

One-decoy state reference-frame-independent quantum key distribution

Xiang Li(李想), Hua-Wei Yuan(远华伟), Chun-Mei Zhang(张春梅), Qin Wang(王琴)

Citation: Chin. Phys. B . 2020, 29(7): 070303 . **doi:** 10.1088/1674-1056/ab90f6
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

Hybrid linear amplifier-involved detection for continuous variable quantum key distribution with thermal states

Yu-Qian He(贺宇千), Yun Mao(毛云), Hai Zhong(钟海), Duang Huang(黄端), Ying Guo(郭迎)

Chin. Phys. B . 2020, 29(5): 050309 . **doi:** 10.1088/1674-1056/ab8216

Reconciliation for CV-QKD using globally-coupled LDPC codes

Jin-Jing Shi(石金晶), Bo-Peng Li(李伯鹏), Duan Huang(黄端)

Chin. Phys. B . 2020, 29(4): 040301 . **doi:** 10.1088/1674-1056/ab6d4f

Reference-frame-independent quantum key distribution with an untrusted source

Jia-Ji Li(李家骥), Yang Wang(汪洋), Hong-Wei Li(李宏伟), Wan-Su Bao(鲍皖苏)

Chin. Phys. B . 2020, 29(3): 030303 . **doi:** 10.1088/1674-1056/ab695d

Performance analysis of continuous-variable measurement-device-independent quantum key distribution under diverse weather conditions

Shu-Jing Zhang(张淑静), Chen Xiao(肖晨), Chun Zhou(周淳), Xiang Wang(汪翔), Jian-Shu Yao(要建姝), Hai-Long Zhang(张海龙), Wan-Su Bao(鲍皖苏)

Chin. Phys. B . 2020, 29(2): 020301 . **doi:** 10.1088/1674-1056/ab5efd

Attacking a high-dimensional quantum key distribution system with wavelength-dependent beam splitter

Ge-Hai Du(杜舸海), Hong-Wei Li(李宏伟), Yang Wang(汪洋), Wan-Su Bao(鲍皖苏)

Chin. Phys. B . 2019, 28(9): 090301 . **doi:** 10.1088/1674-1056/ab343c

---

One-decoy state reference-frame-independent quantum key distribution*

Xiang Li(李想)[1,2,†], Hua-Wei Yuan(远华伟)[1,2,†], Chun-Mei Zhang(张春梅)[1,2], and Qin Wang(王琴)[1,2,‡]

[1] *Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*
[2] *Broadband Wireless Communication and Sensor Network Technology, Key Laboratory of Ministry of Education, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*

(Received 1 March 2020; revised manuscript received 22 April 2020; accepted manuscript online 7 May 2020)

Reference-frame-independent quantum key distribution (RFI-QKD) has been proven to be very useful and practical under realistic environment. Here, we present a scheme for one-decoy state RFI-QKD based on the work of Rusca *et al.* [*Appl. Phys. Lett.* **112**, 171104 (2018)], and carry out investigation on its performance under realistic experimental conditions. Numerical simulation results show that the one-decoy state RFI-QKD can achieve comparable performance in terms of secret key rate and transmission distance as the two-decoy state correspondence under practical experimental conditions. On contrast, it does not need to prepare the vacuum state in the former case, substantially reducing the experimental complexity and random number consumptions. Therefore, our present proposal seems very promising in practical implementations of RFI-QKD.

Keywords: quantum key distribution, RFI-QKD, one decoy state

PACS: 03.67.Dd, 03.67.Hk, 42.65.Lm **DOI:** 10.1088/1674-1056/ab90f6

1. Introduction

Based on the principles of quantum mechanics, quantum key distribution (QKD) provides a way of generating information-theoretic secure keys between two distant parties, Alice and Bob. Since the first BB84 protocol[1] was proposed, much effort has been made to improve practical performance of QKD systems.[2–4] Many QKD experiments have been successfully demonstrated either in laboratories or field environments,[5–13] paving the way towards large-scale commercialization of QKD systems.

