys. B . 2018, 27(9): 090307. **doi:** 10.1088/1674-1056/27/9/090307

## Controlling a sine wave gating single-photon detector by exploiting its filtering loophole

Lin-Xi Feng(冯林溪), Mu-Sheng Jiang(江木生), Wan-Su Bao(鲍皖苏), Hong-Wei Li(李宏伟), Chun Zhou(周淳), Yang Wang(汪洋)

Chin. Phys. B . 2018, 27(8): 080305. **doi:** 10.1088/1674-1056/27/8/080305

## Continuous-variable quantum key distribution based on continuous random basis choice

Weiqi Liu(刘维琪), Jinye Peng(彭进业), Peng Huang(黄鹏), Shiyu Wang(汪诗寓), Tao Wang(王涛), Guihua Zeng(曾贵华)

Chin. Phys. B . 2018, 27(7): 070305. **doi:** 10.1088/1674-1056/27/7/070305

## Practical security of continuous-variable quantum key distribution under finite-dimensional effect of multi-dimensional reconciliation

Yingming Zhou(周颖明), Xue-Qin Jiang(蒋学芹), Weiqi Liu(刘维琪), Tao Wang(王涛), Peng Huang(黄鹏), Guihua Zeng(曾贵华)

Chin. Phys. B . 2018, 27(5): 050301. **doi:** 10.1088/1674-1056/27/5/050301

## Improved quantum randomness amplification with finite number of untrusted devices based on a novel extractor

Ming-Feng Xu(徐明峰), Wei Pan(潘炜), Lian-Shan Yan(闫连山), Bin Luo(罗斌), Xi-Hua Zou(邹喜华), Peng-Hua Mu(穆鹏华), Li-Yue Zhang(张力月)

Chin. Phys. B . 2018, 27(1): 010305. **doi:** 10.1088/1674-1056/27/1/010305

---

# Passive round-robin differential-quadrature-phase-shift quantum key distribution scheme with untrusted detectors*

Hongwei Liu(刘宏伟), Wenxiu Qu(屈文秀), Tianqi Dou(窦天琦), Jipeng Wang(王吉鹏), Yong Zhang(张勇), and Haiqiang Ma(马海强)†

*School of Science, State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China*

(Received 13 June 2018; revised manuscript received 27 July 2018; published online 27 September 2018)

In this paper, we proposed the scheme for a passive round-robin differential-phase-shift quantum key distribution (RRDPS-QKD) set-up based on the principle of Hong–Ou–Mandel interference. Our scheme requires two legitimate parties to prepare their signal state with two different non-orthogonal bases instead of single in original protocol. Incorporating this characteristic, we establish the level of security of our protocol under the intercept-resend attack and demonstrate its detector-flaw-immune feature. Furthermore, we show that our scheme not only inherits the merit of better tolerance of bit errors and finite-sized-key effects but can be implemented using hardware similar to the measurement device independent QKD (MDI-QKD). This ensures good compatibility with the current commonly used quantum system.

**Keywords:** quantum key distribution, round-robin-differential-phase-shift, untrusted detector

**PACS:** 03.67.Dd, 03.67.Hk **DOI:** 10.1088/1674-1056/27/10/100309

## 1. Introduction

Quantum key distribution (QKD) systems facilitate two legitimate parties (commonly named Alice and Bob) to share their security keys in an information-theoretic secure way. Since the conception of first such protocol, i.e., Bennett–Brassard 1984 algorithm (BB84),[1] QKD has attracted significant attention worldwide, following which, many similar protocols and experiments have been presented.[2–13] However, these protocols inherently rely on the original version of the Heisenberg uncertainty principle, which dictates that greater the amount of information obtained by Eve, higher would be the disturbance caused by her on the signal.[14–17] The amount of leaked key information, which is quantified by the phase error $e_{\rm ph}$, can be deduced from the channel disturbance, which in turn is quantified by the bit error $e_{\rm bit}$. However, this leads to a fundamental limitation on the error rate existing in the conventional QKD protocol. For example, in the BB84 protocol equipped with strong symmetries, the phase error rate can be estimated by the bit error rate, i.e., $e_{\rm ph} = e_{\rm bit}$. In the extreme case, where the bit flip error $e_{\rm bit} \geq 11\%$, no secure key can be generated. In other protocols, normally there exists a relationship between the two error rates, as a result upper bounds of error rate thresholds generally exist.[18] This enforces a stringent requirement on the environment of the system, rendering certain issues of practical implementation challenging.

Recently, a new approach known as the round-robin differential-phase-shift (RRDPS) QKD[19] and its alternative scheme[20,21] was proposed. The costs of privacy amplification of this protocol is estimated without any monitoring, but depends exclusively on the state prepared by Alice, such as the number of $L$ sequential pulses and photons ($N$) in the $L$-pulse signal. This distinctive property causes the protocol to have a better tolerance against bit errors and finite-length effects. In theory, by maintaining a large enough value of $L$, the scheme can tolerate up to 50% of bit error rate. However, the realistic experimental apparatus, which is not strictly ideal, poses a serious and non-trivial threat to the security of these protocols, as eavesdropper (denoted Eve) may exploit loopholes caused by imperfections in the apparatus. Recently, it has been proved, that RRDPS-QKD protocol is vulnerable when equipped with practical detectors,[22,23] own to the differences between the theoretical and practical models. Here, we present a new RRDQPS-QKD scheme, in which Alice and Bob prepare their own state by using $X$ or $Y$ basis independently, following which Bob uses Hong–Ou–Mandel (HOM) type interference set-up to read the detected events with time slots, and subsequently broadcasts this information to Alice. Finally, they can calculate the secure key by using this detected information. Since the clicks of detectors are publicly announced, our scheme is immune to all attacks against detectors. However, it cannot exclude all security assumptions about the measurement device, because the original protocol theoretically requires that Bob can arbitrarily choose between an actual or alternative measurement processing.

*Project supported by the Fund from the State Key Laboratory of Information Photonics and Optical Communications (Beijing University of Posts and Telecommunications) (Grant No. IPOC2017ZT0).

