

Improved reference-frame-independent quantum key distribution with intensity fluctuations

Zi-Qi Chen(陈子骐), Hao-Bing Sun(孙昊冰), Ming-Shuo Sun(孙铭烁), and Qin Wang(王琴)

Citation: Chin. Phys. B, 2025, 34 (**2**): 020302. DOI: 10.1088/1674-1056/ad99cb
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

Multi-protocol relay chaining for large-scale quantum key distribution networks

Yuan Cao(曹原), Xiaosong Yu(郁小松), Yongli Zhao(赵永利), Chunhui Zhang(张春辉), Xingyu Zhou(周星宇), Jie Zhang(张杰), and Qin Wang(王琴)
Chin. Phys. B, 2025, 34 (**1**): 010310. DOI: 10.1088/1674-1056/ad9018

Security analysis of satellite-to-ground reference-frame-independent quantum key distribution with beam wandering

Chun Zhou(周淳), Yan-Mei Zhao(赵燕美), Xiao-Liang Yang(杨晓亮), Yi-Fei Lu(陆宜飞), Yu Zhou(周雨), Xiao-Lei Jiang(姜晓磊), Hai-Tao Wang(汪海涛), Yang Wang(汪洋), Jia-Ji Li(李家骥), Mu-Sheng Jiang(江木生), Xiang Wang(汪翔), Hai-Long Zhang(张海龙), Hong-Wei Li(李宏伟), and Wan-Su Bao(鲍皖苏)
Chin. Phys. B, 2024, 33 (**8**): 080306. DOI: 10.1088/1674-1056/ad51f6

Improvement and security analysis of multi-ring discrete modulation continuous variable quantum secret sharing scheme

Huan-Yao Jiang(姜欢窈), Min Nie(聂敏), Guang Yang(杨光), Ai-Jing Sun(孙爱晶), Mei-Ling Zhang(张美玲), and Chang-Xing Pei(裴昌幸)
Chin. Phys. B, 2024, 33 (**7**): 070303. DOI: 10.1088/1674-1056/ad3b81

General multi-attack detection for continuous-variable quantum key distribution with local local oscillator

Zhuo Kang(康茁), Wei-Qi Liu(刘维琪), Jin Qi(齐锦), and Chen He(贺晨)
Chin. Phys. B, 2024, 33 (**5**): 050308. DOI: 10.1088/1674-1056/ad2bf2

A new quantum key distribution resource allocation and routing optimization scheme

Lin Bi(毕琳), Xiaotong Yuan(袁晓同), Weijie Wu(吴炜杰), and Shengxi Lin(林升熙)
Chin. Phys. B, 2024, 33 (**3**): 030309. DOI: 10.1088/1674-1056/ad2503

SPECIAL TOPIC — Quantum communication and quantum network

Improved reference-frame-independent quantum key distribution with intensity fluctuations

Zi-Qi Chen(陈子骐)[1,2], Hao-Bing Sun(孙昊冰)[1,2], Ming-Shuo Sun(孙铭烁)[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 19 September 2024; revised manuscript received 21 November 2024; accepted manuscript online 3 December 2024)

Reference-frame-independent quantum key distribution (RFI-QKD) can avoid real-time calibration operation of reference frames and improve the efficiency of the communication process. However, due to imperfections of optical devices, there will inevitably exist intensity fluctuations in the source side of the QKD system, which will affect the final secure key rate. To reduce the influence of intensity fluctuations, an improved 3-intensity RFI-QKD scheme is proposed in this paper. After considering statistical fluctuations and implementing global parameter optimization, we conduct corresponding simulation analysis. The results show that our present work can present both higher key rate and a farther transmission distance than the standard method.