In most QKD systems, a shared reference frame is needed for Alice and Bob, which inevitably increases the cost and makes the QKD system more complicated. Fortunately, the reference-frame-independent QKD (RFI-QKD) protocol[14] was proposed by Laing *et al.*, which can generate secret keys even with slowly drifted reference frames. Up to date, there are plenty of theoretical and experimental works were carried out on RFI-QKD.[15–21] Moreover, due to the security property of MDI protocol, MDI-QKD has attracted more and more attention recently. Combined with RFI-QKD, there are some experiments on RFI-MDI.[22,23]

On the other hand, deterministic single-photon sources are still not available, and weak coherent laser pulses are usually used in most QKD systems. It brings a chance for eavesdropper (usually called Eve) to exploit the photon-number-splitting (PNS) attack.[24–26] To combat the PNS attack, the decoy-state method[2,27–29] has been adopted in practical QKD systems, where different number of decoy states can be employed. Recently, Rusca *et al.*[30] did investigation on one-decoy state BB84 QKD. In their work, it is demonstrated that the one-decoy state method can show advantages for most experimental settings.

In this paper, different from Rusca *et al.*[30] work which focused on BB84 protocol, we extend one-decoy state method to RFI-QKD and propose a scheme of one-decoy state RFI-QKD, and further compare its performance with two-decoy state correspondence by taking statistical fluctuation analysis into account. Simulation results demonstrate that our one-decoy state RFI scheme can achieve comparable performance as two-decoy state correspondence in terms of secret key rates and transmission distances.

2. One-decoy state scheme

In the one-decoy state RFI-QKD, Alice adopts two intensities ($\lambda \in \{\mu, \nu\}$) and three orthogonal basis (Z_A, X_A, and Y_A) to prepare quantum states, then Bob measures those states with basis Z_B, X_B, and Y_B. Generally speaking, the Z basis can be well aligned for common encoding schemes, and the X and Y basis are allowed to drift slowly with an unknown angle β. That is, the Z, X, and Y basis satisfy $Z_B = Z_A$,

*Project supported by the National Key Research and Development Program of China (Grant Nos. 2018YFA0306400 and 2017YFA0304100), the National Natural Science Foundation of China (Grant Nos. 61590932, 11774180, and 61705110), and the Natural Science Foundation of Jiangsu Province for Leading-edge Technology Program, China (Grant No. BK20192001).

†These authors contributed equally to this work.
‡Corresponding author. E-mail: qinw@njupt.edu.cn

© 2020 Chinese Physical Society and IOP Publishing Ltd

$X_B = \cos\beta X_A + \sin\beta Y_A$, and $Y_B = \cos\beta Y_A - \sin\beta X_A$. Usually, the Z basis is used to generate the final secret keys, the X and Y bases are used to estimate Eve's information.

After the quantum communication phase, the practical detection probability and quantum-bit error-rate (QBER) with intensity λ of quantum states that Alice sends in ξ_A basis and Bob measures in ξ_B basis can be given as

$$P^{\lambda,\mathrm{det}}_{\xi_A\xi_B} = \sum_{i=0}^{\infty} P_{\xi_A} P_{\xi_B} P_\lambda P_i(\lambda) Y_i, \tag{1}$$

$$P^{\lambda,\mathrm{det}}_{\xi_A\xi_B} E^{\lambda,\mathrm{det}}_{\xi_A\xi_B} = \sum_{i=0}^{\infty} P_{\xi_A} P_{\xi_B} P_\lambda P_i(\lambda) Y_i e_i, \tag{2}$$

where $\lambda \in \{\mu, \nu\}$, i denotes the number of photons, P_{ξ_A} (P_{ξ_B}) is the probability that Alice (Bob) choose the ξ_A (ξ_B) basis, P_λ denotes the probability that Alice prepare states with intensity λ, $P_i(\lambda)$ is the i-photon distribution of intensity λ, Y_i and e_i denote the yield and error rate of i-photon states. Concretely, considering the probability of a photon arriving at the erroneous single-photon detector, denoted as e_d, QBER can be calculated by Eq. (14) in Ref. [31], and for simulation, two threshold single-photon detectors are adopted at Bob's side, and the probability of the valid detection events conditional on i-photon states is[31]

$$P(i) = \begin{cases} 1 - Y_0, & i > 0, \\ Y_0(1 - Y_0), & i = 0, \end{cases}$$

where Y_0 is the dark count rate of single-photon detectors.

