

Reference-frame-independent quantum key distribution with two-way classical communication

Chun Zhou(周淳), Hai-Tao Wang(汪海涛), Yi-Fei Lu(陆宜飞), Xiao-Lei Jiang(姜晓磊), Yan-Mei Zhao(赵燕美), Yu Zhou(周雨), Yang Wang(汪洋), Jia-Ji Li(李家骥), Yan-Zang Zhou(周砚扬), Xiang Wang(汪翔), Hong-Wei Li(李宏伟), and Wan-Su Bao(鲍皖苏)

Citation: Chin. Phys. B, 2024, 33 (**10**): 100302. DOI: 10.1088/1674-1056/ad6a3d
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

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

Improved decoy-state quantum key distribution with uncharacterized heralded single-photon sources

Le-Chen Xu(徐乐辰), Chun-Hui Zhang(张春辉), Xing-Yu Zhou(周星宇), and Qin Wang(王琴)
Chin. Phys. B, 2024, 33 (**2**): 020313. DOI: 10.1088/1674-1056/ad062a

---

Reference-frame-independent quantum key distribution with two-way classical communication

Chun Zhou(周淳), Hai-Tao Wang(汪海涛)†, Yi-Fei Lu(陆宜飞), Xiao-Lei Jiang(姜晓磊), Yan-Mei Zhao(赵燕美), Yu Zhou(周雨), Yang Wang(汪洋), Jia-Ji Li(李家骥), Yan-Yang Zhou(周砚扬), Xiang Wang(汪翔)‡, Hong-Wei Li(李宏伟), and Wan-Su Bao(鲍皖苏)

Henan Key Laboratory of Quantum Information and Cryptography, SSF IEU, Zhengzhou 450001, *China*

(Received 22 May 2024; revised manuscript received 19 July 2024; accepted manuscript online 2 August 2024)

The data post-processing scheme based on two-way classical communication (TWCC) can improve the tolerable bit error rate and extend the maximal transmission distance when used in a quantum key distribution (QKD) system. In this study, we apply the TWCC method to improve the performance of reference-frame-independent quantum key distribution (RFI-QKD), and analyze the influence of the TWCC method on the performance of decoy-state RFI-QKD in both asymptotic and non-asymptotic cases. Our numerical simulation results show that the TWCC method is able to extend the maximal transmission distance from 175 km to 198 km and improve the tolerable bit error rate from 10.48% to 16.75%. At the same time, the performance of RFI-QKD in terms of the secret key rate and maximum transmission distance are still greatly improved when statistical fluctuations are considered. We conclude that RFI-QKD with the TWCC method is of practical interest.

Keywords: quantum key distribution, reference-frame-independent, two-way classical communication

PACS: 03.67.Dd, 03.67.Hk, 03.67.–a **DOI:** 10.1088/1674-1056/ad6a3d

1. Introduction

Quantum key distribution (QKD) provides information-theoretic security for legitimate communication between two parties, Alice and Bob, based on the basic principles of quantum mechanics.[1,2] Since Bennett and Brassard proposed BB84 protocol in 1984,[3] researchers have made significant efforts[4–9] to promote the development of QKD.

In most QKD systems, Alice and Bob need to share the reference frame to complete the correct encoding and decoding operation. However, due to the movement of the relative position of the communicating parties and the change of environment, the reference frame of the communicating parties will drift, causing large errors and reducing system performance. Therefore, the communication parties need to actively correct the reference frame to ensure the normal operation of the QKD system, such as the phase compensation in the phase encoding system or the correction of the polarization states in the polarization encoding system. In the practical point-to-point QKD system, especially in the QKD network with large-scale multi-user nodes, active correction of the reference frame will consume a lot of time and reduce the efficiency of the entire communication process. In addition, the device for correcting the reference frame will increase the complexity and cost of the QKD system, and may even bring potential security risks. Fortunately, reference-frame-independent QKD (RFI-QKD)[10] bypasses the requirement of reference frame alignment and can use an unknown and slowly drifting reference frame to generate keys better. The significant progresses[11–18] have been made in several aspects of the RFI-QKD.

The RFI-QKD protocol improves the stability of the system, but the transmission distance and secret key rate are still the key issues worth considering. In order to improve the maximum transmission distance and the tolerable bit error rate, the two-way classical communication (TWCC)[19,20] based on the entanglement distillation has been proposed, which plays a crucial role especially in the scenarios of high channel losses and system errors. The advantage distillation technology is also a kind of the TWCC method, which has been exploited to increase transmission distance.[21–24] Chau[25] further used the TWCC scheme to improve the tolerable bit error rate of the six-state QKD protocol. In 2006, Ma *et al.*[26] combined the TWCC method with the decoy-state method and provided an lower bound of the analytic key rate, which promoted the practical implementation of the TWCC method. In 2016, Tan *et al.*[27] gave the secret key rate formula of the MDI-QKD protocol on the TWCC method. In 2020, Xu *et al.*[28] proposed the active parity-pairing (AOPP) method on the TWCC theory, which effectively improved the secret key rate and maximal transmission distance of the sending-or-not-sending twin-field quantum key distribution (SNS TF-QKD) protocol. However, whether the TWCC method can improve the performance of RFI-QKD protocol is a problem which further worths exploring.