†Corresponding author. E-mail: hqma@bupt.edu.cn

© 2018 Chinese Physical Society and IOP Publishing Ltd 

## 2. Apparatus setup and protocol

In the following paragraphs, we describe a setup of our scheme as depicted in Fig. 1. Alice and Bob independently prepare a block-wise phase random optical pulse train consisting of $L$ pulses, which are strongly attenuated to a value less than one photon per pulse on average, and successively pass through an asymmetric Mach–Zehnder interferometer (AMZI), whose role is to perform time-bin encoding with $X$ or $Y$ basis. Let us consider a simple case when both Alice and Bob have exactly one photon in their $L$-pulse block. The states of Alice and Bob can be represented as follows:

$$|\psi\rangle_p = \frac{\mathrm{e}^{\mathrm{i}\delta_p}}{\sqrt{2L}} \sum_{i=1}^{L} \left( p_{i,r}^{\dagger} + \mathrm{e}^{\mathrm{i}\phi_{\mathrm{pi}}} p_{i,s}^{\dagger} \right) |0\rangle = \frac{\mathrm{e}^{\mathrm{i}\delta_p}}{\sqrt{2L}} \sum_{i=1}^{L} \left( p_{i,r}^{\dagger} + \mathrm{i}^{a_{\mathrm{pi}}} (-1)^{s_{\mathrm{pi}}} p_{i,s}^{\dagger} \right) |0\rangle , \tag{1}$$

where $\delta_p$ is a common random phase shift of all the pulses in a block; $p$ represents a legitimate party, i.e., Alice or Bob; $\phi_{\mathrm{pi}} = (\pi/2)a_{\mathrm{pi}} + \pi s_{\mathrm{pi}}$ is the relative phase between the signal state $|s\rangle$ and reference state $|r\rangle$ of the $i$-th pulse; $p_{i,r}^{\dagger}$ and $p_{i,s}^{\dagger}$ represent the creation operator of reference's and signal's $i$-th position, respectively, as shown in Fig. 1; $a_{\mathrm{pi}} \in \{0,1\}$ represents the as chosen of $X$ or $Y$ basis for the $i$-th pulse and $s_{\mathrm{pi}} \in \{0,1\}$ denotes the random bit value of the $i$-th pulse. Hence, the relative phase of two time-bin on the $X$ and $Y$ basis are $\phi_{\mathrm{pi}X} \in \{0,\pi\}$ and $\phi_{\mathrm{pi}Y} \in \{\pi/2, 3\pi/2\}$, respectively.

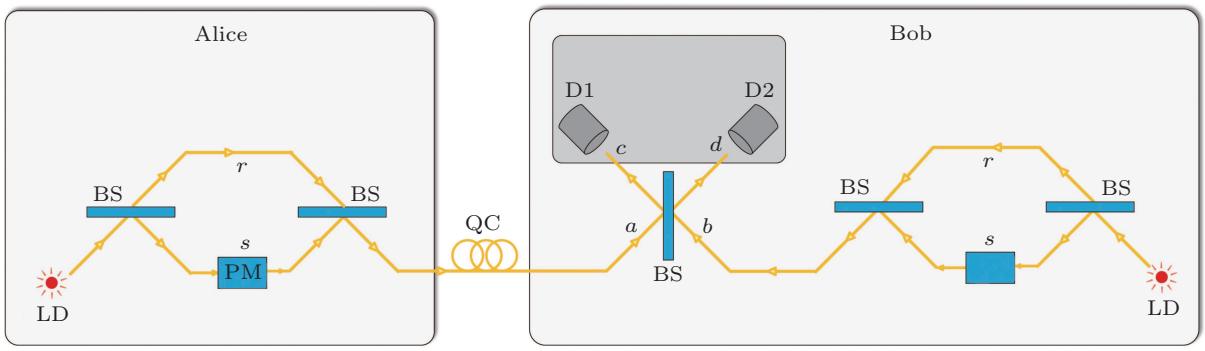



**Fig. 1.** (color online) Passive RRDQPS-QKD scheme. Alice and Bob use a local laser to generate a train of L-pulse independently, which are then encoded onto relative phases of two time-bin $r$ and $s$ by a phase modulator (PM), Bob records the coincidence clicks. LD: laser diode; BS: a 50/50 beam splitter; PM: phase modulator; QC: quantum channel; D1 and D2 in gray box means these two detectors are untrusted.

Since Alice and Bob can share a secure key successfully only when they use identical bases to encode corresponding state, we consider only the situation when $X$ basis is chose for simplicity, i.e., $a_{ai} = a_{bj} = 0$. The common random phase $\delta_p$ cannot influence the response of detectors, so this item is omitted from the following discussion. After the interference caused by the beam splitter (BS), which replaces $a_{i,r(s)}^{\dagger}$ and $b_{i,r(s)}^{\dagger}$ by

$$\frac{c_{i,r(s)}^{\dagger} + d_{i,r(s)}^{\dagger}}{\sqrt{2}}, \frac{c_{i,r(s)}^{\dagger} - d_{i,r(s)}^{\dagger}}{\sqrt{2}}, \tag{2}$$

respectively, where $c_{i,r(s)}^{\dagger}$ and $d_{i,r(s)}^{\dagger}$ are the creation operators at the two detectors, the outcome becomes