Keywords: quantum key distribution, intensity fluctuations, decoy-state method

PACS: 03.67.Dd, 03.67.Hk, 42.65.Lm

DOI: 10.1088/1674-1056/ad99cb **CSTR:** 32038.14.CPB.ad99cb

1. Introduction

In 1984, Bennett and Brassard proposed the so-called BB84 protocol,[1,2] representing the beginning of quantum key distribution (QKD). The security of QKD is based on the law of quantum physics, and in principle, it can allow two distant parties Alice and Bob to construct unconditional secure communications. Thereafter, a great number of theoretical and experimental works have been carried out.[3]

As we know, some assumptions are made in the security proof of QKD, which are very hard to satisfy in practice. This leads to many vulnerabilities in QKD systems.[4–8] An eavesdropper, Eve, can exploit these vulnerabilities to attack QKD systems, and thus threaten their practical security. Besides, there exists drift of reference frames between Alice and Bob in practical QKD applications. People have to do reference frame calibration before the key transmission, making the QKD system inefficient. Fortunately, the reference-frame-independent QKD (RFI-QKD) protocol was proposed,[9] which allows Alice and Bob to share secret keys without the alignment of reference frames. As a result, the RFI-QKD protocol can show much better performance compared with standard BB84 protocols and thus attracted a lot of attention.[10–17] On the other hand, the decoy state method was put forward[18–20] to resist the photon-number-splitting attack.[21–23] Usually, it requires the stability of the light source. However, in practice, imperfect modulators or lasers will inevitably produce intensity fluctuations, making this requirement impossible to achieve. In recent years, several methods were proposed to reduce the influences of intensity fluctuations.[24–26] Here we present an improved RFI-QKD protocol by taking intensity fluctuations into account, and significantly increase its performance.

The paper is arranged as follows: we describe the theory for the improved RFI-QKD protocol with intensity fluctuations in Section 2. Then, we carry out numerical simulations and discussions in Section 3. Finally, conclusions are given in Section 4.

2. Improved RFI-QKD protocol with intensity fluctuations

In this section, we introduce the theory of the improved protocol. Below let us introduce the protocol step by step.

(1) Quantum state preparation: At the sender's side, Alice randomly modulates light sources into three different intensities (μ, ν, 0), each called the signal state, the decoy state, and the vacuum state, with probabilities P_μ, P_ν, and $1-P_\mu-P_\nu$, respectively. For the signal state, Alice prepares each pulse on Z, X, and Y bases with conditional probabilities $P_{Z_A|\mu}$, $P_{X_A|\mu}$, and $1-P_{Z_A|\mu}-P_{X_A|\mu}$, respectively. For the decoy state, Alice prepares each pulse on Z, X, and Y bases with conditional probabilities $P_{Z_A|\nu}$, $P_{X_A|\nu}$, and $1-P_{Z_A|\nu}-P_{X_A|\nu}$, correspondingly.

(2) Quantum state measurement: At the receiver's side, Bob randomly selects Z, X, or Y bases to measure the received pulses with probabilities P_{Z_B}, P_{X_B}, and $1-P_{Z_B}-P_{X_B}$, respec-

†Corresponding author. E-mail: qinw@njupt.edu.cn

© 2025 Chinese Physical Society and IOP Publishing Ltd. All rights, including for text and data mining, AI training, and similar technologies, are reserved.

tively, and records the measurement results.

(3) Basis vector comparison: Alice and Bob publicly announce the basis and intensity selection information, and obtain the sifted key.

(4) Parameter estimation: Alice and Bob select some bits from the sifted key for comparison, and estimate the single-photon count rate and single-photon error rate.

(5) Post-processing: Alice and Bob perform error correction, and privacy amplification processes to extract the secure key.

In RFI-QKD protocol, as shown in Fig. 1, the Z basis of the Alice and Bob ends can remain aligned, while the X and Y bases can be unaligned, and the three bases satisfy the following relationship:

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

where β represents the deflection angle of the reference frame.

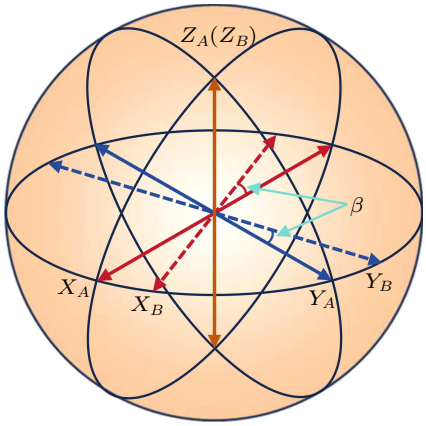


Fig. 1. Bloch sphere of Alice and Bob's reference frames. The solid line represents Alice's reference frame, while the dashed line represents Bob's drifted reference frame.