In this study, we improve the performance of RFI-QKD

†Corresponding author. E-mail: wht@qiclab.cn
‡Corresponding author. E-mail: dixonwx@163.com

© 2024 Chinese Physical Society and IOP Publishing Ltd

by exploiting the TWCC method. Based on the TWCC method, we analyze its influence on the performance of decoy-state RFI-QKD protocols in both asymptotic and nonasymptotic cases. The simulation results demonstrate that the proposed scheme extends the transmission distance from 175 km to 198 km in the asymptotic case. The maximum tolerable quantum bit error rate (QBER) of the proposed system is increased from 10.48% to 16.75%. Moreover, in order to make the RFI-QKD protocol more practical, we study the performance of the RFI-QKD protocol with TWCC when considering statistical fluctuations. Under the condition of the nonasymptotic case, the simulation results show that the TWCC method can improve the secret key rate and maximum transmission distance, and make the system more tolerant to the bit error rate. Notably, the TWCC method only modifies the classical postprocessing step without changing the hardware of a realistic RFI-QKD system and can be directly applied to current RFI-QKD systems.

This paper is arranged as follows: in Section 2, we propose the security analysis of RFI-QKD with TWCC. In Section 3, we combine the TWCC method with decoy-state RFI-QKD. We use the TWCC method to conduct the statistical fluctuation in the decoy-state RFI-QKD. In Section 4, the numerical simulation and discussion is given. Finally, the conclusion is given in Section 5.

2. RFI-QKD with TWCC

Firstly, we briefly review the RFI-QKD protocol and perform security analysis. Define the three Pauli matrices $\{\sigma_X,\sigma_Y,\sigma_Z\}$ as $\{X,Y,Z\}$ respectively. In RFI-QKD, it is assumed that the Z basis remains well aligned at Alice's end and Bob's end, that is, $Z_{\rm A}=Z_{\rm B}$, while the X basis and Y basis may change slowly over time in the quantum channel. Therefore, the other two sets of encoding basis between Alice and Bob have the following relationship:

$$\begin{aligned} X_{\rm B}&=\cos\beta X_{\rm A}+\sin\beta Y_{\rm A},\\ Y_{\rm B}&=\cos\beta Y_{\rm A}-\sin\beta X_{\rm A}, \end{aligned} \tag{1}$$

where β represents the drift amount of the reference frame between the X basis and Y basis of the communicating parties, which changes slowly with time.[10] The value of β can be measured experimentally, but Alice and Bob do not need to measure the value of β in the RFI-QKD protocol, which means that the value of β is unknown to Alice and Bob.

Alice and Bob share a pair of entangled states, which are ideally Bell states $|\phi^+\rangle=|00\rangle+|11\rangle/\sqrt{2}$, they randomly choose one basis to measure the quantum signal, and then announce their chosen basis in the classic channel. Both parties use the Z basis to generate the raw key, the corresponding quantum bit error rate (QBER) is given as follows:[10]

$$Q=\frac{1-\langle Z_{\rm A}Z_{\rm B}\rangle}{2}. \tag{2}$$

The event where both of them select X and Y bases is used to estimate Eve's information, and we can define the intermediate quantity[10]

$$C=\langle X_{\rm A}X_{\rm B}\rangle^2+\langle X_{\rm A}Y_{\rm B}\rangle^2+\langle Y_{\rm A}X_{\rm B}\rangle^2+\langle Y_{\rm A}Y_{\rm B}\rangle^2, \tag{3}$$

which is independent of β according to Eq. (1). The maximum value of C is 2 and the value of Q is 0. At this time, there are no eavesdroppers and other system errors, and the two qubits are maximum entangled state.

In this study, we focus on the entanglement-based version of RFI-QKD. First, we assume that Alice and Bob share the two-qubit quantum state $\rho_{\rm AB}$. Without loss of generality, it is considered that $\rho_{\rm AB}$ is known to Eve and can be expressed as a diagonalization matrix of Bell states. We find that C is invariant when making the transformation $X_{\rm A}\to -X_{\rm A}$, $Y_{\rm A}\to -Y_{\rm A}$, $X_{\rm B}\to -X_{\rm B}$, $Y_{\rm B}\to -Y_{\rm B}$. This transformation can be implemented on $\rho_{\rm AB}$ itself by the unitary $Z_{\rm A}Z_{\rm B}$. Therefore, there is no limit to replacing $\rho_{\rm AB}$ with $\tilde{\rho}_{\rm AB}=(\rho_{\rm AB}+Z_{\rm A}Z_{\rm B}\rho_{\rm AB}Z_{\rm A}Z_{\rm B})/2$ for analysis, and Eve can obtain the same information from $\rho_{\rm AB}$ and $Z_{\rm A}Z_{\rm B}\rho_{\rm AB}Z_{\rm A}Z_{\rm B}$. As for Alice and Bob, they will not be affected in any way since they only focus on the values of Q and C. Thus, we can obtain[10]

$$\begin{aligned} \tilde{\rho}_{\rm AB}=&\mu_1P_{\Phi^+}+\mu_2P_{\Phi^-}+\left(\frac{a}{2}|\Phi^-\rangle\langle\Phi^+|+{\rm H.c.}\right)\\ &+\mu_3P_{\psi^+}+\mu_4P_{\psi^-}+\left(\frac{b}{2}|\psi^-\rangle\langle\psi^+|+{\rm H.c.}\right), \end{aligned} \tag{4}$$