$$\begin{aligned}
&\frac{1}{\sqrt{2L}} \sum_{i=1}^{L} \left( a_{i,r}^{\dagger} + (-1)^{s_{ai}} a_{i,s}^{\dagger} \right) \otimes \frac{1}{\sqrt{2L}} \sum_{i=1}^{L} \left( b_{i,r}^{\dagger} + (-1)^{s_{bi}} b_{i,s}^{\dagger} \right) \\
&= \frac{1}{2\sqrt{L}} \sum_{i=1}^{L} \left( c_{i,r}^{\dagger} + d_{i,r}^{\dagger} + (-1)^{s_{ai}} \left( c_{i,s}^{\dagger} + d_{i,s}^{\dagger} \right) \right) \otimes \frac{1}{2\sqrt{L}} \sum_{i=1}^{L} \left( c_{i,r}^{\dagger} - d_{i,r}^{\dagger} + (-1)^{s_{bi}} \left( c_{i,s}^{\dagger} - d_{i,s}^{\dagger} \right) \right) \\
&= \frac{1}{4L} \sum_{i=1}^{L} \left[ \begin{array}{l} \left( c_{i,r}^{\dagger} c_{i,r}^{\dagger} - d_{i,r}^{\dagger} d_{i,r}^{\dagger} \right) + (-1)^{s_{ai}+s_{bi}} \left( c_{i,s}^{\dagger} c_{i,s}^{\dagger} - d_{i,s}^{\dagger} d_{i,s}^{\dagger} \right) \\ + \left( (-1)^{s_{ai}} + (-1)^{s_{bi}} \right) \left( c_{i,r}^{\dagger} c_{i,s}^{\dagger} - d_{i,r}^{\dagger} d_{i,s}^{\dagger} \right) + \left( (-1)^{s_{ai}} - (-1)^{s_{bi}} \right) \left( c_{i,r}^{\dagger} d_{i,s}^{\dagger} - d_{i,r}^{\dagger} c_{i,s}^{\dagger} \right) \end{array} \right] \\
&\quad + \frac{1}{4L} \sum_{1 \le i < j \le L} \left[ \begin{array}{l} 2 \left( c_{i,r}^{\dagger} c_{j,r}^{\dagger} - d_{i,r}^{\dagger} d_{j,r}^{\dagger} \right) + \left( (-1)^{s_{ai}+s_{bj}} + (-1)^{s_{bi}+s_{aj}} \right) \left( c_{i,s}^{\dagger} c_{j,s}^{\dagger} - d_{i,s}^{\dagger} d_{j,s}^{\dagger} \right) \\ + \left( (-1)^{s_{aj}} + (-1)^{s_{bj}} \right) \left( c_{i,r}^{\dagger} c_{j,s}^{\dagger} - d_{i,r}^{\dagger} d_{j,s}^{\dagger} \right) + \left( (-1)^{s_{ai}} + (-1)^{s_{bi}} \right) \left( c_{i,s}^{\dagger} c_{j,r}^{\dagger} - d_{i,s}^{\dagger} d_{j,r}^{\dagger} \right) \end{array} \right] \\
&\quad + \frac{1}{4L} \sum_{1 \le i < j \le L} \left[ \begin{array}{l} \left( (-1)^{s_{aj}} - (-1)^{s_{bj}} \right) \left( c_{i,r}^{\dagger} d_{j,s}^{\dagger} - d_{i,r}^{\dagger} c_{j,s}^{\dagger} \right) + \left( (-1)^{s_{ai}} - (-1)^{s_{bi}} \right) \left( c_{j,r}^{\dagger} d_{i,s}^{\dagger} - d_{j,r}^{\dagger} c_{i,s}^{\dagger} \right) \\ + \left( (-1)^{s_{bi}+s_{aj}} - (-1)^{s_{ai}+s_{bj}} \right) \left( c_{i,s}^{\dagger} d_{j,s}^{\dagger} - d_{i,s}^{\dagger} c_{j,s}^{\dagger} \right) \end{array} \right].
\end{aligned} \tag{3}$$

From Eq. (3), we can see that Bob counts photons occasionally and randomly and records the values as a function of time. Since there are two photons in a block, one from Alice and one from Bob, Bob would obtain at the most two detection clicks. He postselects to choose the block which corresponds to exactly two detections and announces his choice of basis, detection results, and positions $i$ and $j$ corresponding to time-bins $r$ or $s$. However, if $i=j$ or Bob's basis choice mismatched with Alice's, the results will be discarded. Hence, after the interference and Bob's postselection, the quantum state at the two detectors becomes one of the following

$$\begin{aligned}
&\left[1+(-1)^{s_{aj}+s_{bj}}\right]c^{\dagger}_{i,r}c^{\dagger}_{j,s}|0\rangle,\quad \left[1+(-1)^{s_{aj}+s_{bj}}\right]d^{\dagger}_{i,r}d^{\dagger}_{j,s}|0\rangle,\\
&\left[1+(-1)^{s_{ai}+s_{bi}}\right]c^{\dagger}_{i,s}c^{\dagger}_{j,r}|0\rangle,\quad \left[1+(-1)^{s_{ai}+s_{bi}}\right]d^{\dagger}_{i,s}d^{\dagger}_{j,r}|0\rangle,\\
&\left[1-(-1)^{s_{aj}+s_{bj}}\right]c^{\dagger}_{i,r}d^{\dagger}_{j,s}|0\rangle,\quad \left[1-(-1)^{s_{aj}+s_{bj}}\right]d^{\dagger}_{i,r}c^{\dagger}_{j,s}|0\rangle,\\
&\left[1-(-1)^{s_{ai}+s_{bi}}\right]c^{\dagger}_{j,r}d^{\dagger}_{i,s}|0\rangle,\quad \left[1-(-1)^{s_{ai}+s_{bi}}\right]d^{\dagger}_{j,r}c^{\dagger}_{i,s}|0\rangle,\\
&\left[1+(-1)^{(s_{ai}+s_{aj})+(s_{bi}+s_{bi})}\right]c^{\dagger}_{i,s}c^{\dagger}_{j,s}|0\rangle,\\
&\left[1+(-1)^{(s_{ai}+s_{aj})+(s_{bi}+s_{bi})}\right]d^{\dagger}_{i,s}d^{\dagger}_{j,s}|0\rangle,\\
&\left[1-(-1)^{(s_{ai}+s_{aj})+(s_{bi}+s_{bi})}\right]c^{\dagger}_{i,s}d^{\dagger}_{j,s}|0\rangle,\\
&\left[1-(-1)^{(s_{ai}+s_{aj})+(s_{bi}+s_{bi})}\right]d^{\dagger}_{i,s}c^{\dagger}_{j,s}|0\rangle.
\end{aligned}\tag{4}$$

This means Alice and Bob can calculate their raw key by utilizing the following Table 1.

**Table 1.** Detector clicks corresponding to Alice's and Bob's raw key.

| $i$-th Time-bin | $j$-th Time-bin | Alice's key | Bob's key |
|---|---|---|---|
| $c(d)_i$ and $c(d)_j$ clicks: | | | |
| $r$ | $s$ | $s_{aj}$ | $s_{bj}$ |
| $s$ | $r$ | $s_{ai}$ | $s_{bi}$ |
| $s$ | $s$ | $s_{ai}\oplus s_{aj}$ | $s_{bi}\oplus s_{bj}$ |
| $c(d)_i$ and $d(c)_j$ clicks: | | | |
| $r$ | $s$ | $s_{aj}$ | $1\oplus s_{bj}$ |
| $s$ | $r$ | $s_{ai}$ | $1\oplus s_{bi}$ |
| $s$ | $s$ | $s_{ai}\oplus s_{aj}$ | $1\oplus s_{bi}\oplus s_{bj}$ |