Considering the post-processing speed of a QKD system mainly depends on the block size being processed, *i.e.*, the number of pulses detected by Bob in Z basis within certain time window, here in our analysis, we assume the block size with a fixed value (n_{ZZ}). We can get the corresponding number of pulses that need to be sent (N_{tot}) by Alice with

$$N_{\mathrm{tot}} = \frac{n_{ZZ}}{P^{\mathrm{tot,det}}_{ZZ}}, \tag{3}$$

in which

$$P^{\mathrm{tot,det}}_{\xi_A\xi_B} = \sum_{\lambda=\mu,\nu} P^{\lambda,\mathrm{det}}_{\xi_A\xi_B}. \tag{4}$$

Then we can get the number of detection $n_{\xi_A\xi_B}$ and the number of errors $m_{\xi_A\xi_B}$ corresponding to basis $\xi_A\xi_B$

$$n_{\xi_A\xi_B} = N_{\mathrm{tot}} P^{\mathrm{tot,det}}_{\xi_A\xi_B}, \tag{5}$$

$$m_{\xi_A\xi_B} = n_{\xi_A\xi_B} \frac{P^{\mathrm{tot,det}}_{\xi_A\xi_B} E^{\mathrm{tot,det}}_{\xi_A\xi_B}}{P^{\mathrm{tot,det}}_{\xi_A\xi_B}}, \tag{6}$$

where

$$P^{\mathrm{tot,det}}_{\xi_A\xi_B} E^{\mathrm{tot,det}}_{\xi_A\xi_B} = \sum_{\lambda=\mu,\nu} P^{\lambda,\mathrm{det}}_{\xi_A\xi_B} E^{\lambda,\mathrm{det}}_{\xi_A\xi_B}. \tag{7}$$

Through the following equation, we can calculate the fraction of $n_{\xi_A\xi_B}$ corresponding to a certain intensity λ

$$n^\lambda_{\xi_A\xi_B} = n_{\xi_A\xi_B} \frac{P^{\lambda,\mathrm{det}}_{\xi_A\xi_B}}{P^{\mathrm{tot,det}}_{\xi_A\xi_B}}. \tag{8}$$

Similarly, the number of errors caused by pulses of intensity λ is

$$m^\lambda_{\xi_A\xi_B} = n_{\xi_A\xi_B} \frac{P^{\lambda,\mathrm{det}}_{\xi_A\xi_B} E^{\lambda,\mathrm{det}}_{\xi_A\xi_B}}{P^{\mathrm{tot,det}}_{\xi_A\xi_B}}. \tag{9}$$

In the following, let us take the finite-data size effect[30,32] into account. We can obtain the relation between the observed variables $n^\lambda_{\xi_A\xi_B}$ ($m^\lambda_{\xi_A\xi_B}$) and the corresponding asymptotic case $\hat{n}^\lambda_{\xi_A\xi_B}$ ($\hat{m}^\lambda_{\xi_A\xi_B}$) by Hoeffding's inequality as follows:

$$\left|\hat{n}^\lambda_{\xi_A\xi_B} - n^\lambda_{\xi_A\xi_B}\right| \le \delta(n_{\xi_A\xi_B}, \varepsilon_1), \tag{10}$$

$$\left|\hat{m}^\lambda_{\xi_A\xi_B} - m^\lambda_{\xi_A\xi_B}\right| \le \delta(m_{\xi_A\xi_B}, \varepsilon_2), \tag{11}$$

where the above inequalities hold with probabilities $1 - 2\varepsilon_1$ and $1 - 2\varepsilon_2$, respectively, and $\delta(x, \varepsilon) := \sqrt{x \log(1/\varepsilon)/2}$.

According to Ref. [30], the upper bound and the lower bound of $n^\lambda_{\xi_A\xi_B}$ ($m^\lambda_{\xi_A\xi_B}$) are given by

$$n^{\lambda,\pm}_{\xi_A\xi_B} := \frac{\mathrm{e}^\lambda}{P_\lambda}\left(n^\lambda_{\xi_A\xi_B} \pm \sqrt{\frac{n_{\xi_A\xi_B}}{2}\log\frac{1}{\varepsilon_1}}\right), \tag{12}$$

$$m^{\lambda,\pm}_{\xi_A\xi_B} := \frac{\mathrm{e}^\lambda}{P_\lambda}\left(m^\lambda_{\xi_A\xi_B} \pm \sqrt{\frac{m_{\xi_A\xi_B}}{2}\log\frac{1}{\varepsilon_2}}\right). \tag{13}$$