In the real protocol, as shown in Fig. 2(a), Alice sends out N light pulses, and randomly modulates each pulse into three different intensities $(\mu, \nu, 0)$. Due to the instability of the light source, the intensity of the signal state in the i-th light pulse is denoted as μ^i, and the intensity of the decoy state in the i-th light pulse is denoted as ν^i, where

$$\begin{aligned} \mu^i &= \left(1+\delta_\mu^i\right)\mu, \\ \nu^i &= \left(1+\delta_\nu^i\right)\nu, \end{aligned} \tag{2}$$

and $|\delta_\mu^i| \le \delta_\mu$, $|\delta_\nu^i| \le \delta_\nu$, δ_μ and δ_ν are known values in this protocol. The lower and upper bounds of a physical quantity are represented by the superscripts L and U, respectively. Therefore, we have

$$\begin{aligned} \mu^{\mathrm{U}} &= \left(1+\delta_\mu\right)\mu, \quad \mu^{\mathrm{L}} = \left(1-\delta_\mu\right)\mu, \\ \nu^{\mathrm{U}} &= \left(1+\delta_\nu\right)\nu, \quad \nu^{\mathrm{L}} = \left(1-\delta_\nu\right)\nu. \end{aligned} \tag{3}$$

In order to give a tighter estimation, below we construct a virtual protocol,[26] as shown in Fig. 2(b). Its security is exactly equivalent to that of the real protocol. We assume that we can strictly control the fluctuation range in $[-\delta_\nu, +\delta_\nu]$, and we can precisely control the intensity of the decoy state as ν^{U}.[25]

In the actual experiment, we will first measure the intensity fluctuation multiple times and then take its maximum value among the signal state and the decoy state. The intensity fluctuation value mentioned in the paper is based on accumulated data. After passing the attenuator we get $\nu^i = \left(1+\delta_\nu^i\right)\nu$. From this, we can get the attenuation factor η^i of the attenuator, which is

$$\eta^i = \frac{\nu^i}{\nu^{\mathrm{U}}} = \frac{1+\delta_\nu^i}{1+\delta_\nu}. \tag{4}$$

Then we have $\mu'^i = \mu^i/\eta^i$, where μ'^i is the intensity of the signal state before the attenuator and μ^i is the intensity of the signal state after passing the attenuator.

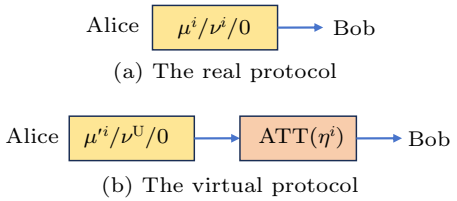


Fig. 2. Comparison between (a) the real protocol and (b) the virtual protocol. ATT represents the attenuator and η^i is the attenuation factor. In the real protocol, Alice sends signal state μ^i, decoy state ν^i and vacuum state 0 to Bob. In the virtual protocol, Alice sends signal state μ'^i, decoy state ν^{U} and vacuum state 0 to Bob.

Here we use the weak coherent source (WCS) as the light source, which obeys the Poisson distribution

$$\rho_\lambda = \sum_{k=0}^{+\infty} \frac{\lambda^k \mathrm{e}^{-\lambda}}{k!} |k\rangle\langle k|, \quad (\lambda = \mu, \nu;\ k = 0, 1, 2\ldots). \tag{5}$$

In the i-th light pulse of preparing quantum states by the RFI-QKD protocol, at the sending end, Alice sends intensity pulses of signal state, decoy state and vacuum state with probability P_μ, P_ν and $1-P_\mu-P_\nu$, respectively. For the signal pulse, the probability that Alice chooses the Z, X and Y bases is $P_{Z_A|\mu}$, $P_{X_A|\mu}$ and $1-P_{Z_A|\mu}-P_{X_A|\mu}$, respectively. For the decoy pulse, the probability that Alice chooses the Z, X and Y bases is $P_{Z_A|\nu}$, $P_{X_A|\nu}$ and $1-P_{Z_A|\nu}-P_{X_A|\nu}$, respectively. At the receiving end, Bob randomly selects the Z, X and Y bases to measure the pulse with probabilities P_{Z_B}, P_{X_B} and $1-P_{Z_B}-P_{X_B}$, respectively. If source ν is chosen, Alice actually prepares a WCS pulse in state $|\mathrm{e}^{\mathrm{i}\theta_\nu^i}\sqrt{\nu^{\mathrm{U}}}\rangle$, where θ_ν^i is random in $[0, 2\pi]$, the imaginary unit is represented by i and $\nu^{\mathrm{U}} = (1+\delta_\nu)\nu$. If source μ is chosen, Alice actually prepares a WCS pulse in state $|\mathrm{e}^{\mathrm{i}\theta_\mu^i}\sqrt{\mu'^i}\rangle$, where