## 3. Security analysis

### 3.1. The ideal single photon source setup

For performing the security analysis, we consider an alternative measurement model executed by Bob, as shown in Fig. 2. In this model, in the case of single-photon situation, Bob simply measures the location of the photon in the incoming train of $L$ pulses to determine one of the indices $i$, when the first photon is detected. The other indices represented by $j$ are passively determined by the position of the rest photon. In other words, Bob postselects the block where two clicks detect photons at positions $i$ and $j$, but owing to the indistinguishability of photons, it is difficult to tell whether the photon causing the click belongs to Alice or Bob. Suppose Bob's photon is at $i$, the $L-1$ possible positions of Bob's photon $i$ (excluding the position of Alice's photon $j$) have the same weight owing to the symmetry of all the pulses. This is equivalent to the procedure that Bob generates at a random bit $b$, and eventually the Random Number Generator (RNG) announces the value $r$, which determines the index $j$ using the relation $j=i+(-1)^b r\,(\mathrm{mod}\ L)$, as depicted in the original RRDPS-QKD protocol.[19]

We can prove this procedure to be equivalent to our protocol depicted in Fig. 1 in the context of the production of outcome $(i,j)$. An arbitrary single photon inputting to the interferometer from Alice (possibly corrupted by Eve) and Bob is represented as

$$\sum_{i=1}^{L}\gamma_{ai}a^{\dagger}_{i}\otimes\sum_{i=1}^{L}\gamma_{bi}b^{\dagger}_{i},\tag{5}$$

where $P(i)=|\gamma_i|^2$ is the probability that a photon is found in $i$-th time-stamp. After interfering at BS, it transforms into

$$\sum_{i,j}\left[\left(\gamma_{ai}\gamma_{bj}+\gamma_{aj}\gamma_{bi}\right)\left(c^{\dagger}_{i}c^{\dagger}_{j}-d^{\dagger}_{i}d^{\dagger}_{j}\right)+\left(\gamma_{aj}\gamma_{bi}-\gamma_{ai}\gamma_{bj}\right)\left(c^{\dagger}_{i}d^{\dagger}_{j}-d^{\dagger}_{i}c^{\dagger}_{j}\right)\right]|0\rangle.\tag{6}$$

Hence, the probability of outputting the $(i,j)$ pair is

$$\begin{aligned}
&\left|\gamma_{ai}\gamma_{bj}+\gamma_{aj}\gamma_{bi}\right|^2+\left|\gamma_{aj}\gamma_{bi}-\gamma_{ai}\gamma_{bj}\right|^2=2\left|\gamma_{ai}\gamma_{bj}\right|^2\\
&\quad+2\left|\gamma_{aj}\gamma_{bi}\right|^2,
\end{aligned}\tag{7}$$

where we have omitted the normalization for the sake of simplicity. Considering the indistinguishability of photons, Bob cannot tell whether the photon causing the click belongs to Alice or Bob. However, it is not difficult to confirm that a photon in the $i$-th input pulse fails to arrive at the valid timing with probability 1/2, and is paired with each of the other $(L-1)$ pulses with an equal probability of $1/[2(L-1)]$. General considerations, the probability of $(i,j)$ announced in Fig. 1 is

$$\Pr\{i,j\}=\frac{\left|\gamma_{ai}\gamma_{bj}\right|^2+\left|\gamma_{bi}\gamma_{aj}\right|^2}{2(L-1)}.\tag{8}$$

For the model in Fig. 2, it reveals whether the photon was originally located in the $i$-th or in the $j$-pulse. Hence, Bob can announce an ordered pair $(i,j)$, such that the first index $i$ always represents the detected position of the photon, and its probability for $i\neq j$ is given by

$$\Pr(i,j)=\frac{\left|\gamma_{ai}\gamma_{bj}\right|^2}{2(L-1)}.\tag{9}$$

If we regard the announced pair as an unordered pair, its statistics is identical to the pair corresponding to the one shown in Fig. 1. This is confirmed by the relation

$$\Pr\{i,j\} = \Pr(i,j) + \Pr(j,i) = \frac{|\gamma_{ai}\gamma_{bj}|^2}{2(L-1)} + \frac{|\gamma_{bi}\gamma_{aj}|^2}{2(L-1)}. \quad (10)$$

Hence, the equivalence between the two measurement methods shown in Fig. 1 and Fig. 2 is proved. In the alternative measurement in the original protocol,[19] the probability of detecting photons at $(i,j)$ is $(P(i)+P(j))/2(L-1)$, where $P(i) = |\gamma_i|^2$ and $P(j) = |\gamma_j|^2$, because the signal states are prepared by Alice. However, in our scheme discussed in this paper, Alice and Bob independently prepare their encoded states and the random delay $r = |i-j|$ is generated through a passive route. In principle, our protocol can be regarded as a scheme equivalent to the original one. Since Alice has emitted just one photon, most of the $L$ bits should be unknown to Eve, for values of $L$ corresponding to $L \gg 1$. In Fig. 2, Eve's intervention only affects the decision of the photon at index $i(j)$, and the other index $j(i)$ is chosen randomly from the rest of the $L-1$ bits. Thus, we may expect that Eve has little information on $s_{j(i)}$, and hence, on the different cases of $s_i \oplus s_j$ as listed in Table 1, $\oplus$ denotes binary addition. Thus, the phase error $e_{ph}$ can also be bounded by $1/(L-1)$. The two bases are used for the preparation of state, so the encoded states are non-orthogonal and Eve cannot fully decipher the transmitted signal. This characteristic will further enhance the security of our scheme.

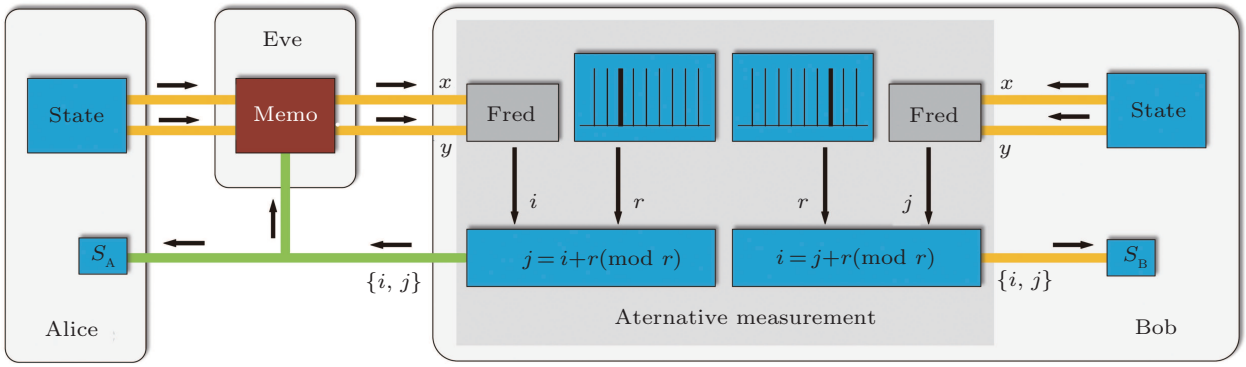



**Fig. 2.** (color online) Equivalent model of measurement. Bob obtains a click at position $i$ or $j$, and generates two random numbers $r \in \{1,\ldots,L-1\}$ and $b \in \{0,1\}$ to obtain $j = i+(-1)^b r$ or $i = j+(-1)^b r$, and publicly announces $i$ and $j$ to Alice.