where $P_\psi=|\psi\rangle\langle\psi|$ and four states represent the usual Bell bases. Due to symmetry, $\tilde{\rho}_{\rm AB}(a,b)$ and $\tilde{\rho}_{\rm AB}(-a^*,-b^*)$ have the same value of C, then one can get $\rho'=\frac{1}{2}[\tilde{\rho}(a,b)+\tilde{\rho}(-a^*,b^*)]=\tilde{\rho}({\rm i}A,{\rm i}B)$, with $A={\rm Im}(a)$, $B={\rm Im}(b)$. The Bell state diagonalization expansion can be given as follows:[10]

$$\rho'_{\rm AB}=\sum_{k=1}^{4}\lambda_k|\Phi_k\rangle\langle\Phi_k|, \tag{5}$$

where

$$|\Phi_{1(2)}\rangle=\frac{{\rm e}^{{\rm i}\chi}|00\rangle\pm{\rm e}^{-{\rm i}\chi}|11\rangle}{\sqrt{2}},\ |\Phi_{3(4)}\rangle=\frac{{\rm e}^{{\rm i}\chi'}|01\rangle\pm{\rm e}^{-{\rm i}\chi'}|10\rangle}{\sqrt{2}}.$$

Define

$$A'=\sqrt{(\mu_1-\mu_2)^2+A^2},\quad B'=\sqrt{(\mu_3-\mu_4)^2+B^2},$$

then

$$\begin{aligned} \lambda_{1(2)}&=\frac{(\mu_1+\mu_2\pm A')}{2},\ \cos^2\chi=\frac{1}{2}+\frac{\mu_1-\mu_2}{A'},\\ \lambda_{3(4)}&=\frac{(\mu_3+\mu_4\pm B')}{2},\ \cos^2\chi'=\frac{1}{2}+\frac{\mu_3-\mu_4}{B'}. \end{aligned}$$

In this case, C has the same value as previous report and now can be expressed as[10]

$$C=2[(\lambda_1-\lambda_2)^2+(\lambda_3-\lambda_4)^2], \tag{6}$$

where $\{\lambda_1,\lambda_2,\lambda_3,\lambda_4\}$ are constrained by the following three conditions: $\sum_{i=1}^{4}\lambda_i=1$ and the practical measured values of Q and C can be obtained, and one of the free variables can get Eve's information maximum. Here, two parameters u and v can be introduced to represent the above constraints. According to the first two constraints, the expression of four parameters can be obtained as follows:[10]

$$\lambda_1=(1-Q)\frac{1+u}{2},\quad \lambda_2=(1-Q)\frac{1-u}{2},$$
$$\lambda_3=Q\frac{1+v}{2},\quad \lambda_4=Q\frac{1-v}{2}. \tag{7}$$

In this case, the information obtained by Eve can be expressed as[10]

$$I_{\mathrm{E}}(Q,u,v)=(1-Q)H\Big(\frac{1+u}{2}\Big)+QH\Big(\frac{1+v}{2}\Big), \tag{8}$$

where $H(x)=-x\log_2 x-(1-x)\log_2(1-x)$ is the binary entropy function. To obtain the security key rate of the RFI-QKD protocol, we need to consider the worst case, that is, consider the maximum value of Eve information $I_{\mathrm{E}}(0,C)=H[(1+\sqrt{C/2})/2]$. For $Q>0$, $v(u)=\sqrt{C/2-(1-Q)^2u^2}/Q$ and $u\in[u_{\min},u_{\max}]$, where $u_{\min}=\frac{1}{1-Q}\sqrt{\max[\frac{C}{2}-Q^2,0]}$ and $u_{\max}=\min[\frac{1}{1-Q}\sqrt{\frac{C}{2}},1]$. Therefore, the secret key rate formula can be written as

$$\begin{aligned}R&\geq\min_{\{\lambda_1,\lambda_2,\lambda_3,\lambda_4\}}[S(A|E)-H(A|B)]\\&=\min_{\{\lambda_1,\lambda_2,\lambda_3,\lambda_4\}}[1-H(A|B)-I_{\mathrm{E}}(Q,u,v)].\end{aligned} \tag{9}$$

We can get from Eq. (7) that $u=\frac{\lambda_1-\lambda_2}{\lambda_1+\lambda_2}$, $v=\frac{\lambda_3-\lambda_4}{\lambda_3+\lambda_4}$. Then, we can derive $v(u)=\frac{1}{\lambda_3+\lambda_4}\sqrt{\frac{C}{2}-(\lambda_1-\lambda_2)^2}$, $u_{\min}=\frac{1}{\lambda_1+\lambda_2}\sqrt{\max[\frac{C}{2}-(\lambda_3+\lambda_4)^2,0]}$ and $u_{\max}=\min[\frac{1}{\lambda_1+\lambda_2}\sqrt{\frac{C}{2}},1]$.

Next, we briefly introduce the TWCC method. The two-way classical communication consists of a series of B steps and P steps. In the B step, Alice and Bob perform a bilateral XOR (BXOR) operation between EPR pairs and measure the target qubits in the Z basis. If Alice's and Bob's measurement outcomes disagree, they discard the remaining EPR pair; otherwise, they keep the control qubit. In the P step, Alice and Bob group the EPR pairs into three sets, and measure X_1X_2 and X_1X_3 on each set. If Alice and Bob disagree on one measurement, Bob concludes that the phase error was probably on one of the EPR pairs which was measured and does nothing; if both measurements disagree for Alice and Bob, Bob assumes that the phase error was on the surviving EPR pair and corrects it by performing a Z operation. However, the P step is proved to be less useful than the B step when it came to contributing to the key generation rate. In the following, we consider only using the B step when performing two-way classical communication.