The lower-bound of single-photon events, the lower-bound and the upper-bound of vacuum events in basis $\xi_A\xi_B$ can be estimated with the following formulae

$$s^{\mathrm{L}}_{\xi_A\xi_B,1} = \frac{\tau_1\mu}{\nu(\mu-\nu)}\left(n^{\nu,-}_{\xi_A\xi_B} - \frac{\nu^2}{\mu^2} n^{\mu,+}_{\xi_A\xi_B} - \frac{\mu^2-\nu^2}{\mu^2}\frac{s^{\mathrm{U}}_{\xi_A\xi_B,0}}{\tau_0}\right), \tag{14}$$

$$s^{\mathrm{L}}_{\xi_A\xi_B,0} = \frac{\tau_0}{\mu-\nu}\left(\mu n^{\nu,-}_{\xi_A\xi_B} - \nu n^{\mu,+}_{\xi_A\xi_B}\right), \tag{15}$$

$$s^{\mathrm{U}}_{\xi_A\xi_B,0} = \min\left\{2\left[m_{\xi_A\xi_B} + \delta(n_{\xi_A\xi_B}, \varepsilon_1)\right], 2\tau_0\frac{\mathrm{e}^\lambda}{P_\lambda}\left[m^\lambda_{\xi_A\xi_B} + \delta(m_{\xi_A\xi_B}, \varepsilon_2)\right] + 2\delta(n_{\xi_A\xi_B}, \varepsilon_1)\right\}, \tag{16}$$

where $\tau_i = \sum_{\lambda\in\mu,\nu} P_\lambda \, \mathrm{e}^{-\lambda}\lambda^i/i!$ is the total probability to send an i-photon state, L and U denote the lower bound and the upper bound, respectively.

The upper bound of single-photon error rate $e^{1,\mathrm{U}}_{\xi_A\xi_B}$, and the upper bound of single-photon bits errors $v^{\mathrm{U}}_{\xi_A\xi_B,1}$ in the $\xi_A\xi_B$ basis can be expressed as follows:

$$e^{1,\mathrm{U}}_{\xi_A\xi_B} = \frac{v^{\mathrm{U}}_{\xi_A\xi_B,1}}{s^{\mathrm{L}}_{\xi_A\xi_B,1}}, \tag{17}$$

$$v^{\mathrm{U}}_{\xi_A\xi_B,1} = \frac{\tau_1}{\mu-\nu}\left(m^{\mu,+}_{\xi_A\xi_B} - m^{\nu,-}_{\xi_A\xi_B}\right). \tag{18}$$

In an RFI-QKD, an intermediate quantity C can be used to monitor Eve's information, given by

$$C = \left(1-2e^{1,\mathrm{U}}_{XX}\right)^2 + \left(1-2e^{1,\mathrm{U}}_{XY}\right)^2 + \left(1-2e^{1,\mathrm{U}}_{YX}\right)^2 + \left(1-2e^{1,\mathrm{U}}_{YY}\right)^2. \tag{19}$$

Normally, one can extract out secure keys under the condition that $e^{1,\mathrm{U}}_{ZZ} \leq 15.9\%$ in an RFI protocol, and estimate Eve's information with

$$I_{\mathrm{E}} = \left(1-e^{1,\mathrm{U}}_{ZZ}\right) h\left(\frac{1+\phi}{2}\right) + e^{1,\mathrm{U}}_{ZZ} h\left(\frac{1+\varphi}{2}\right), \tag{20}$$

where

$$\phi = \min\left[\frac{\sqrt{C/2}}{1-e^{1,\mathrm{U}}_{ZZ}}, 1\right], \tag{21}$$

$$\varphi = \frac{\sqrt{C/2-(1-e^{1,\mathrm{U}}_{ZZ})^2\phi^2}}{e^{1,\mathrm{U}}_{ZZ}}, \tag{22}$$

and $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy function.