To calculate the rate of secure key generation, we should know two important parameters, which is the bit and phase error rate, respectively. While the bit error rate can be obtained directly from the experiment, so we just need to estimate the phase error rate, which is used to quantify the information disclosed to Eve.

Moreover, we need to consider an entanglement-based virtual procedure performed by Alice, she encodes her signal state by preparing an $L$-pulse state $|\Psi\rangle$ and $L$ ancillary qubits $|0_Z\rangle = (1/\sqrt{2})(|0_X\rangle + |1_X\rangle)$, where $|\cdot_Z\rangle$ and $|\cdot_X\rangle$ represents the state prepared by $Z$ and $X$ basis respectively. The initial state prepared by Alice is represented as:

$$\begin{aligned}|\Psi\rangle_{\text{Alice}} &= 2^{-L/2}\prod_{k=1}^{L}\left(|0_X\rangle + (-1)^{\hat{n}_k}|1_X\rangle\right)|\Psi\rangle \\ &= 2^{-L/2}\sum_{\vec{s}\in\{0,1\}^L}\left(\prod_{k=1}^{L}|s_{Xk}\rangle_k(-1)^{s_{Xk}\hat{n}_k}\right)|\Psi\rangle, \quad (11)\end{aligned}$$

where $\vec{s} = (s_1, s_2 \ldots s_L)$, $|s_{Xk}\rangle$ is the $k$-th ancillary qubit, and $\hat{n}_k$ is the photon number operator which acts only on the $k$-th pulse. The density matrix of the initial state of Alice's ancillary qubit is $|0_Z\rangle\langle 0_Z|$. If Eve becomes aware of the result of this measurement, then this state becomes

$$\frac{1}{2}(|0_X\rangle\langle 0_X| + |1_X\rangle\langle 1_X|) = \frac{1}{2}(|0_Z\rangle\langle 0_Z| + |1_Z\rangle\langle 1_Z|). \quad (12)$$

Hence, the total phase error rate can be estimated by finding the $|1_Z\rangle$ states. According to Eq. (11), the state of the $k$-th qubit depends on the photon number corresponding to the $k$-th pulse. If and only if the photon number $n_k$ is odd, its state is $|1_Z\rangle$, and the corresponding number of odd-photon-number pulses in the $L$-pulse train is no larger than total the numbers of photon, $N$. Eve cannot determine Bob's state, and the other index $j$ is chosen randomly from the $(L-1)$ candidates according to the alternative measurement scheme presented in Fig. 2. If only one basis is used by Alice and Bob to prepare their states, the phase error rate can be bounded by $N/(L-1)$. However, in our scheme, there are two non-orthogonal bases, which are used to randomly prepare four states. Thus, if Eve performs a typical individual attack, i.e., intercept-resend attack, she will eavesdrop the key information with a probability of 1/2 at most, since the probability of basis matching between Alice and Eve is 1/2. For the security of our scheme, we pessimistically assume that Eve can get full of the information, when her basis is the same with that of Alice. Thus, the phase

error rate, when Eve performs intercept-resend attack, can be bounded by $N/2(L-1)$. If we only consider the photon distribution except in the $i$-th pulse corresponding to Bob's post-selection, a more strict bound on the total phase error rate can be derived according to the method discussed in a previously reported work.[20] It is represented as

$$\frac{1}{2}\times\frac{1-[(L-3)/(L-1)]^N}{2}, \tag{13}$$

where the one factor 1/2 is because the basis matching between Alice and Eve. It is noted that this phase error rate is also deduced in the case of intercept-resend attacks, and we will study its more strictly bound under the general attacks in the future works.

### 3.2. The weak coherence source setup

The security analysis above is based on an ideal single-photon source. However, most experimental implementations of QKD protocols are based on weak coherent sources that have photon statistics given by the Poisson distribution. It is well know that a weak coherent source with multiple decoy intensities can be used to overcome the photon-number-splitting (PNS) attack against the multiphoton pulses and achieve secret key rates similar to an ideal single-photon source.[24] It has been proved that the decoy technique can be applied to the RRDPS-QKD protocol,[25,26] we will develop our scheme based on the decoy state in the future work. Below we will estimate the information leaked to Eve caused by the multi-photon pulses.

Considering the weak-coherent-source scenario, we follow the method introduced in a previous report[20] since our works are based on the same model. In this scenario, multi-photon components may exist in both Alice and Bob's respective pulse trains. We assume that Bob randomly chooses two detected positions $i$ and $j$, when he receives two or more detector clicks in a block. To estimate the phase error rate, we consider the mean photon number of Alice's $L$-pulse train and Bob's $L$-pulse train to be both $v$, and set a proper mean photon number threshold $v_{\rm th}$ with a probability $\Pr(v>v_{\rm th})\le e_{\rm src}$, where $v_{\rm th}$ is an integer less than $v_{\rm th}<(L-1)/2$, and $e_{\rm src}$ is a constant. The phase error rate can be deduced when each of the following four cases for events corresponding to one detector click in each of the two pulses are considered separately.

(i) $v\le v_{\rm th}$, and two clicks are one from Alice and one from Bob;

(ii) $v\le v_{\rm th}$ and two clicks are both from Alice or both from Bob;

(iii) $v>v_{\rm th}$;

(iv) The event where at least one of the clicks is caused by more than one photon, in which case the first three cases are excluded.