Finally, we consider applying the TWCC method to the RFI-QKD protocol. This is shown in Fig. 1. The TWCC method only changes the postprocessing steps. The only change is in the postprocessing procedure of the original RFI-QKD. The specific details are presented in the following. Alice and Bob divide their raw key into blocks of 2 bits $\{x_1,x_2\}$ and $\{y_1,y_2\}$, and calculate the parity of each pair of bits, $x_1\oplus x_2$ and $y_1\oplus y_2$. Afterwards, both Alice and Bob announce the parities. If their parities are the same, they retain x_1 and y_1 as the original key; otherwise, discard x_1, x_2, y_1 and y_2. Finally, Alice and Bob perform error correction and privacy amplification on the original key to extract the secret key. After the two-way classic communication, the survival probability p_{S} is given by

$$p_{\mathrm{S}}=(1-Q)^2+Q^2. \tag{10}$$

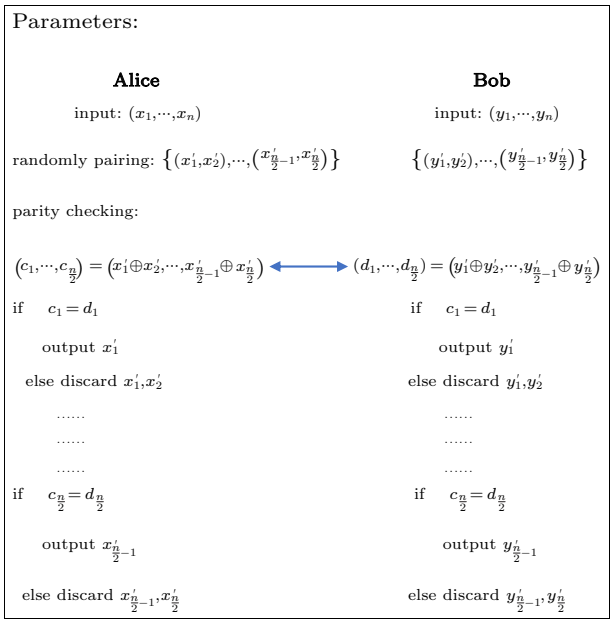


Fig. 1. Classical description of the TWCC method in RFI-QKD.

After the two-way classical communication between Alice and Bob, the QBER Q' can be changed from Q to

$$Q'=\frac{Q^2}{p_{\mathrm{S}}}, \tag{11}$$

and then the quantum state shared by Alice and Bob can be expressed as

$$\rho_{\mathrm{AB}}''=\sum_{i=1}^{4}\lambda'_k|\Phi_i\rangle\langle\Phi_i|, \tag{12}$$

where

$$\lambda_1'=\frac{\lambda_1^2+\lambda_2^2}{p_{\mathrm{S}}},\quad \lambda_2'=\frac{\lambda_3^2+\lambda_4^2}{p_{\mathrm{S}}},$$
$$\lambda_3'=\frac{2\lambda_3\lambda_4}{p_{\mathrm{S}}},\quad \lambda_4'=\frac{2\lambda_1\lambda_2}{p_{\mathrm{S}}}.$$

What's more, we put these coefficients into the expression of the intermediate quantities C, u, and v, which can be modified

to

$$
\begin{aligned}
&C' = 2[(\lambda'_1-\lambda'_2)^2+(\lambda'_3-\lambda'_4)^2],\\
&v'(u) = \frac{1}{\lambda'_3+\lambda'_4}\sqrt{\frac{C'}{2}-(\lambda'_1-\lambda'_2)^2},\\
&u'_{\min} = \frac{1}{\lambda'_1+\lambda'_2}\sqrt{\max[\frac{C'}{2}-(\lambda'_3+\lambda'_4)^2,\ 0]},\\
&u'_{\max} = \min\left[\frac{1}{\lambda'_1+\lambda'_2}\sqrt{\frac{C'}{2}},\ 1\right].
\end{aligned}
\tag{13}
$$

Lastly, the key rate formula of RFI-QKD based on the TWCC method can be expressed as

$$
\begin{aligned}
R &\geq \min_{\{\lambda_1,\lambda_2,\lambda_3,\lambda_4\}} \frac{1}{2}p_{\rm S}[S'(A|E)-H'(A|B)]\\
&= \min_{\{\lambda_1,\lambda_2,\lambda_3,\lambda_4\}} [1-H'(A|B)-I_{\rm E}(Q',u',v')].
\end{aligned}
\tag{14}
$$

3. Decoy state RFI-QKD with TWCC

Next, we combine TWCC with the decoy-state method to perform security analysis on decoy-state RFI-QKD. Due to the lack of ideal single-photon source in the practical QKD system, we usually combine the weak coherent state (WCS) with the decoy-state method in the practical RFI-QKD system. Thus, we focus on the three-intensity decoy state scheme,[29] and give the decoy-state RFI-QKD protocol with TWCC as follows:

