

# Passive Decoy-State Reference-Frame-Independent Quantum Key Distribution with Heralded Single-Photon Source \*

Jia-Ji Li(李家骥)<sup>1,2</sup>, Yang Wang(汪洋)<sup>1,2</sup>, Hong-Wei Li(李宏伟)<sup>1,2</sup>, Peng Peng(彭朋)<sup>1,2</sup>, Chun Zhou(周淳)<sup>1,2</sup>, Mu-Sheng Jiang(江木生)<sup>1,2</sup>, Hong-Xin Ma(马鸿鑫)<sup>1,2</sup>, Lin-Xi Feng(冯林溪)<sup>1,2</sup>, Wan-Su Bao(鲍皖苏)<sup>1,2\*\*</sup>

<sup>1</sup>Henan Key Laboratory of Quantum Information and Cryptography, Zhengzhou Information Science and Technology Institute, Zhengzhou 450001

<sup>2</sup>Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026

(Received 6 September 2017)

*Reference-frame-independent (RFI) quantum key distribution (QKD) is a protocol which can share unconditional secret keys between two remote users without the alignment of slowly varying reference frames. We propose a passive decoy-state RFI-QKD protocol with heralded single-photon source (HSPS) and present its security analysis. Compared with RFI QKD using a weak coherent pulse source (WCPS), numerical simulations show that the passive decoy-state RFI QKD with HSPS performs better not only in secret key rate but also in secure transmission distance. Moreover, our protocol is robust against the relative motion of the reference frames as well as RFI QKD with the WCPS. In addition, we also exploit Hoeffding's inequality to investigate the finite-key effect on the security of the protocol.*

PACS: 03.67.Dd, 03.67.Hk, 03.67.-a

DOI: 10.1088/0256-307X/34/12/120301

Quantum key distribution (QKD) can theoretically realize unconditional secure transmission of secret keys. Since BB84 protocol was proposed,<sup>[1]</sup> researchers have carried out a series of theoretical and experimental research.<sup>[2–5]</sup> In most QKD experimental realizations, the users need to share a reference frame. For example, the polarization state needs to be aligned in the polarization encoding system while the stability of the interference is also required in the phase encoding system. However, reference frames cannot be perfectly aligned in practical QKD systems. To solve this problem, Laing *et al.* proposed the reference-frame-independent (RFI) QKD,<sup>[6]</sup> which can overcome the alignment problem of the reference frame. In particular, it is suitable for satellite-based QKD and chip-to-chip QKD. Experiments for RFI QKD have been implemented in the telecom fiber<sup>[7]</sup> and the free space.<sup>[8]</sup>

Moreover, Liang *et al.*<sup>[9]</sup> have combined the decoy state method<sup>[10–12]</sup> with RFI QKD to resist the photon-number-splitting (PNS) attacks<sup>[13,14]</sup> and demonstrated a proof-of-principle experiment over an optical fiber. The security of decoy state RFI QKD with source flaws and the valid conditions of RFI QKD have also been presented, respectively.<sup>[15,16]</sup> By exploiting the idea of measurement device independence,<sup>[17]</sup> the reference-frame-independent measurement-device-independent (RFI-MDI) QKD has been presented to remove all side channel attacks of RFI QKD.<sup>[18]</sup> Subsequently, a proof-of-principle experiment of RFI-MDI QKD has been demonstrated.<sup>[19]</sup> Both the above demonstration and the practical security analysis<sup>[20]</sup> highlight the

practicality of decoy-state RFI QKD.