$$\mu'^i = \frac{1+\delta_\nu}{1+\delta_\nu^i}\mu^i, \tag{6}$$

and then we can derive that

$$\mu^{\mathrm{L}} = \mu, \tag{7}$$

$$\mu^{\mathrm{U}} = \frac{1+\delta_\mu}{1-\delta_\mu}\mu. \tag{8}$$

After considering the intensity fluctuations, the photon number distribution of WCS follows the Poisson distribution with an average photon number of λ^i, whose upper bound and lower bound are respectively

$$P_n^{\mathrm{L}}(\lambda^{\mathrm{L}}) = \sum_{n=0}^{+\infty} \frac{(\lambda^{\mathrm{L}})^n}{n!} \mathrm{e}^{-\lambda^{\mathrm{L}}}, \tag{9}$$

$$P_n^{\mathrm{U}}(\lambda^{\mathrm{U}}) = \sum_{n=0}^{+\infty} \frac{(\lambda^{\mathrm{U}})^n}{n!} \mathrm{e}^{-\lambda^{\mathrm{U}}}, \tag{10}$$

where $P^{\lambda}_{\xi_A^0\xi_B^0}$ represents the probability that Bob's measurement result after using ξ_B basis measurement is 0 under the condition that Alice prepares the quantum state ξ_A^0, $\xi_A \in \{X_A, Y_A, Z_A\}$, $\xi_B \in \{X_B, Y_B, Z_B\}$, and its upper and lower bounds are

$$\begin{aligned} P^{\lambda,\mathrm{L}}_{\xi_A^0\xi_B^0} &= \sum_{n=0}^{+\infty} P_n^{\mathrm{L}}(\lambda^{\mathrm{L}}) \\ &\quad \times \sum_{j=0}^{n} C_n^j \eta^j (1-\eta)^{n-j} \left(|\langle \xi_A^0 | \xi_B^0 \rangle|^2\right)^j F(j), \end{aligned} \tag{11}$$

$$\begin{aligned} P^{\lambda,\mathrm{U}}_{\xi_A^0\xi_B^0} &= \sum_{n=0}^{+\infty} P_n^{\mathrm{U}}(\lambda^{\mathrm{U}}) \\ &\quad \times \sum_{j=0}^{n} C_n^j \eta^j (1-\eta)^{n-j} \left(|\langle \xi_A^0 | \xi_B^0 \rangle|^2\right)^j F(j). \end{aligned} \tag{12}$$

In the same way, we can get the expression for the upper and lower bounds of $P^{\lambda}_{\xi_A^0\xi_B^1}$, $P^{\lambda}_{\xi_A^1\xi_B^0}$ and $P^{\lambda}_{\xi_A^1\xi_B^1}$.

Then we can get the upper and lower bounds of the gain $Q^{\lambda}_{\xi_A\xi_B}$:

$$Q^{\lambda,\mathrm{L}}_{\xi_A\xi_B} = \frac{1}{2}\left(P^{\lambda,\mathrm{L}}_{\xi_A^0\xi_B^0} + P^{\lambda,\mathrm{L}}_{\xi_A^0\xi_B^1} + P^{\lambda,\mathrm{L}}_{\xi_A^1\xi_B^0} + P^{\lambda,\mathrm{L}}_{\xi_A^1\xi_B^1}\right), \tag{13}$$

$$Q^{\lambda,\mathrm{U}}_{\xi_A\xi_B} = \frac{1}{2}\left(P^{\lambda,\mathrm{U}}_{\xi_A^0\xi_B^0} + P^{\lambda,\mathrm{U}}_{\xi_A^0\xi_B^1} + P^{\lambda,\mathrm{U}}_{\xi_A^1\xi_B^0} + P^{\lambda,\mathrm{U}}_{\xi_A^1\xi_B^1}\right). \tag{14}$$