As we know, the formula on calculating the secret keys of BB84 protocol has been addressed in Refs. [30,32]

$$l \leq s^{\mathrm{L}}_{ZZ,0} + s^{\mathrm{L}}_{ZZ,1}[1-h(\phi^{\mathrm{U}}_{ZZ})] - \lambda_{\mathrm{EC}} - a\log_2(b/\varepsilon_{\mathrm{sec}}) - \log_2(2/\varepsilon_{\mathrm{cor}}), \tag{23}$$

where ϕ^{U}_{ZZ} is the upper bound of the phase-error rate, λ_{EC} refers to the number of discarded bits during the error correction stage, $\varepsilon_{\mathrm{sec}}$ and $\varepsilon_{\mathrm{cor}}$ each corresponds to the secrecy and correctness parameters. a and b depend on the specific security analysis taken into account.[30,32]

Through similar method, we can deduce out the formula on calculating the secret key rate for RFI-QKD as

$$R \leq [s^{\mathrm{L}}_{ZZ,0} + s^{\mathrm{L}}_{ZZ,1}(1-I_E) - n_{ZZ} f h(E^{\mathrm{tot,det}}_{ZZ}) - a\log_2(b/\varepsilon_{\mathrm{sec}}) - \log_2(2/\varepsilon_{\mathrm{cor}})]/N_{\mathrm{tot}}, \tag{24}$$

where

$$\varepsilon_{\mathrm{sec}} = 3(2\alpha_1+\alpha_2+\alpha_3) + \gamma + 15\varepsilon_1 + 15\varepsilon_2, \tag{25}$$

which is the security parameter in one-decoy RFI-QKD, and the coefficients in the front of the term ε_1 and ε_2 are equal to the number of times of the inequalities (10) and (11) that implemented in the secret key length formula, respectively. α_1, α_2, α_3, and γ are the error terms. Comparing the security parameter between our present work and Refs. [30,32], the difference is the number of estimated parameters, a holds the same value as 6. For simplicity, here we set each error term with a common value ε, and obtain $\varepsilon_{\mathrm{sec}} = 43\varepsilon$. Therefore, $b = 43$.

3. Numerical simulations

In this section, we first simulate the value of C for both one-decoy and two-decoy state RFI-QKDs under different rotation angles (β), and further do comparison between their key generation rates under the same experimental conditions. Finally, we investigate the effect of the finite-data size on one-decoy RFI-QKD, we study the performance of the one-decoy state RFI-QKD with different block sizes (n_{ZZ}). It should be noted that, the efficiency of the detector and the internal losses of Bob's apparatus are included in the value of global attenuation η in our simulations. The experimental parameters used for simulations are all listed in Table 1.

Table 1. List of device parameters for simulations. Y_0 is the dark count rate of single-photon detectors; e_d is the misalignment error rate of optical systems; f is the error correction efficiency; $\varepsilon_{\mathrm{sec}}$ and $\varepsilon_{\mathrm{cor}}$ correspond to privacy and correctness parameters.

Y_0	e_d	f	$\varepsilon_{\mathrm{sec}}$	$\varepsilon_{\mathrm{cor}}$
10^{-8}	0.01	1.16	10^{-9}	10^{-15}

In Fig. 1, we investigate the value of C in one-decoy state and two-decoy state RFI-QKDs with different relative rotation angles of reference frames ($\beta \in \{0^\circ, 10^\circ, 20^\circ, 30^\circ\}$). The performance of both schemes deteriorates with the increase of β, which is attributed to the smearing of correlations of and $e^{1,\mathrm{U}}_{XX}$, $e^{1,\mathrm{U}}_{XY}$, $e^{1,\mathrm{U}}_{YX}$, $e^{1,\mathrm{U}}_{YY}$, and thus poor estimation of C. As we can see from Fig. 1, when the relative rotation angle is small, the values of C in the one-decoy state RFI-QKD is almost the same as that in the two-decoy state method. While when the rotation angle is getting larger, *i.e.*, $> 20^\circ$, the value of C in the one-decoy state scheme becomes lower than that in the two-decoy state method, representing worse parameter estimations of the one-decoy state scheme under this circumstance.

Figure 2 shows comparisons of the key rate between our present one-decoy state RFI-QKD and former two-decoy state RFI-QKDs under different rotation angles of reference frames. For general, we did not consider the dead time of single-photon detectors c_{DT} as in Ref. [30], which mainly affects the high-speed systems on the key generation rate in the initial global attenuation. Simulation results show that our present

results can exhibit better performance than the latter when relative rotation angle β is small ($< 20°$), benefiting from the less sensitive finite size effect in the one-decoy state method. While as the relative rotation angle β is getting larger ($> 20°$), the key rate of the latter scheme exceeds the former, which is mainly due to the worse parameter estimations of the one-decoy state scheme, as indicated with the C value in Fig. 1. That is, with the relative rotation angle β is getting larger, the correlations of $e_{XX}^{1,U}$, $e_{XY}^{1,U}$, $e_{YX}^{1,U}$, and $e_{YY}^{1,U}$ are smearing, which results in the C value in the one-decoy state RFI-QKD getting worse faster than that in the two-decoy state RFI-QKD, and will affect the key generation rate.