Step 1 Quantum state preparation. Alice randomly selects an intensity $l_a \in \{u_a, v_a, w_a\}$ to prepare a phase-randomized weak coherent state $|{\rm e}^{{\rm i}\theta_{\rm A}}\sqrt{l_a}\rangle_x$ with $\theta_{\rm A}\in[0,2\pi)$. Then Alice randomly chooses a basis $\zeta_{\rm A}\in\{X_{\rm A},Y_{\rm A},Z_{\rm A}\}$ and a bit $m_a\in\{0,1\}$ to prepare the corresponding quantum state, and sends it to Bob through the quantum channel. The prepared quantum state is related to the specific coding method. Here, we consider to use polarization coding. There are three groups of bases and two bits corresponding to six states $\{|H\rangle,|V\rangle,|+\rangle,|-\rangle,|+{\rm i}\rangle,|-{\rm i}\rangle\}$. For example, when Alice chooses the Z basis and 0 bit, she can prepare a quantum state $|{\rm e}^{{\rm i}\theta_{\rm A}}\sqrt{l_a}\rangle_H$ by polarization encoding.

Step 2 Measurement and announcement. Bob randomly chooses a basis $\zeta_{\rm B}\in\{X_{\rm B},Y_{\rm B},Z_{\rm B}\}$ to measure the received light pulse. Alice then publicly announces her basis and intensity information, and Bob publicly announces her (his) basis information through the authenticated classic channel.

Step 3 Basis sifting. After Alice and Bob publicly exchange the basis information, they retain the events with the basis combination $\{X_{\rm A}X_{\rm B},X_{\rm A}Y_{\rm B},Y_{\rm A}X_{\rm B},Y_{\rm A}Y_{\rm B}\}$.

Step 4 Parameter estimation. Alice and Bob use the Z basis to generate a key. They apply the decoy-state method to estimate the lower bound of single-photon counting rates Y_1 and the upper bound of Eve's information $I_{\rm E}^U$.

Step 5 Two-way classical communication. Alice and Bob apply the TWCC method on the sifted key to extract highly correlated raw key, and then calculate the bit errors, residuals of untagged bits, and other variables. However, the two-way classical communication may be omitted if the QBER is small in practical QKD systems, where the TWCC method may have no advantage in improving the performance of QKD systems.

Step 6 Postprocessing. Alice and Bob perform error correction and privacy amplification on the raw key data to extract the final secret key.

Since all errors in the post-processing step must be corrected by Alice and Bob, $H'(A|B)$ can be expressed as $H'(A|B)\leq fH(E')$, where $E'=\frac{E^2}{E^2+(1-E)^2}$ is the total bit error rate after the two-way classical communication step, f is the error correction efficiency. Since Eve can obtain all the classical information in the classical channel, this represents the maximum information that Eve can steal in the error correction process. Therefore, the secret key rate of the decoy-state RFI-QKD protocol combined with two-way classic communication can be given as follows:

$$
\begin{aligned}
R \geq \min_{\lambda_1,\lambda_2,\lambda_3,\lambda_4} & r'_{\rm B}Q_{u_a}^{Z_{\rm A}Z_{\rm B}}\Big\{\Omega'\Big[1-(\lambda'_1+\lambda'_2)H\Big(\frac{1+u'}{2}\Big)\\
&-(\lambda'_3+\lambda'_4)H\Big(\frac{1+v'}{2}\Big)\Big]-fH(E')\Big\},
\end{aligned}
\tag{15}
$$

where E' is the overall bit error rate, $r'_{\rm B}$ is the overall survival residue, Ω' is the fraction of untagged states in the final survival states, and $Q_{u_a}^{Z_{\rm A}Z_{\rm B}}$ is the overall gain of Alice sending out state with u_a intensity and the $Z_{\rm A}Z_{\rm B}$ basis combination after a sequence of B steps. In the following, we will show how these variables change on performing B steps.

Firstly, we consider how the fraction of untagged states Ω, the bit error rate of the overall surviving state E, the bit error rate of the untagged states $E_{\rm untagged}$ are transformed after performing a B step. Before performing one B step, the fraction of the untagged states is $\Omega=\frac{Q_1^{Z_{\rm A}Z_{\rm B}}}{Q_{u_a}^{Z_{\rm A}Z_{\rm B}}}$ ($Q_{u_a}^{Z_{\rm A}Z_{\rm B}}$ is the number of successful measurement events in which Alice sends a single photon state under the $Z_{\rm A}Z_{\rm B}$ basis combination), the overall QBER is E, the bit error rate of the untagged states is $E_{\rm untagged}$. In addition, the overall survival probability $p_{\rm S}$ and the survival probability of the untagged states $p_{\rm S}^{\rm untagged}$ after one B step are given by[20]

$$
\begin{aligned}
&p_{\rm S} = (1-E)^2+E^2,\\
&p_{\rm S}^{\rm untagged} = [E_{\rm untagged}^2+(1-E_{\rm untagged})^2].
\end{aligned}
\tag{16}
$$