The first case is mainly contributing to the final secure key, the phase error rate is equal to the one corresponding to the single-photon protocol. For the second case, without loss of generality, we assume that the two photons are both from Alice, then the response of detector will be

$$\begin{aligned}
&\frac{1}{\sqrt{2L}}\sum_{i=1}^{L}\left(a_{i,r}^{\dagger}+i^{a_{ai}}(-1)^{s_{ai}}a_{i,s}^{\dagger}\right)\otimes\frac{1}{\sqrt{2L}}\sum_{j=1}^{L}\left(a_{j,r}^{\dagger}+i^{a_{aj}}(-1)^{s_{aj}}a_{j,s}^{\dagger}\right)\\
&=\frac{1}{4L}\sum_{1\le i<j\le L}\left[\begin{array}{l}2\left(c_{i,r}^{\dagger}c_{j,r}^{\dagger}+d_{i,r}^{\dagger}d_{j,r}^{\dagger}\right)+2i^{a_{ai}+a_{aj}}(-1)^{s_{ai}+s_{aj}}\left(c_{i,s}^{\dagger}c_{j,s}^{\dagger}+d_{i,s}^{\dagger}d_{j,s}^{\dagger}\right)\\+2i^{a_{aj}}(-1)^{s_{aj}}\left(c_{i,r}^{\dagger}c_{j,s}^{\dagger}+d_{i,r}^{\dagger}d_{j,s}^{\dagger}\right)+2i^{a_{ai}}(-1)^{s_{ai}}\left(c_{i,s}^{\dagger}c_{j,r}^{\dagger}+d_{i,s}^{\dagger}d_{j,r}^{\dagger}\right)\end{array}\right]\\
&\quad+\frac{1}{4L}\sum_{1\le i<j\le L}\left[\begin{array}{l}2\left(c_{i,r}^{\dagger}d_{j,r}^{\dagger}+d_{i,r}^{\dagger}c_{j,r}^{\dagger}\right)+2i^{a_{aj}}(-1)^{s_{aj}}\left(c_{i,r}^{\dagger}d_{j,s}^{\dagger}+d_{i,r}^{\dagger}c_{j,s}^{\dagger}\right)\\+2i^{a_{ai}}(-1)^{s_{ai}}\left(c_{j,r}^{\dagger}d_{i,s}^{\dagger}+d_{j,r}^{\dagger}c_{i,s}^{\dagger}\right)+2i^{a_{ai}+a_{aj}}(-1)^{s_{ai}+s_{aj}}\left(c_{i,s}^{\dagger}d_{j,s}^{\dagger}+d_{i,s}^{\dagger}c_{j,s}^{\dagger}\right)\end{array}\right].
\end{aligned}\tag{14}$$

Evidently, the events for which the same detector clicks ($c_{i,}^{\dagger}c_{j,}^{\dagger}$ and $d_{i,}^{\dagger}d_{j,}^{\dagger}$) and different detectors clicks ($c_{i,}^{\dagger}d_{j,}^{\dagger}$ and $d_{i,}^{\dagger}c_{j,}^{\dagger}$) have the same amplitude exhibit the same probability. Hence, it will introduce 50% bit error regardless of Bob's encoding state. However, the corresponding value of phase error can be set to 0. The situation will be the same when we consider the case where the two participating photons are from Bob. In summary, this case will introduce only 25% total inherent bit error rate. When the mean photon number of Alice's and Bob's L-pulse train are assumed to be both $\mu$, the probability of the first and the second case has been proved to being the same.[20] Thus, under these two circumstances and considering the intercept-resend attacks, the phase error rate is

$$\frac{1-[(L-3)/(L-1)]^{v_{\rm th}}}{8}. \tag{15}$$

When the overall phase is randomized, it is shown that the state of the whole pulse train can be described by a statistical mixture of the Fock state, whose photon number follows a Poisson distribution.[27] Thus, in principle, Alice can tag each of the rounds with $v>v_{\rm th}$,[28] and we assume that this tagged

portion, at most $e_{\rm src}/Q$, is fully leaked to Eve, while $Q$ represents the overall gain. As for the fourth case, to present the worst estimate, we suppose that all these events also contribute to the maximal phase error. According to the fair sampling assumption, as deduced in Ref. [20], the probability of occurrence of this case is

$$\frac{m/M}{2(1-m/M)}, \tag{16}$$

where $m$ is the total number of photon counts of one detector, and $M$ is the total number of pulses. In summary, we can obtain the phase error rate under the weak-coherent-source scenario and is represented as

$$e_{\rm ph}^{\rm WCS} = \frac{e_{\rm src}}{Q} + \left(1-\frac{e_{\rm src}}{Q}\right)\frac{1-[(L-3)/(L-1)]^{\nu_{\rm th}}}{8} + \frac{m/M}{2(1-m/M)}. \tag{17}$$

The three additive terms in the phase error correspond to the probability of more than $\nu_{\rm th}$ photons, the probability of less than $\nu_{\rm th}$ photons, and the probability that two or more photons simultaneously enter the same detector at the same time stamp.

### 3.3. Untrusted detector

In the original protocol, it is assumed that Bob's detectors are independent of Eve, they cannot leak the information to Eve, and even be control by Eve. However, this assumption is unsustainable at the practical applications. When the weak coherence source is used, detectors may be controlled by Fred depicted in Fig. 2, and he can cooperate with Eve to announce the filtered $(i,j)$ pair,[22] whose corresponding detector click position has been predicted by Eve. Subsequently, she will know the relative phase differential between Alice's $i$-th and $j$-th pulse, and finally obtain the maximum information about the secure key. There is a more practical and efficient eavesdropping scheme proposed in Ref. [23], wherein Eve can launch the bright light into the detectors rendering them insensitive to photons,[29,30] and subsequently she can control the occurrence of detector click to obtain the entire information about the secure key based on her measurement results.

Our scheme can remove the assumptions on the detector, as required in the original protocol. The detectors in our scheme can be completely controlled by Eve, and the information of the clicks of detector is allowed to reveal to Eve. Thus, the detector parts can be regarded as a "Black Box" for Alice and Bob. As we can see, Eve's main purpose in the attacks showed above is to obtain the information about the click position of the detectors, i.e., in the attack scheme proposed in Ref. [22], Fred, who have controlled the detector's clicks, can announce a filtered $(i,j)$ pairs, which are known by Bob in advance. However, the specific detected results are also required to be published in our protocol. Since Eve may not know the encoding information of Bob's signal pulses, these attack schemes cannot work effectively in our protocol, where the secure key is generated according to the specific detector responses and the states are prepared by legitimated parties. Hence, our protocol can effectively immune to all attacks against the detector. Furthermore, the signal states are encoded with two non-orthogonal bases, and Eve cannot identify the transmitted signal entirely. This characteristic will further enhance the security of our scheme.