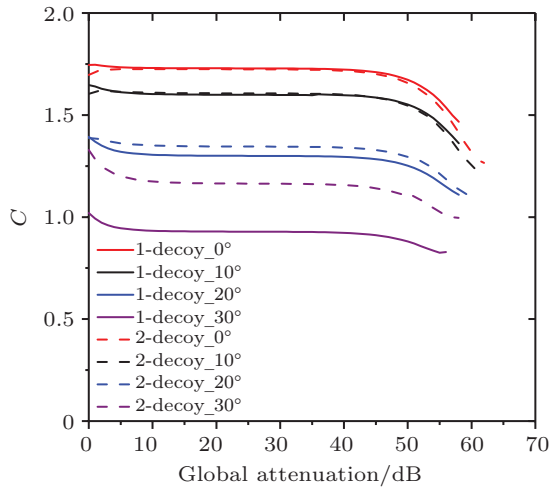


Fig. 1. Values of C for one-decoy state RFI-QKD at different relative rotation angles ($\beta \in \{0°, 10°, 20°, 30°\}$). The lines from top to bottom denote the results of $\beta = 0°$, $10°$, $20°$, and $30°$, respectively. Here we set block size $n_{ZZ} = 10^6$.

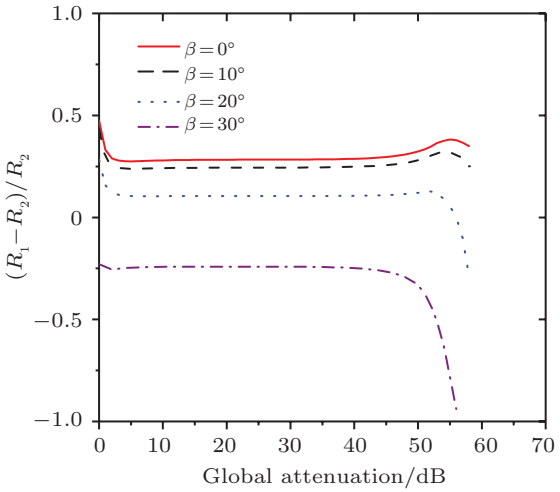


Fig. 2. Comparison of the key rate between the one-decoy state and the two-decoy state RFI-QKDs at different rotation angles β, where the SKR difference denoted by $(R_1 - R_2)/R_2$. Lines from top to bottom represent $\beta = 0°$, $10°$, $20°$, and $30°$, respectively. Here we set block size $n_{ZZ} = 10^6$.

In order to investigate the effect of the finite-data size on the one-decoy RFI-QKD, we compare the performance of the one-decoy state RFI-QKD with different sizes of block while setting the relative rotation angle with $20°$ ($n_{ZZ} \in \{10^5, 10^6, 10^7, 10^8\}$), as shown in Fig. 3. Obviously, the performance of the one-decoy state RFI-QKD will increase when the block size is getting larger. While when the block size is relatively larger, *e.g.*, $> 10^7$, the key rate is not sensitive to the finite data-size effect. Therefore, proper block sizes should be chosen in practical applications of the present scheme.

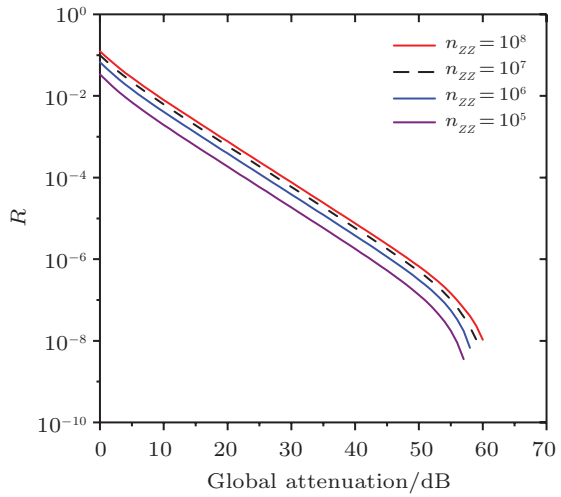


Fig. 3. Key rates *versus* global attention for the one-decoy RFI-QKD with different block sizes ($n_{ZZ} \in \{10^5, 10^6, 10^7, 10^8\}$). Lines from bottom to top denote the results of $n_{ZZ} = 10^5$, 10^6, 10^7, 10^8, individually. Here we set $\beta = 20°$.