Then the residue after one B step is given as follows:

$$
r'_{\rm B} = \frac{1}{2}p_{\rm S},
\tag{17}
$$

where the $1/2$ is due to the fact that Alice and Bob keep only one qubit from a survival pair. Then, after one B step, the fraction of untagged states Ω', the overall bit error rate E',

the bit error rate of the untagged states E'_{untagged}, parameter $\{\lambda_1,\lambda_2,\lambda_3,\lambda_4\}$ and parameter C are given by

$$\Omega' = \frac{\Omega^2 P_{\text{S}}^{\text{untagged}}}{p_{\text{S}}}, \tag{18}$$

$$E' = \frac{E^2}{(1-E)^2+E^2}, \tag{19}$$

$$E'_{\text{untagged}} = \frac{E^2_{\text{untagged}}}{E^2_{\text{untagged}}+(1-E_{\text{untagged}})^2}, \tag{20}$$

$$C' = 2[(\lambda'_1-\lambda'_2)^2+(\lambda'_3-\lambda'_4)^2]. \tag{21}$$

In practical QKD systems, only a finite number of signals are transmitted. Thus there are certain statistical fluctuations in the parameter estimations (our analysis only contain statistical fluctuation, but the full finite-key analysis is not contained). Then, we can apply TWCC for statistical fluctuation analysis. In the non-asymptotic case, the secret key rate with decoy-state RFI-QKD can be given by

$$\tilde{R} \geq \min_{\lambda_1,\lambda_2,\lambda_3,\lambda_4} \frac{1}{N} r'_{\text{B}} N_{u_a}^{Z_{\text{A}}Z_{\text{B}}} \Big\{ \Omega' \Big(1-(\lambda'_1+\lambda'_2) H\Big(\frac{1+u'}{2}\Big) - (\lambda'_3+\lambda'_4) H\Big(\frac{1+v'}{2}\Big)\Big) - f H(E') \Big\}, \tag{22}$$

where N is the total number of emitted pulses, $N_{u_a}^{Z_{\text{A}}Z_{\text{B}}}$ is the total number of detection counts of Alice sending the state in the $Z_{\text{A}}Z_{\text{B}}$ basis combination with intensity u_a, and $n_1^{Z_{\text{A}}Z_{\text{B}}}$ is the number of successful measurement events in which Alice sent the single-photon state in the $Z_{\text{A}}Z_{\text{B}}$ basis combination.

Based on the decoy-state method, we can derive the lower bound of the single photon events $n_1^{Z_{\text{A}}Z_{\text{B}},L}$ and the upper bound of the corresponding bit error rate $e_1^{Z_{\text{A}}Z_{\text{B}},U}$ of the RFI-QKD protocol:

$$\begin{aligned} n_1^{Z_{\text{A}}Z_{\text{B}}} \geq n_1^{Z_{\text{A}}Z_{\text{B}},L} = {} & \frac{u_a\tau_1}{(v_a-w_a)(u_a-v_a-w_a)} \\ & \times \Big[\frac{u_a^2-{w_a}^2-v_a w_a}{u_a^2} \frac{e^{v_a} n_{v_a}^{Z_{\text{A}}Z_{\text{B}},U}}{p_{v_a}} \\ & - \frac{{u_a}^2-{v_a}^2-v_a w_a}{u_a^2} \frac{e^{v_a} n_{w_a}^{Z_{\text{A}}Z_{\text{B}},L}}{p_{w_a}} \\ & - \frac{{v_a}^2-{w_a}^2}{u_a^2} \frac{e^{u_a} n_{v_a}^{Z_{\text{A}}Z_{\text{B}},U}}{p_{u_a}} \Big], \end{aligned} \tag{23}$$

$$\begin{aligned} e_1^{Z_{\text{A}}Z_{\text{B}}} \leq e_1^{Z_{\text{A}}Z_{\text{B}},U} = {} & \frac{\tau_1}{(v_a-w_a) n_1^{Z_{\text{A}}Z_{\text{B}},L}} \\ & \times \Big[\frac{\text{e}^{v_a} m_{v_a}^{Z_{\text{A}}Z_{\text{B}},U}}{p_{v_a}} - \frac{\text{e}^{w_a} m_{w_a}^{Z_{\text{A}}Z_{\text{B}},L}}{p_{w_a}} \Big], \end{aligned} \tag{24}$$

where τ_1 is the probability that Alice prepares a single photon state, $n_\alpha^{Z_{\text{A}}Z_{\text{B}}}$ is the total number of detections when Alice sends the state with intensity α under the $Z_{\text{A}}Z_{\text{B}}$ basis combination, $m_\alpha^{Z_{\text{A}}Z_{\text{B}}}$ is the total number of errors when Alice sends the state with intensity α under the $Z_{\text{A}}Z_{\text{B}}$ basis combination, and p_α is the probability of Alice's modulation intensity α.

For a limited number of samples, if we adopt the improved Chernoff bound[30,31] to analyze the statistical fluctuations of independent random samples, the relationship between the observed value n_α^{d} and the expected value $\langle n_\alpha^{\text{d}}\rangle$ is expressed as

$$\langle n_\alpha^{\text{d,U}}\rangle = \frac{n_\alpha^{\text{d}}}{1-\delta_{\text{U}}}, \quad \langle n_\alpha^{\text{d,L}}\rangle = \frac{n_\alpha^{\text{d}}}{1+\delta_{\text{L}}} \tag{25}$$

under the condition that the failure probability is at least $1-2\xi$, the values δ_{U} and δ_{L} can be obtained by solving the equation

$$\Big[\frac{\text{e}^{-\delta_{\text{U}}}}{(1-\delta_{\text{U}})^{1-\delta_{\text{U}}}}\Big]^{X/(1-\delta_{\text{U}})} = \xi = \Big[\frac{\text{e}^{\delta_{\text{L}}}}{(1+\delta_{\text{L}})^{1+\delta_{\text{L}}}}\Big]^{X/(1+\delta_{\text{L}})}. \tag{26}$$

Thus, we can get the upper bound and lower bound of $\langle n_\alpha^{\text{d}}\rangle$. In the same way, the upper and lower bounds of $\langle m_\alpha^{\text{d}}\rangle$ can also be obtained. Finally, we can obtain the lower bound of final key rate of the decoy state RFI-QKD combining with the above formula.