The upper and lower bounds of quantum-bit error rate $E^{\lambda}_{\xi_A\xi_B}$ can be expressed as

$$E^{\lambda,\mathrm{L(U)}}_{\xi_A\xi_B} = \min\left\{\tilde{E}^{\lambda,\mathrm{L(U)}}_{\xi_A\xi_B}, 1-\tilde{E}^{\lambda,\mathrm{L(U)}}_{\xi_A\xi_B}\right\}, \tag{15}$$

where

$$\tilde{E}^{\lambda,\mathrm{L(U)}}_{\xi_A\xi_B} = e_d\left(1-2e^{\lambda,\mathrm{L(U)}}_{\xi_A\xi_B}\right) + e^{\lambda,\mathrm{L(U)}}_{\xi_A\xi_B}, \tag{16}$$

$$e^{\lambda,\mathrm{L(U)}}_{\xi_A\xi_B} = \frac{P^{\lambda,\mathrm{L(U)}}_{\xi_A^0\xi_B^1} + P^{\lambda,\mathrm{L(U)}}_{\xi_A^1\xi_B^0}}{2Q^{\lambda,\mathrm{U(L)}}_{\xi_A\xi_B}}. \tag{17}$$

The lower bound $Y^{1,\mathrm{L}}_{Z_AZ_B}$ of the single photon count rate and the upper bound $e^{1,\mathrm{U}}_{Z_AZ_B}$ of the single photon bit error rate under the basis vector combination Z_AZ_B can be obtained as follows:[27]

$$Y^{1,\mathrm{L}}_{Z_AZ_B} \geq \frac{P_2^{\mathrm{L}}(\mu^{\mathrm{L}})Q^{\nu,L}_{Z_AZ_B} - P_2^{\mathrm{U}}(\nu^{\mathrm{U}})Q^{\mu,\mathrm{U}}_{Z_AZ_B} - \left[P_2^{\mathrm{L}}(\mu^{\mathrm{L}})P_0^{\mathrm{U}}(\nu^{\mathrm{U}}) - P_0^{\mathrm{L}}(\mu^{\mathrm{L}})P_2^{\mathrm{U}}(\nu^{\mathrm{U}})\right]Q^{0,\mathrm{U}}}{P_2^{\mathrm{L}}(\mu^{\mathrm{L}})P_1^{\mathrm{U}}(\nu^{\mathrm{U}}) - P_1^{\mathrm{L}}(\mu^{\mathrm{L}})P_2^{\mathrm{U}}(\nu^{\mathrm{U}})}, \tag{18}$$

$$e^{1,\mathrm{U}}_{Z_AZ_B} \leq \frac{E^{\nu,\mathrm{U}}_{Z_AZ_B}Q^{\nu,\mathrm{U}}_{Z_AZ_B} - P_0^{\mathrm{U}}(\nu^{\mathrm{U}})E^0Q^{0,\mathrm{L}}}{P_1^{\mathrm{U}}(\nu^{\mathrm{U}})Y^{1,\mathrm{L}}_{Z_AZ_B}}, \tag{19}$$

where $E^0 = 0.5$.

Using the same method, the upper bounds $e^{1,\mathrm{U}}_{X_AX_B}$, $e^{1,\mathrm{U}}_{X_AY_B}$, $e^{1,\mathrm{U}}_{Y_AX_B}$ and $e^{1,\mathrm{U}}_{Y_AY_B}$ of the single-photon bit error rate for basis vector combinations X_AX_B, X_AY_B, Y_AX_B and Y_AY_B can be estimated. By using $e^{1,\mathrm{U}}_{X_AX_B}$, $e^{1,\mathrm{U}}_{X_AY_B}$, $e^{1,\mathrm{U}}_{Y_AX_B}$ and $e^{1,\mathrm{U}}_{Y_AY_B}$, the intermediate parameter C can be obtained, and the calculation formula is[9]

$$\begin{aligned} C &= \left(1-2e^{1,\mathrm{U}}_{X_AX_B}\right)^2 + \left(1-2e^{1,\mathrm{U}}_{X_AY_B}\right)^2 \\ &\quad + \left(1-2e^{1,\mathrm{U}}_{Y_AX_B}\right)^2 + \left(1-2e^{1,\mathrm{U}}_{Y_AY_B}\right)^2. \end{aligned} \tag{20}$$