The active decoy-state method, which requires that Alice actively prepares decoy states, has been used in the above decoy-state RFI QKD. What is more, the passive decoy-state method, which only uses one-intensity signal, can be realized by heralded single-photon source (HSPS).<sup>[21–23]</sup> It can reduce the complexity of practical QKD systems and can avoid the leakage of side channel information in the decoy-state preparation procedure. In addition, QKD protocols with HSPS have better performance than common QKD protocols with a weak coherent pulse source (WCPS).<sup>[24,25]</sup> To improve the performance of RFI QKD, the passive decoy-state RFI QKD with HSPS is worthy of further study. In this study, the method to estimate Eve's information and the secret key rate for passive decoy state RFI QKD with HSPS are proposed. In the practical implementation, the keys could not be infinite, thus we should consider the protocol in finite-key scenarios. We also analyze the security of the protocol for the case with statistical fluctuations. Finally, we carry out numerical simulations to compare the performance of RFI QKD with two different sources and cases with different numbers of total pulses. In this work, our security analysis is against coherent attacks by an eavesdropper in the asymptotic case. When considering the protocol in finite-key scenarios, our security analysis is against collective attacks.

Firstly, we introduce the RFI QKD. In the ideal single photon source RFI QKD,  $|0\rangle$  and  $|1\rangle$  consist of the  $Z$  basis,  $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$  and  $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$  consist of the  $X$  basis, and  $|+i\rangle =$

\*Supported by the National Basic Research Program of China under Grant No 2013CB338002, and the National Natural Science Foundation of China under Grant Nos 61505261, 61675235, 61605248 and 11304397.

\*\*Corresponding author. Email: 2010thzz@sina.com

© 2017 Chinese Physical Society and IOP Publishing Ltd

$(|0\rangle + i|1\rangle)/\sqrt{2}$  and  $|-i\rangle = (|0\rangle - i|1\rangle)/\sqrt{2}$  consist of the  $Y$  basis. Alice randomly chooses one of the three groups of bases to encode and sends it to Bob. These three bases follow<sup>[6]</sup>

$$\begin{aligned} Z_A &= Z_B, \\ X_B &= X_A \cos \beta + Y_A \sin \beta, \\ Y_B &= Y_A \cos \beta - X_A \sin \beta, \end{aligned} \quad (1)$$

where  $Z_{A(B)}$ ,  $X_{A(B)}$  and  $Y_{A(B)}$  denote Alice's (Bob's) local reference frames in  $Z$ ,  $X$  and  $Y$  bases, and  $\beta$  is the angular deviation between two reference frames. When receiving the pulses, Bob randomly chooses one of the three bases to make measurement. Alice and Bob obtain secret keys from  $Z$  basis as it is unaffected by the reference frame deviation. After the appropriate number of rounds, they obtain the bit error rate for the  $Z_A Z_B$  basis,<sup>[6]</sup>

$$E_{ZZ} = \frac{1 - \langle Z_A Z_B \rangle}{2}, \quad (2)$$

where the subscripts  $i$  and  $j$  where  $i, j \in \{X, Y, Z\}$  denote that Alice sends a state in  $i$  basis while Bob measures it in  $j$  basis. The information of Eve is estimated by the measurement outcomes in  $X$  and  $Y$  bases. Eve's information can be estimated by a parameter  $C$  defined as<sup>[6]</sup>

$$C = \langle X_A X_B \rangle^2 + \langle X_A Y_B \rangle^2 + \langle Y_A X_B \rangle^2 + \langle Y_A Y_B \rangle^2. \quad (3)$$

Then Eve's information  $I_E$  can be estimated by

$$I_E = (1 - E_{ZZ})h\left(\frac{1 + v_{\max}}{2}\right) - E_{ZZ}h\left(\frac{1 + f(v_{\max})}{2}\right), \quad (4)$$

where

$$\begin{aligned} v_{\max} &= \min[\sqrt{C/2}/(1 - E_{ZZ}), 1], \\ f(v_{\max}) &= \sqrt{C/2 - (1 - E_{ZZ})^2 v_{\max}^2 / E_{ZZ}}, \end{aligned} \quad (5)$$

and  $h(x) = -x \log_2(x) - (1 - x) \log_2(1 - x)$  is the Shannon entropy function. In a practical QKD system, usually  $E_{ZZ} \leq 15.9\%$ , thus the secret key rate is  $R = 1 - h(E_{ZZ}) - I_E$ .<sup>[9]</sup>