4. Numerical simulation

In this section, we simulate the impact of the TWCC method on the performance of decoy state RFI-QKD under asymptotic and non-asymptotic conditions. We set the experimental parameters and analyze the experimental results. First, we define $\eta = 10^{-\gamma L/10}$ as the fiber transmittance, where γ is the fiber loss coefficient (dB/km), η_{d} is the single-photon detector efficiency, and p_{d} is the detector dark count. The failure probability of statistical fluctuation analysis is fixed as $\xi = 1\times10^{-10}$, f is the error correction efficiency, and β is the reference frame deviation. The practical parameters[32,33] for all numerical simulations used by us are listed in Table 1.

Table 1. Simulation parameters.

Variable	Parameter	Simulation value
γ	fiber loss coefficient	0.2 dB/km
η_{d}	single-photon detector efficiency	0.145
e_{d}	intrinsic misalignment error	3.3%
f	error correction efficiency	1.22
p_{d}	dark count rate	10^{-7}
ξ	failure probability of statistical fluctuations analysis	10^{-10}

As illustrated in Fig. 2, we demonstrate the impact of the TWCC method on the performance of decoy-state RFI-QKD in the asymptotic case. The blue solid line corresponds to the results with the TWCC method, and the orange solid line corresponds to the results without the TWCC method. And we find that the maximal transmission distance can be improved from 175 km to 198 km, the maximal tolerable background error rate e_{d} can be improved from 10.48% to 16.75%, and the maximal transmission distance can be improved from 0 km to

167 km when $e_{\rm d} = 10.49\%$. The simulation results show that the TWCC method can significantly improve the performance of decoy state RFI-QKD.

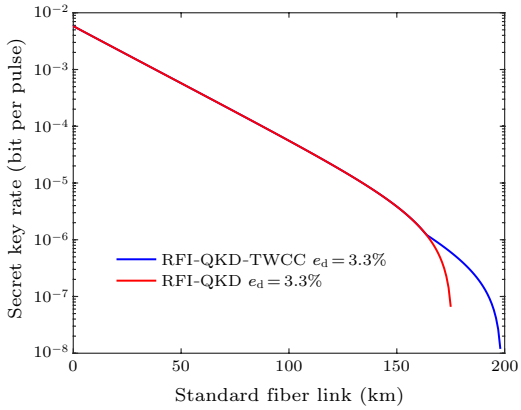


Fig. 2. Performance comparison between the proposed scheme (RFI-QKD-TWCC) and the original RFI-QKD scheme and the relationship between the optimal key rates (per pulse) and the transmission distance assuming $e_{\rm d} = 3.3\%$ in the asymptotic case. The blue solid line represents the secret key rate of the proposed scheme, the orange solid line represents the secret key rate of the original RFI-QKD scheme.

Furthermore, as shown in Fig. 3, we analyze the impact of the TWCC method on decoy state RFI-QKD for the non-asymptotic case. Here we set the total number of transmitted pulses $N = 10^{13}$ and the reference frame deviation $\beta = 0,\ \pi/9,\ \pi/6$. And it can be seen from Fig. 3 that the maximum transmission distance is increased from 173 km to 191 km, from 162 km to 186 km, and from 143 km to 178 km respectively, when $\beta = 0,\ \pi/9,\ \pi/6$.

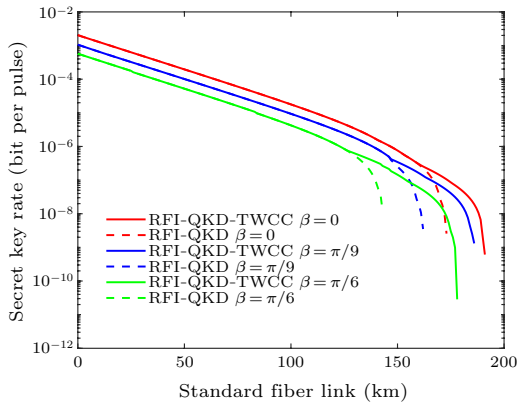


Fig. 3. Performance of the proposed scheme corresponding to different β. Relationship between the secret key rate and the total transmission distance corresponding to different β. The solid lines and dotted lines of different colors represent the performances of the proposed scheme and the original RFI-QKD corresponding to different β.

To further analyze the improvement effect of the TWCC method on the decoy state RFI-QKD protocol for the non-asymptotic case, we consider the statistical fluctuation based on the improved Chernoff bound. We set the reference frame deviation $\beta = \pi/12$ and different total number of transmission pulses $N = 10^{11}, 10^{12}, 10^{13}$. As shown in Fig. 4 the maximum transmission distance is increased from 140 km to 167 km, from 161 km to 182 km, and from 170 km to 192 km, respectively. This observation results implies that TWCC can still improve the key rate and transmission distance under statistical fluctuation conditions.