The information I_E stolen by Eve is a function of the upper bound $e^{1,\mathrm{U}}_{Z_AZ_B}$ of the single-photon error rate, the intermediate parameter C and the basis vector combination Z_AZ_B, which can be expressed as[9]

$$I_E = (1-e^{1,\mathrm{U}}_{Z_AZ_B})H\left(1+\frac{w}{2}\right) + e^{1,\mathrm{U}}_{Z_AZ_B}H\left(1+\frac{V}{2}\right), \tag{21}$$

where

$$w = \min\left\{\frac{\sqrt{C/2}}{1-e^{1,\mathrm{U}}_{Z_AZ_B}}, 1\right\}, \tag{22}$$

$$V = \frac{\sqrt{C/2 - \left(1-e^{1,\mathrm{U}}_{Z_AZ_B}\right)^2 w^2}}{e^{1,\mathrm{U}}_{Z_AZ_B}}, \tag{23}$$

$H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon function.

Combined with the above analysis and GLLP formula, the formula of the RFI-QKD protocol security key rate with source errors is[9]

$$\begin{aligned} R^{\mathrm{L}} &= P_\mu P_{Z_A|\mu} P_{Z_B}\left[P_1^{\mathrm{L}}(\mu^{\mathrm{L}})Y^{1,\mathrm{L}}_{Z_AZ_B}(1-I_E)\right. \\ &\quad \left. - fQ^{\mu,L}_{Z_AZ_B}H\left(E^{\mu,U}_{Z_AZ_B}\right)\right], \end{aligned} \tag{24}$$

where f is the error correction efficiency.

3. Numerical simulation and discussion

In this section, we carry out corresponding numerical simulations. To demonstrate the performance of our scheme, we fixed the deflection angle of the reference frame β and the light source fluctuation value δ respectively, and compared the key rate and the transmission distance between the standard method and our present work. In addition, we applied our work to the BB84-QKD protocol and compared it with the RFI-QKD protocol, proving the better characteristics of the RFI-QKD protocol. To be more realistic, we consider statistical fluctuations and global optimization. The system parameters we used are shown in Table 1. Here, $\eta_{\rm d}$ is the detection efficiency of detectors; Y_0 is the dark count rate of the single photon detector; $e_{\rm d}$ is the misalignment error probability; α is the loss coefficient of the transmission fibers; f is the error correction efficiency; γ is a parameter corresponding to the standard deviation of statistical fluctuations; N is the total number of signals sent by Alice and Bob. We carried out full parameter optimization for μ, ν, P_μ, P_ν, $P_{Z_A|\mu}$, $P_{X_A|\mu}$, $P_{Z_A|\nu}$, $P_{X_A|\nu}$, P_{Z_B} and P_{X_B}.

Table 1. List of experimental parameters used in numerical simulations.

$\eta_{\rm d}$	Y_0	$e_{\rm d}$	α	f	γ	N
0.145	3.0×10^{-6}	1.5%	0.2 dB/km	1.16	5.3	1.0×10^{11}

In Fig. 3, we make a comparison between our present work and the standard method for different intensity fluctuations by setting the deflection angle β at 0. We can see from Fig. 3 that when the value of intensity fluctuations δ increases from 0.03 to 0.05, the transmission distance of our present work only slightly decreases its value, i.e., by 1.4 km. However, for the standard method, its transmission distance depresses more than 6 km. We also analyzed the situation where the intensity fluctuation value is beyond the normal range ($\delta = 0.15$), and it can be seen that our method still performs much better, which means it is not limited by the intensity fluctuation value δ. The longest transmission distances for different methods are listed in Table 2.