Then we will present the security of passive decoy-state RFI QKD with HSPS. HSPS can be produced by the spontaneous parametric down conversion (SPDC) process. HSPS produces two-mode states. When Alice measures one mode with a practical detector, the other mode can be divided into triggered pulses and nontriggered pulses according to the responses of the detector. Using the passive decoy state method, the triggered pulses and the nontriggered pulses are treated as signal states and decoy states, respectively. Then Alice and Bob obtain the gain of the triggered pulses and the nontriggered pulses  $Y_t, Y_{nt}$ , and the bit error rates of the triggered pulses and the nontriggered pulses under different bases  $E_{ij}^t, E_{ij}^{nt}$  ( $ij \in \{ZZ, XX, YY, XY, YX\}$ ), respectively. Here the superscript  $t$  represents the triggered pulse, and  $nt$  represents the nontriggered pulse.

The subscripts  $i$  and  $j$  denote that Alice sends a state in  $i$  basis while Bob measures it in  $j$  basis.

In the decoy state method,  $n$ -photon pulses are divided into triggered  $n$ -photon pulses and nontriggered  $n$ -photon pulses. The probability of generating  $n$ -photon pulses is  $p_n$ , the probability of generating triggered  $n$ -photon pulses is  $p_n^{(t)}$ , the probability of generating nontriggered  $n$ -photon pulses is  $p_n^{(nt)}$ , and  $\gamma_n$  is the probability of triggering when  $n$ -photons are emitted from the SPDC process, then

$$\begin{aligned} p_n^{(t)} &= p_n \gamma_n, \\ p_n^{(nt)} &= p_n (1 - \gamma_n), \\ p_n &= \frac{\mu^n}{(1 + \mu)^{n+1}}, \\ \gamma_n &= 1 - (1 - d_A)(1 - \eta_A)^n, \end{aligned} \quad (6)$$

where  $\mu$  denotes the intensity of HSPS,  $n$  is the photon number,  $d_A$  and  $\eta_A$  are the dark count rate and detection efficiency of Alice's detector, respectively. In the ideal case, we consider that the detection rate and bit error rate of the triggered photon pulses and nontriggered photon pulses are equal to

$$Y_n^{(t)} = Y_n^{(nt)}, \quad e_n^{(t)} = e_n^{(nt)}. \quad (7)$$

Then the counting probabilities for  $n$ -photon pulses can be written as

$$Q_n^{(t)} = Y_n^{(t)} p_n \gamma_n, \quad Q_n^{(nt)} = Y_n^{(nt)} p_n (1 - \gamma_n), \quad (8)$$

where  $Q_n^{(t)} = \delta_n Q_n^{(nt)}$  and  $\delta_n = \frac{\gamma_n}{1 - \gamma_n}$ . We can see that  $\delta_n$  has an increasing relationship with  $n$ . Then the counting rates of the triggered pulse and nontriggered pulse can be expressed as

$$\begin{aligned} Y_t &= \sum_{n=0}^{\infty} Q_n^{(t)} = \sum_{n=0}^{\infty} Y_n^{(t)} p_n \gamma_n, \\ Y_{nt} &= \sum_{n=0}^{\infty} Q_n^{(nt)} = \sum_{n=0}^{\infty} Y_n^{(nt)} p_n (1 - \gamma_n). \end{aligned} \quad (9)$$

We assume  $\delta = \frac{Y_t}{Y_{nt}}$ , and with these values, the lower bound of the single-photon contribution can be estimated as<sup>[26]</sup>

$$\begin{aligned} Q_1^{(nt)} &\geq \frac{(\delta_2 - \delta)Y_{nt} - (\delta_2 - \delta_0)Q_0^{(nt)}}{\delta_2 - \delta_1} = Q_1^{(nt)L}, \\ Q_1^{(t)L} &= \delta_1 Q_1^{(nt)L}. \end{aligned} \quad (10)$$