Actually, the model of our scheme is similar to that of the MDI-QKD protocol, Alice and Bob need prepare their states independently, and then encoded states are transmitted to the untrusted part, named Charlie. However, it is noted that the security of the original RRDPS-QKD protocol is ensured by the principle of information causality and complementarity, which suggests that Bob is required to switch the measurement procedures depicted between Fig. 1 and Fig. 2 arbitrarily, and thus, the measurement unit in our scheme may not fully be placed at an untrusted third party. Nevertheless, compared with the MDI-QKD, our scheme has a better tolerance against bit errors and finite-sized-key effects. Even though the detector-device-independent (DDI) scheme has been proved insecure for the type of the BB84 protocol,[30,31] our scheme, which can be treat as a DDI version for the RRDPS-QKD protocol, is still secure, since our scheme is based on the two photon interference, and only two simultaneous clicks can be treated as a successful Bell state measurement. Whereas, the original DDI-QKD protocol is based on the two-qubit single photon, and the successful Bell state measurement is extracted from single click.

## 4. Secure key generation rates

In order to examine the performance of our scheme, we calculated the secure key generation rate based on the following model and the parameter for simulation[32] listed in Table 2. From the Gottesman–Lo–Lutkenhaus–Preskill (GLLP) formula,[28] we obtain an asymptotic formula for secure key rate per pulse

$$R = \frac{1}{2L}\left\{Q - Qfh(e_{\rm bit}) - \left\{e_{\rm src} + (Q-e_{\rm src})h\left\{\frac{1-[(L-3)/(L-1)]^{\nu_{\rm th}}}{8}\right\} + Q\frac{m/M}{2(1-m/M)}\right\}\right\}, \tag{18}$$

where $f$ is the parameter related to the efficiency of the employed error correction code, and $h(x)$ is the binary Shannon entropy function defined as $h(x) = -x\log_2(x) - (x-1)\log_2(x-1)$. In the infinite data size limit, $m = \eta\mu M$, where $\mu$ is the mean photon number per pulse, $\eta$ represents the overall transmittance of the system and can be calculated by $\eta = \eta_c\eta_d$, $\eta_d$ is the detector efficiency, $\eta_c = 10^{-(\alpha D/10)}$ the transmittance of the quantum channel, $D$ the transmission distance, and $\alpha$ represents the loss coefficient of the channel measured in units dB/km. Since, Alice's and Bob's basis choice has 50% probability of mismatch, it leads to the factor 1/2 in Eq. (18). In the weak-coherent-source scenario, $Q$ and $e_{\rm src}$ is written as

$$Q = \left(\frac{L\eta\mu}{2}\right)^2 \exp(-L\eta\mu), \tag{19}$$

$$e_{\rm src} = 1 - \exp(-L\mu)\sum_{v=0}^{v_{\rm th}} \frac{(L\mu)^v}{v!}. \tag{20}$$

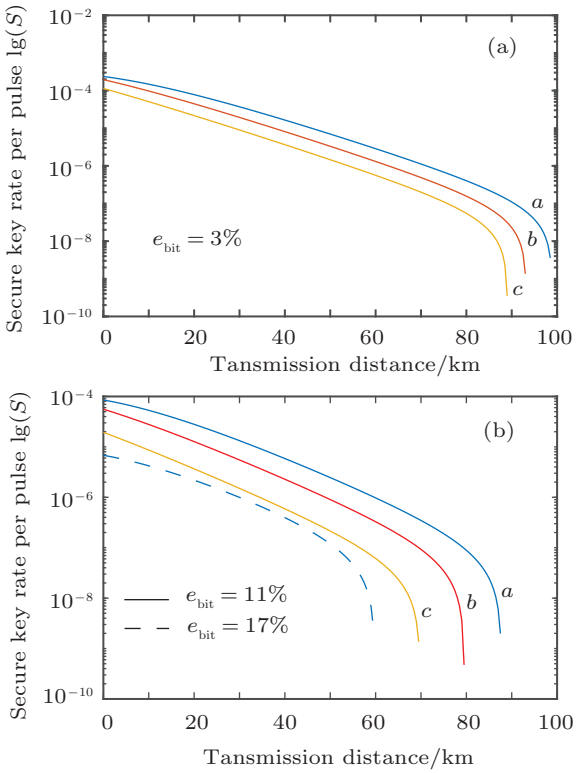



**Fig. 3.** (color online) Key rates versus transmission distance. (a) The rates for $e_{\rm bit} = 3\%$; (b) The rates for $e_{\rm bit} = 11\%$ (solid line)and $e_{\rm bit} = 17\%$ (dashed line). Lines labelled $a$–$c$ represent the proposed protocol with $L$=128, 64, and 32, dashed line in panel (b) is the result when $L$=128.

In Fig. 3, we depict the plot of the key rate per pulse versus transmission distance for $L$=128, 64, and 32 respectively. For simplicity, we assume that the dark counting is negligible and there exists a constant bit error rate of 3%, 11%, and 17% for the sake of comparison. In the case of simulation, where the mean photon number per pulse $\mu$ is set to a constant value of 0.05, the value of the $v_{\rm th}$ photon is optimized to 21, 15, and 11 for $L$=128, 64, and 32 respectively. Since no positive secure key rate is produced for $L$ =64 and 32 when $e_{\rm bit} = 17\%$, this situation is not represented in Fig. 2(b). When $L$=128 and $e_{\rm bit} = 17\%$, the simulation result shows that our protocol can still cover over 60km transmission distance, while the conventional BB84 protocol can maximally tolerate 11% error rate based on Shor–Preskill security proof.[15] This means that when $e_{\rm bit} > 11\%$, no secure key can be generated. It is noted that these values are just partially optimized, $\mu$ and $v_{\rm th}$ is actually all that is needed to be optimized for a different transmission distance in a practical system as executed in the previously reported works.[20,32–34] We believe our scheme will exhibit improved bit error tolerance and cover longer transmission distance when a full optimization method is adopted in the future work.