4. Conclusion

In summary, we have proposed a scheme on one-decoy state reference-frame-independent quantum key distribution, and investigate its performance under realistic environments. Numerical simulation results show that, the performance of our present scheme can exceed traditional two-decoy state RFI-QKD when the rotation angle of reference frame is not larger, *e.g.*, $< 20°$. Moreover, it does not need to prepare the vacuum state in the former, and thus reduce the experimental complexity of QKD systems. Therefore, our present work could provide valuable references for practical implementation of the RFI-QKD.

References

[1] Bennett C H and Brassard G 1984 *Proceddings of the IEEE International Conference on Computers, Systems and Signal Processing*, 1999, Bangalore, India (IEEE, New York, 1984) p. 175
[2] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[3] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[4] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 *Nature* **557** 400
[5] Sasaki M, Fujiwara M, Ishizuka H, *et al.* 2011 *Opt. Express* **19** 10387
[6] Wang S, Chen W, Yin Z Q, *et al.* 2014 *Opt. Express* **22** 21739
[7] Tang Y L, Yin H L, Zhao Q, *et al.* 2016 *Phys. Rev. X* **6** 011024
[8] Fr?hlich B, Lucamarini M, Dynes J F, *et al.* 2017 *Optica* **4** 163
[9] Boaron A, Boso G, D Rusca, *et al.* 2018 *Phys. Rev. Lett.* **121** 190502
[10] Wang S, He D Y, Yin Z Q, *et al.* 2019 *Phys. Rev. X* **9** 021046
[11] Wang S, Chen W, Guo J F, *et al.* 2012 *Opt. Lett.* **37** 1008
[12] Wang S, Yin Z Q, Chen W, He D Y, *et al.* 2015 *Nat. Photon.* **9** 832
[13] Wang S, Chen W, Yin Z Q, He D Y, *et al.* 2018 *Opt. Lett.* **43** 2030
[14] Laing A, Scarani V, Rarity J G and O'Brien J L 2010 *Phys. Rev. A* **82** 012304

[15] Liang W Y, Wang S, Li H W, Yin Z Q, Chen W, Yao Y and Han Z F 2014 *Sci. Rep.* **4** 3617
[16] Yin Z Q, Wang S, Chen W, Li H W, Guo G C and Han Z F 2014 *Quantum Inf. Process.* **13** 1237
[17] Wang C, Sun S H, Ma X C, Tang G Z and Liang L M 2015 *Phys. Rev. A* **92** 042319
[18] Zhang C M, Zhu J R and Wang Q 2017 *Phys. Rev. A* **95** 032309
[19] Wang J P, Liu H w, Ma H Q and Sun S H 2019 *Phys. Rev. A* **99** 032309
[20] Liu H W, Wang J P, Ma H Q and Sun S H 2019 *Phys. Rev. A* **12** 034039
[21] Zhang P, Aungskunsiri K, Martín-López E, *et al.* 2014 *Phys. Rev. Lett.* **112** 130501
[22] 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
[23] Wang C, Yin Z Q, Wang S, Chen W, Guo G C and Han Z F 2017 *Optica* **4** 1016
[24] Brassard G, Lütkenhaus N, Mor T and Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330
[25] Lütkenhaus N 2000 *Phys. Rev. A* **61** 052304
[26] Lütkenhaus N and Jahma M 2002 *New J. Phys.* **4** 44
[27] Lo H, Ma X F and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[28] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[29] Hayashi M and Nakayama R 2014 *New J. Phys.* **16** 063009
[30] Rusca D, Boaron A, Grünenfelder F, Martin A and Zbinden H 2018 *Appl. Phys. Lett.* **112** 171104
[31] Zhang C M, Zhu J R and Wang Q 2018 *J. Phys. Commun.* **2** 055029
[32] Lim C C W, Curty M, Walenta N, *et al.* 2014 *Phys. Rev. A* **89** 022307