Then the challenge is to estimate the bit error rate under different bases. The bit error rate of  $n$ -photon state  $e_{n,ij}$  is given as<sup>[27]</sup>

$$e_{n,ij} = \frac{e_{ij} \eta_n + \frac{1}{2} d_B}{Y_n}, \quad (11)$$

where  $e_{ij}$ ,  $\eta_n$  and  $d_B$  denote the erroneous detection probability under  $i$  and  $j$  bases, the detection

efficiency of  $n$ -photon state and the dark count rate of Bob's detector, respectively. Here  $e_{ZZ} = \frac{1-P}{2}$ ,  $e_{XY} = e_{YX} = \frac{1}{2}$ ,  $e_{XX} = e_{YY} = \frac{1-P \cos \beta}{2}$ , where  $P$  represents the probability that the signal state is correctly measured, and  $\beta$  represents the deviation of the angle between two reference frames. Then we consider the bit error rates under  $Z$  basis of the triggered pulses and the nontriggered pulses, respectively,

$$\begin{aligned} E_{ZZ}^t &= \frac{1}{Y_t} \sum_{n=0}^{\infty} Q_n^{(t)} e_{n,ZZ}^{(t)}, \\ E_{ZZ}^{\text{nt}} &= \frac{1}{Y_{\text{nt}}} \sum_{n=0}^{\infty} Q_n^{(\text{nt})} e_{n,ZZ}^{(\text{nt})}. \end{aligned} \quad (12)$$

According to the decoy-state method, the upper bound of bit error rate in the single-photon pulse can be effectively estimated. From the above equation we can obtain two upper bounds

$$\begin{aligned} e_{1,ZZ}^{(t)U} &= \frac{1}{Q_1^{(t)U}} (Y_t E_{ZZ}^t - \frac{1}{2} Q_0^{(t)}), \\ e_{1,ZZ}^{(\text{nt})U} &= \frac{1}{Q_1^{(\text{nt})L}} (Y_{\text{nt}} E_{ZZ}^{\text{nt}} - \frac{1}{2} Q_0^{(\text{nt})}). \end{aligned} \quad (13)$$

Similarly, when Alice and Bob obtain  $E_{ij}^t, E_{ij}^{\text{nt}} (ij \in \{XX, YY, XY, YX\})$ , they can estimate  $e_{1,ij}^{(t)U}, e_{1,ij}^{(\text{nt})U} (ij \in \{XX, YY, XY, YX\})$ . We select the minimum value to be the upper bound of the bit error rate in the single-photon pulse

$$\begin{aligned} e_{1,ZZ}^U &= \min(e_{1,ZZ}^{(t)U}, e_{1,ZZ}^{(\text{nt})U}), \\ e_{1,XX}^U &= e_{1,YY}^U = \min(e_{1,XX}^{(t)U}, e_{1,XX}^{(\text{nt})U}), \\ e_{1,XY}^U &= e_{1,YX}^U = \min(e_{1,XY}^{(t)U}, e_{1,XY}^{(\text{nt})U}). \end{aligned} \quad (14)$$

Then the lower bound of  $C$  for the single-photon pulse  $C_1^L$  and Eve's information for sifted key bits  $I_E$  can be estimated by

$$\begin{aligned} C_1^L &= (1 - 2e_{1,XX}^U)^2 + (1 - 2e_{1,XY}^U)^2 \\ &\quad + (1 - 2e_{1,YX}^U)^2 + (1 - 2e_{1,YY}^U)^2, \\ I_E &= (1 - e_{1,ZZ}^U)^2 h\left(\frac{1 + V_{\max}}{2}\right) \\ &\quad - e_{1,ZZ}^U h\left(\frac{1 + f(V_{\max})}{2}\right), \end{aligned} \quad (15)$$

where

$$\begin{aligned} V_{\max} &= \min[\sqrt{C_1^L/2/(1 - e_{1,ZZ}^U)}, 1], \\ f(V_{\max}) &= \sqrt{C_1^L/2 - (1 - e_{1,ZZ}^U)^2 V_{\max}^2} e_{1,ZZ}^U. \end{aligned} \quad (16)$$