**Table 2.** Key parameters for simulation.[32]

| $\mu$ | $\eta_d$ | $f$ | $\beta$(dB/km) |
|---|---|---|---|
| 0.05 | 19% | 1.16 | 0.2 |

## 5. Discussions and conclusion

So far, we have described a new passive RRDPQS protocol with untrusted detectors. According to simulation results, our protocol can cover over 60-km transmission distance when the error rate $e_{\rm bit} > 17\%$, while no secure key can be generated under such a high bit error rate for a conventional BB84 protocol. Since the random delay $r = |j-i|$ is passively generated in our scheme, the parameter $L$ can be decided during the postprocessing step, which has an advantage in the case with large fluctuations in the environment. However, the pulse train length $L$ in original scheme needs to be optimized before performing the experiment, which requires a precise calibration system. Furthermore, two non-orthogonal bases for encoding are used to enhance the security of our protocol. Thus, our scheme is more efficient and secure compared to the original RRDPS-QKD protocol. We note that our analysis is limited to the case when Eve performs the intercept-resend attack; it remains to be prove the more strictly bound of phase error rate under the general attack in the future works. In this simulation, the parameter is partially optimized, and we believe our scheme will exhibit a better performance when a full parameter optimization is considered in the future work.

The Decoy state technique has been recently studied in RRDPS-QKD protocol,[25,26] and the error rate is considered to improve the rate of secure key generation for a small value of $L$.[35,36] It will be an interesting exercise to combine these novel works to test the performance of proposed scheme under a more practical situation. It is noted that a MDI-RRDPS-QKD has been proposed by Chau *et al.*[37] However, their protocol required photon number resolving detectors, it is infeasible with current technology. We believe our scheme will

contribute significantly to the formulation of a feasible MDI version of RRDPS-QKD and its practical applications. Furthermore, our scheme can be implemented with a hardware similar to the MDI-QKD, ensuring good compatibility with the current quantum system.

## References


[1] Bennett C H, Brassard G 1984 *Proceedings ofIEEE International Conference on Computers, Systems, and Signal Processing* pp. 175–99
[2] Yang X Q, Wei K J, Ma H Q, Sun S H, Liu H W, Yin Z Q, Li Z H, Lian S B, Du Y G and Wu L A 2016 *Phys. Rev. A* **93** 052303
[3] Liu H W, Ma H Q, Wei K J, Yang X Q, Qu W X, Dou T Q, Chen Y T, Li R X and Zhu W 2016 *Phys. Lett. A* **380** 2349
[4] Wei K J, Ma H Q and Yang J H 2013 *Opt. Express* **21** 16663
[5] Ma H Q, Wei K J and Yang J H 2013 *Opt. Lett.* **38** 4494
[6] Tang G Z, Sun S H, Chen H, Li C Y, and Liang L M 2016 *Chin. Phys. Lett.* **33** 120301
[7] Liu C Q, Zhu C H, Wang L H, Zhang L X and Pei C X 2016 *Chin. Phys. Lett.* **33** 100301
[8] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[9] Inoue K, Waks E and Yamamoto Y 2002 *Phys. Rev. Lett.* **89** 037902
[10] Hatakeyama A, Mizutani A, Kato G, Imoto N and Tamaki K 2017 *Phys. Rev. A* **95** 042301
[11] Inoue K and Iwai Y 2009 *Phys. Rev. A* **79** 022319
[12] Stucki D, Brunner N, Gisin N, Scarani V and Zbinden H 2005 *Appl. Phys. Lett.* **87** 194108
[13] Stucki D, Walenta N, Vannel F, Thew R T, Gisin N, Zbinden H, Gray S, Towery C R and Ten S 2009 *New. J. Phys.* **11** 075003
[14] Lo H K and Chua H F 1999 *Science* **283** 2050
[15] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[16] Moroder T, Curty M, Lim C C W, Thinh L P, Zbinden H and Gisin N 2012 *Phys. Rev. Lett.* **109** 260501
[17] Kawakami S, Sasaki T and Koashi M 2016 *Phys. Rev. A* **94** 022332
[18] Curty M, Lewenstein M and Lütkenhaus N 2004 *Phys. Rev. Lett.* **92** 217903
[19] Sasaki T, Yamamoto Y and Koashi M 2014 *Nature* **509** 475
[20] Guan J Y, Cao Z, Liu Y, Shen Tu G L, Pelc J S, Fejer M M, Peng C Z, Ma X F, Zhang Q and Pan J W 2015 *Phys. Rev. Lett.* **114** 180502
[21] Zhou C, Zhang Y Y, Bao W S, Li H W, Wang Y, Peng and Jiang M S 2017 *Chin. Phys. B* **26** 020303
[22] Cao Z, Yin Z Q and Han Z F 2016 *Phys. Rev. A* **93** 022310
[23] Iwakoshi T 2015 *Proc. SPIE* **9505** 950504
[24] Jiao R Z, Zhang C and Ma H Q 2011 *Acta Phys. Sin.* **60** 110303 (in Chinese)
[25] Zhang Y Y, Bao W S, Zhou C, Li H W, Wang Y and Jiang M S 2017 *Chin. Phys. Lett.* **34** 040301
[26] Liu L, Guo F Z, Qin S J and Wen Q Y 2017 *Sci. Rep.* **7** 42261
[27] Lo H K, Lo H K and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[28] Gottesman D, Ma X F, Lütkenhaus N and Preskill J 2004 *Quantum Inform. Comput.* **4** 325
[29] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 *Nat. Photon.* **4** 686
[30] Wei K J, Liu H W, Ma H Q, Yang X Q, Zhang Y, Sun Y M, Xiao J H and Ji Y F 2017 *Sci. Rep.* **7** 449
[31] Lim C C W, Korzh B, Martin A, Bussieres F, Thew R and Zbinden H 2014 *Appl. Phys. Lett.* **105** 221112
[32] Takesue H, Sasaki T, Tamaki K and Koashi M 2015 *Nat. Photon.* **9** 827
[33] Wang S, Yin Z Q, Chen W, He D Y, Song X T, Li H W, Zhang L J, Zhou Z, Guo G C and Han Z F 2015 *Nat. Photon.* **9** 832
[34] Li Y H, Cao Y, Dai H, Lin J, Zhang Z, Chen W, Xu Y, Guan J Y, Liao S K, Yin J, Zhang Q, Ma X F, Peng C Z and Pan J W 2016 *Phys. Rev. A* **93** 030302
[35] Toshihiko S and Masato K 2017 *Quantum Sci. Technol.* **2** 024006
[36] Yin Z Q, Wang S, Chen W, Han Y G, Wang R, Guo G C and Han Z F 2018 *Nat. Commun.* **9** 457
[37] Chau H F, Wong C, Wang Q N and Huang T Q 2016 arXiv: 1608.08329v1 [quant-ph]