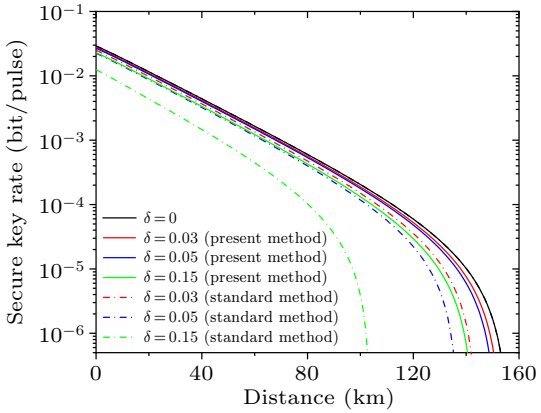


Fig. 3. Comparison of the key rate between our present work and the standard method, setting the deflection angle as $\beta = 0$. The dashed lines represent key rates using the standard method. The solid lines represent the key rates using our present work.

Table 2. Comparison of transmission distance between standard method and present work. ($\beta = 0$, $R = 5.0\times10^{-7}$ bit/pulse).

	$\delta = 0$	$\delta = 0.03$	$\delta = 0.05$	$\delta = 0.15$
Standard method	153.1 km	141.9 km	135.1 km	102.6 km
Present work	153.1 km	150.4 km	148.7 km	140.5 km

In Fig. 4, we compare the key rate between the standard method and our present work under different deflection angles by setting intensity fluctuation value δ at 0.05. We find that our present work can give a much higher key rate than the standard method when the deflection angle is 0. When the deflection angle increases to $\pi/8$, the transmission distance of our present work only decreases by a few kilometers, while that of the standard method will reduce more than 13 km. The transmission distances for different methods under different deflection angles are listed in Table 3.

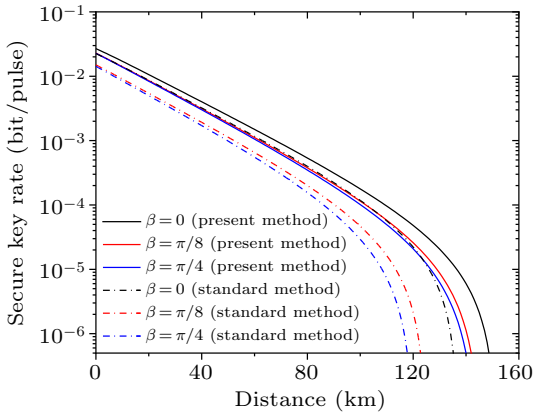


Fig. 4. Comparison of the key rate between our present work and the standard method, setting the intensity error as $\delta = 0.05$. The dashed lines represent key rates using the standard method. The solid lines represent the key rates using our present work.

Table 3. Comparison of transmission distance between standard method and present work. ($\delta = 0.05$, $R = 5.0\times10^{-7}$ bit/pulse).

	$\beta = 0$	$\beta = \pi/8$	$\beta = \pi/4$
Standard method	135.1 km	122.8 km	117.9 km
Present work	148.7 km	142.0 km	140.0 km

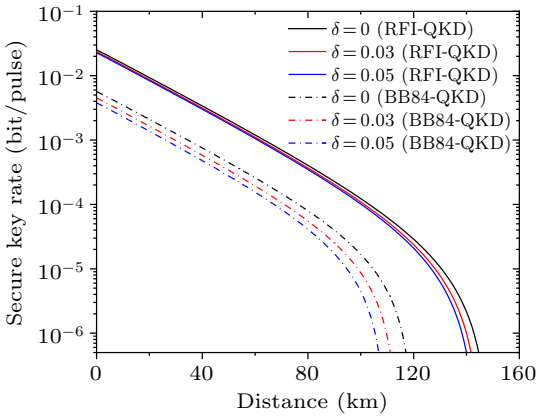


Fig. 5. Comparison of the key rate between the RFI-QKD protocol and the BB84-QKD protocol when using our present method and setting the deflection angle at $\beta = \pi/4$. The dashed lines represent key rates of the RFI-QKD protocol. The solid lines represent the key rates of the BB84-QKD protocol.

Table 4. Comparison of transmission distance between BB84-QKD and RFI-QKD. ($\beta = \pi/4$, $R = 5.0 \times 10^{-7}$ bit/pulse).