When the distance is not so large, we produce a secret key not only from the triggered pulse but also from the nontriggered pulse. In this case, it is more efficient to apply the error reconciliation separately to

the triggered pulse and the nontriggered pulse. However, the privacy amplification is applied together.<sup>[22]</sup> The secret key rate can be calculated as

$$\begin{aligned} R &= -Y_t f[E_{ZZ}^t] h[E_{ZZ}^t] - Y_{\text{nt}} f[E_{ZZ}^{\text{nt}}] h[E_{ZZ}^{\text{nt}}] \\ &\quad + (Q_1^{t,L} + Q_1^{\text{nt},L})(1 - I_E), \end{aligned} \quad (17)$$

where  $f[E_{ZZ}^t]$  and  $f[E_{ZZ}^{\text{nt}}]$  denote the reconciliation efficiencies for the triggered pulse and the nontriggered pulse, respectively.

Considering the finite-key effect, we assume that the bases are chosen with probability  $P_X = P_Y = a$  and  $P_Z = 1 - 2a$ . Experimentally, each value of  $E_{ij}^t (ij \in \{XX, YY, XY, YX\})$  is estimated using  $m = Na^2 Y_t$  signals, and each value of  $E_{ij}^{\text{nt}} (ij \in \{XX, YY, XY, YX\})$  is estimated using  $n = Na^2 Y_{\text{nt}}$  signals. Meanwhile, values of  $E_{zz}^t$  and  $E_{zz}^{\text{nt}}$  are estimated using  $m1 = N(1 - 2a)^2 Y_t$  signals and  $n1 = N(1 - 2a)^2 Y_{\text{nt}}$  signals, respectively. For finite sample sizes, by exploiting Hoeffding's inequality<sup>[28,29]</sup> for independent events, we can correct  $E_{zz}^t$  and  $E_{zz}^{\text{nt}}$  as  $E_{zz}^{\prime t} = E_{zz}^t + \delta(m1 E_{zz}^t)$  and  $E_{zz}^{\prime \text{nt}} = E_{zz}^{\text{nt}} + \delta(n1 E_{zz}^{\text{nt}})$ , and  $E_{ij}^t, E_{ij}^{\text{nt}} (ij \in \{XX, YY, XY, YX\})$  can be corrected as  $E_{ij}^{\prime t} = E_{ij}^t - \delta(m)$  and  $E_{ij}^{\prime \text{nt}} = E_{ij}^{\text{nt}} - \delta(n E_{ij}^{\text{nt}})$ . Similarly, we can correct  $Y_t$  and  $Y_{\text{nt}}$  as  $Y'_t = Y_t + \delta(N)$  and  $Y'_{\text{nt}} = Y_{\text{nt}} - \delta(N)$ , where

$$\delta(x) = \sqrt{\frac{1}{2x} \ln \frac{1}{\varepsilon}}. \quad (18)$$

The key generation rate per pulse is given by

$$\begin{aligned} R &= -Y'_t f[E_{ZZ}^{\prime t}] h[E_{ZZ}^{\prime t}] \\ &\quad - Y'_{\text{nt}} f[E_{ZZ}^{\prime \text{nt}}] h[E_{ZZ}^{\prime \text{nt}}] \\ &\quad + (Q_1^{t,L} + Q_1^{\text{nt},L})(1 - I_E) \\ &\quad - \frac{1}{N} \left( \log_2 \frac{8}{\varepsilon_{\text{cor}}} + 2 \log_2 \frac{2}{\varepsilon_{\text{sec}}} + 2 \log_2 \frac{1}{2\varepsilon_{\text{PA}}} \right), \end{aligned} \quad (19)$$