	$\delta = 0$	$\delta = 0.03$	$\delta = 0.05$
BB84-QKD	117.1 km	111.1 km	106.7 km
RFI-QKD	144.6 km	141.8 km	140.0 km

In Fig. 5, we make comparisons between the BB84-QKD protocol and the RFI-QKD protocol when both using the improved method of analyzing intensity fluctuations by setting the deflection angle at $\beta = \pi/4$. Obviously, our present improved RFI-QKD protocol can show much better performance than the BB84-QKD protocol for $\delta = 0$, $\delta = 0.03$, and $\delta = 0.05$. And the larger the intensity fluctuation, the more advantages our present work can show. The detailed transmission distances for different protocols are listed in Table 4.

4. Conclusion

In this study, we propose an improved method to enhance the performance of the RFI-QKD protocol with intensity fluctuations. In order to obtain a tighter boundary, we introduce an equivalent virtual RFI-QKD protocol and construct the security model. Moreover, we take the finite data size effect into account and implement full parameter optimization in our simulations. Simulation results show that, when there exists intensity fluctuation in light sources, our present work can show much better performance than either the standard RFI-QKD protocol and the BB84 protocol. Therefore, our work can provide a valuable tool for practical implementation of quantum key distributions in the near future.

Acknowledgements

We gratefully acknowledge the financial support from the Industrial Prospect and Key Core Technology Projects of Jiangsu Provincial Key R&D Program (Grant No. BE2022071), the Natural Science Foundation of Jiangsu Province (Grant No. BK20192001), the National Natural Science Foundation of China (Grant No. 12074194), and the Postgraduate Research & Practice Innovation Program of Jiangsu Province (Grant No. KYCX220954).

References

[1] Bennett C H and Brassard G 2014 *Theoretical Computer Science* **560** 7
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Zhang C X, Wu D, Cui P W, *et al*. 2023 *Chin. Phys. B* **32** 124207
[4] Gottesman D, Lo H K, Lutkenhaus N and Preskill J 2004 *Quantum Inf. Comput.* **4** 325
[5] Qi B, Fung C H F, Lo H K and Ma X 2007 *Quantum Inf. Comput.* **7** 73
[6] Qi B, Fung C H F, Lo H K, *et al.* 2005 arXiv preprint quant-ph/0512080
[7] Kartalopoulos S V 2005 *MILCOM* **2005** 2788
[8] Brazaola-Vicario, Aitor, *et al*. 2024 *Opt. Commun.* **2024** 1438
[9] Laing A, Scarani V, Rarity J G, *et al*. 2010 *Phys. Rev. A* **82** 012304
[10] Wang C, Sun S H, Ma X C, *et al*. 2015 *Phys. Rev. A* **92** 042319
[11] Wang F, Zhang P, Wang X, *et al*. 2016 *Phys. Rev. A* **94** 062330
[12] Pramanik T, Park B K, Cho Y W, *et al*. 2017 *Phys. Rev. A* **381** 2497
[13] Liu H, Wang J, Ma H, *et al*. 2019 *Phys. Rev. Appl.* **12** 034039
[14] Zhou X Y, Ding H J, Sun M S, *et al*. 2021 *Phys. Rev. Appl.* **15** 064016
[15] Liu J Y, Zhou X Y, Zhang C H, *et al*. 2021 *J. Lightwave Technol.* **39** 5486
[16] Wei K J, Chen Z H, Li Z J, *et al*. 2022 *J. Opt. Soc. Am. B* **39** 3041
[17] Zhou C, Zhao Y M, Yang X L, *et al*. 2024 *Chin. Phys. B* **33** 080306
[18] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[19] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[20] Lo H K, Ma X F and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[21] Inoue K and Honjo T 2005 *Phys. Rev. A* **71** 042305
[22] Niederberger A, Scarani V and Gisin N. 2005 *Phys. Rev. A* **71** 042316
[23] Acin A, Gisin N and Scarani V 2004 *Phys. Rev. A* **69** 012309
[24] Wang X B 2007 *Phys. Rev. A* **75** 052301
[25] Wang X B, Peng C Z, Pan J W, *et al*. 2008 *Phys. Rev. A* **77** 042311
[26] Jiang C, Yu Z W, Hu X L, *et al.* 2023 *National Science Review* **10** nwac186
[27] Zhou Y H, Yu Z W and Wang X B 2014 *Phys. Rev. A* **89** 052325