where  $\varepsilon_{\text{cor}}$ ,  $\varepsilon_{\text{sec}}$ ,  $\varepsilon_{\text{PA}}$  and  $\varepsilon$  denote the maximal probability that the outputs on Alice's side and on Bob's side are not identical, the probability that Eve obtains the information of the final secret keys, the probability that privacy amplification fails and the probability that the real value of a parameter lies outside of the chosen fluctuation range, respectively,  $f[E_{ZZ}^t]$  and  $f[E_{ZZ}^{\text{nt}}]$  denote the reconciliation efficiency for the triggered pulse and the non-triggered pulse, respectively. Here we set  $\varepsilon = \varepsilon_{\text{cor}} = \varepsilon_{\text{sec}} = \varepsilon_{\text{PA}} = 10^{-10}$ . To obtain the correct information of Eve in the finite key case, we must adopt  $E_{ij}^{\prime t}, E_{ij}^{\prime \text{nt}} (ij \in \{XX, YY, XY, YX\})$  instead of  $E_{ij}^t, E_{ij}^{\text{nt}} (ij \in \{XX, YY, XY, YX\})$ . Similarly, to obtain the correct lower bound of the single-photon contribution, we adopt  $Y'_t$  and  $Y'_{\text{nt}}$  instead of  $Y_t$  and  $Y_{\text{nt}}$ . Then, the secret key rate in the finite key case can be calculated by Eq. (19).

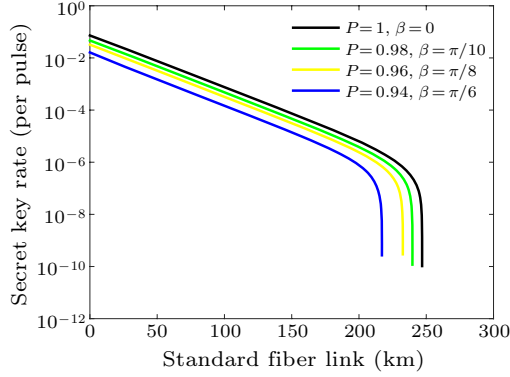
In this work, we use the practical parameters listed in Table 1, which come from Ref. [24,26] to theoretically simulate the final key rate. In addition, we

set  $\mu = 0.5$  and  $f[E_{ZZ}^t] = f[E_{ZZ}^{nt}] = f[E_{ZZ}^{\prime t}] = f[E_{ZZ}^{\prime nt}] = f$ .

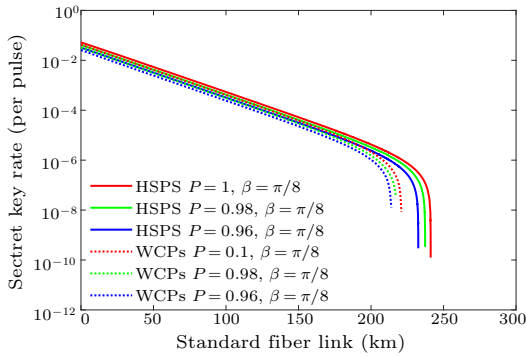
**Table 1.** Simulation parameters for decoy-state RFI QKD. Here  $d_B$  ( $\eta_B$ ) is the dark count rate (detection efficiency) of Bob's detector,  $d_A$  ( $\eta_A$ ) is the dark count rate (detection efficiency) of Alice's detector,  $\alpha$  is the loss coefficient in the standard fiber link, and  $f$  is the key reconciliation efficiency.

$d_B$	$d_A$	$\alpha$ (dB/km)	$\eta_A$	$\eta_B$	$f$
$6 \times 10^{-7}$	$10^{-6}$	0.2	0.8	0.2	1.16

Firstly, we simulate the secret key rate of passive decoy-state RFI QKD with HSPS under different conditions, and our simulation results are shown in Fig. 1.



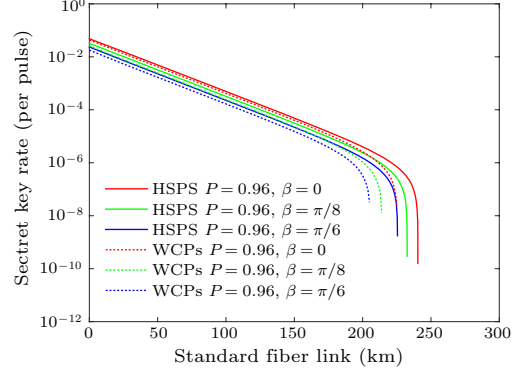
**Fig. 1.** Secret key rates of passive decoy-state RFI QKD with HSPS under different conditions. The lines from top to bottom are the secret key rates when  $P = 1, \beta = 0$ ;  $P = 0.98, \beta = \frac{\pi}{10}$ ;  $P = 0.96, \beta = \frac{\pi}{8}$ ; and  $P = 0.94, \beta = \frac{\pi}{6}$ , respectively.



**Fig. 2.** Comparison of the secret key rate between passive decoy-state RFI QKD using HSPS and decoy-state RFI QKD using the WCPS when the misalignments of reference frames are fixed but the probabilities that the signal state is correctly measured are different. The lines from top to bottom are the secret key rates of passive decoy-state RFI QKD using HSPS when  $P = 1, \beta = \frac{\pi}{8}$ ;  $P = 0.98, \beta = \frac{\pi}{8}$ ;  $P = 0.96, \beta = \frac{\pi}{8}$  and that using the WCPS when  $P = 1, \beta = \frac{\pi}{8}$ ;  $P = 0.98, \beta = \frac{\pi}{8}$ ; and  $P = 0.96, \beta = \frac{\pi}{8}$ , respectively.

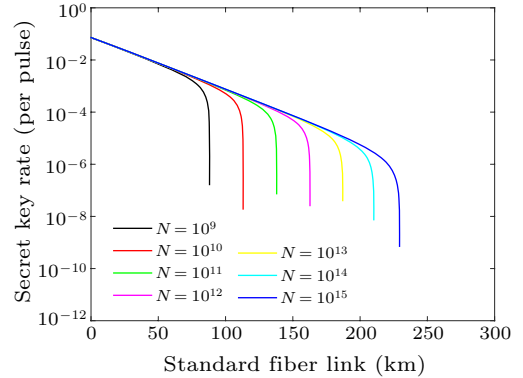
As shown in Fig. 1, our protocol is robust against the relative motion of the reference frames, which can distribute secret key bits even at  $\frac{\pi}{6}$  misalignment of reference frames when the distance from Alice to Bob is about 220 km in the asymptotic case. Then we compare the performance of passive decoy-state RFI QKD using HSPS with decoy-state RFI QKD using the WCPS in different cases. Our simulation results

are shown in Figs. 2 and 3.



**Fig. 3.** Comparison of the secret key rate between passive decoy-state RFI QKD using HSPS and decoy-state RFI QKD using the WCPS at different misalignments of reference frames. The lines from top to bottom are the secret key rates of passive decoy-state RFI QKD using HSPS when  $P = 0.96, \beta = 0$ ;  $P = 0.96, \beta = \frac{\pi}{8}$ ;  $P = 0.96, \beta = \frac{\pi}{6}$  and that using the WCPS when  $P = 0.96, \beta = 0$ ;  $P = 0.96, \beta = \frac{\pi}{8}$ ; and  $P = 0.96, \beta = \frac{\pi}{6}$ , respectively.

From Figs. 2 and 3, we can see that the passive decoy-state RFI QKD using HSPS in different cases performs better than the decoy-state RFI QKD using the WCPS in both secret key rate and secure transmission distance. Finally, with Hoeffding's inequality, we simulate the secret key rate of the passive decoy-state RFI QKD with HSPS. The results are shown in Fig. 4.



**Fig. 4.** RFI QKD with HSPS under different pulse number conditions when  $P = 1, \beta = 0$ . The lines from left to right are the secret key rate with the pulse number being  $10^9, 10^{10}, 10^{11}, 10^{12}, 10^{13}, 10^{14}$  and  $10^{15}$ .

In conclusion, we have proposed a passive decoy-state RFI QKD with HSPS and analyze its security. We have shown how to calculate the parameter  $C$  and the information of Eve in our protocol. With Hoeffding's inequality, we consider the statistical fluctuations. The results of the numerical simulation show that by combining the HSPS and the practical passive decoy-state method together, one not only can strengthen the secure transmission distance of RFI QKD, but also can improve the secret key rate of RFI QKD. Moreover, our protocol is as robust as the RFI QKD with the WCPS. In our protocol, Alice can dis-

tribute secret key bits even at  $\frac{\pi}{6}$  misalignment of reference frames to Bob when the distance is about 220 km in the asymptotic case. Therefore, the passive decoy-state RFI QKD with HSPS seems to be promising for practical implementation of QKD.

## References

- [1] Bennett C H and Brassard G 1984 *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (New York: IEEE) p 175
- [2] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dusek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301
- [3] Lo H K, Curty M and Tamaki K 2014 *Nat. Photon.* **8** 595
- [4] Tang G Z, Sun S H, Chen H, Li C Y and Liang L M 2016 *Chin. Phys. Lett.* **33** 120301
- [5] Tan Y G and Liu Q 2016 *Chin. Phys. Lett.* **33** 090303
- [6] Laing A, Scarani V, Rarity J G and O'Brien J L 2010 *Phys. Rev. A* **82** 012304
- [7] Zhang P, Aungskunsiri K, Martín-López E, Wabnig J, Lobino M, Nock R W, Munns J, Bonneau D, Jiang P, Li H W, Laing A, Rarity J G, Niskanen A O, Thompson M G and O'Brien J L 2014 *Phys. Rev. Lett.* **112** 130501
- [8] Wabnig J, Bitauld D, Li H W, Laing A, O'Brien J L and Niskanen A O 2013 *New J. Phys.* **15** 073001
- [9] Liang W Y, Wang S, Li H W, Yin Z Q, Chen W, Yao Y, Huang J Z, Guo G C and Han Z F 2015 *Sci. Rep.* **4** 3617
- [10] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
- [11] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
- [12] Lo H K, Ma X F and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
- [13] Brassard G, Lütkenhaus N, Mor T and Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330
- [14] Lütkenhaus N 2000 *Phys. Rev. A* **61** 052304
- [15] Wang C, Sun S H, Ma X C, Tang G Z and Liang L M 2015 *Phys. Rev. A* **92** 042319
- [16] Wang F M, Zhang P, Wang X L and Li F L 2016 *Phys. Rev. A* **94** 062330
- [17] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
- [18] Yin Z Q, Wang S, Chen W, Li H W, Guo G C and Han Z F 2014 *Quantum Inf. Process.* **13** 1237
- [19] Wang C, Song X T, Yin Z Q, Wang S, Chen W, Zhang C M, Guo G C and Han Z F 2015 *Phys. Rev. Lett.* **115** 160502
- [20] Zhang C M, Zhu J R and Wang Q 2017 *Phys. Rev. A* **95** 032309
- [21] Maurer W and Silberhorn C 2007 *Phys. Rev. A* **75** 050305
- [22] Adachi Y, Yamamoto T, Koashi M and Imoto N 2007 *Phys. Rev. Lett.* **99** 180503
- [23] Li Y, Bao W S, Li H W, Zhou C and Wang Y 2014 *Phys. Rev. A* **89** 032329
- [24] Wang Q, Wang X B and Guo G C 2007 *Phys. Rev. A* **75** 012312
- [25] Wang Q and Karlsson A 2007 *Phys. Rev. A* **76** 014309
- [26] Zhou C, Bao W S, Li H W, Wang Y, Li Y, Yin Z Q, Chen W and Han Z F 2014 *Phys. Rev. A* **89** 052328
- [27] Pramanik T, Park B K, Cho Y W, Han S W, Lee S Y, Kim Y S and Moon S 2017 *Phys. Lett. A* **381** 2497
- [28] Hoeffding W 1963 *J. Am. Stat. Assoc.* **58** 13
- [29] Wang Y, Bao W S, Zhou C, Jiang M S and Li H W 2016 *Phys. Rev. A* **94** 032335