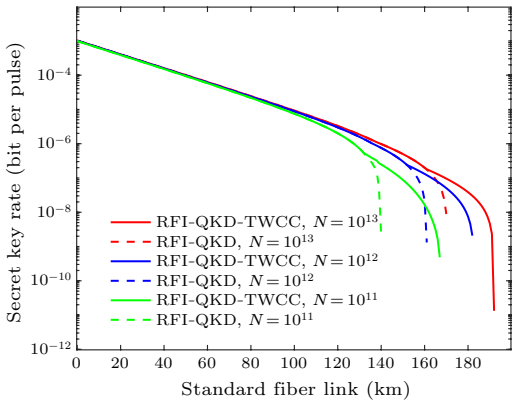


Fig. 4. Relationship between the secret key rate and the total transmission distance with and without the TWCC method corresponding to different $N = 10^{11}, 10^{12}, 10^{13}$ for $\beta = \pi/12$. The solid lines and dotted lines of different colors represent the performances of the proposed scheme and the original RFI-QKD corresponding to different N.

In the end, we study the effect of misalignment error $e_{\rm d}$ on the performance of the proposed scheme, and the results are shown in Fig. 5. When $e_{\rm d} = 1\%$ ($e_{\rm d} = 4\%$, $e_{\rm d} = 6\%$), the transmission distance of the proposed scheme increases by 18 km (25 km, 33 km). The simulation results demonstrate that, as the system misalignment error increases, the distance extension of the scheme with the TWCC method also increases.

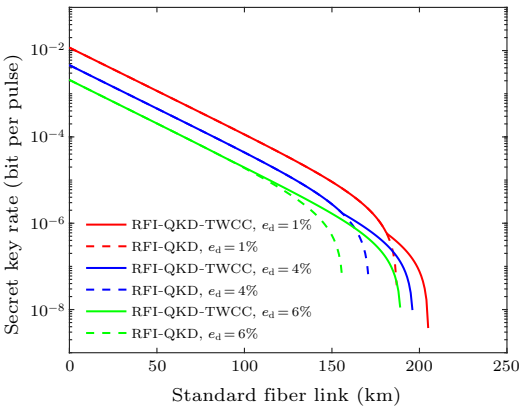


Fig. 5. Performance of the proposed scheme corresponding to different $e_{\rm d}$. Relationship between the secret key rate and the total transmission distance corresponding to different $e_{\rm d}$. The solid lines and dotted lines of different colors represent the performances of the proposed scheme and the original RFI-QKD corresponding to different $e_{\rm d}$.

5. Conclusion

In summary, this study applies the TWCC method to RFI-QKD and analyzes the impact of the TWCC method on the performance of decoy-state RFI-QKD. The analysis results reveal that the TWCC method can significantly improve the maximum transmission distance and tolerable bit error rate of decoy-state RFI-QKD. We find that the TWCC method can still improve the performance of decoy-state RFI-QKD when reference frame deviation changes, statistical fluctuations and misalignment error are considered in the non-asymptotic case.

Thus, the combination of TWCC and RFI-QKD protocols enhances the robustness of the QKD system. More importantly, the TWCC method does not change the quantum process of the RFI-QKD protocol, it only needs to adjust the classical post-processing process. Thus, it can be applied to existing RFI-QKD systems easily to improve their performance. We hope that our study can promote applications of the TWCC method in different QKD systems in the future research.

Acknowledgments

The project was supported by the National Natural Science Foundation of China (Grant Nos. 61505261, 62101597, 61605248, and 61675235), the National Key Research and Development Program of China (Grant No. 2020YFA0309702), the China Postdoctoral Science Foundation (Grant No. 2021M691536), the Natural Science Foundation of Henan Province (Grant Nos. 202300410534 and 202300410532), and the Anhui Initiative in Quantum Information Technologies.

References

[1] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[2] Xu F H, Ma X F, Zhang Q, Lo H K and Pan J W 2020 *Rev. Mod. Phys.* **92** 025002
[3] Bennett C H and Brassard G 1984 *Quantum cryptography: Public key distribution and coin tossing* (New York: IEEE) p. 175
[4] Boaron A, Boso G, Rusca D, *et al.* 2018 *Phys. Rev. Lett.* **121** 190502
[5] Comandar L, Lucamarini M, Fröhlich B, *et al.* 2016 *Nat. Photon.* **10** 312
[6] Wang S, Yin Z Q, He D Y, *et al.* 2022 *Nat. Photon.* **16** 154
[7] Fan-Yuan G J, Lu F Y, Wang S, *et al.* 2022 *Optica* **9** 812
[8] Han Y X, Sun Z Q, Dou T Q, Wang J P, Li Z H, Huang Y Q, Li P Y and Ma H Q 2022 *Chin. Phys. Lett.* **39** 070301
[9] Zhang C X, Wu D, Cui P W, Ma J C, Wang Y and An J M 2023 *Chin. Phys. B* **32** 124207
[10] Laing A, Scarani V, Rarity J G and O'Brien J L 2010 *Phys. Rev. A* **82** 012304
[11] Liang W Y, Wang S, Li H W, *et al.* 2014 *Sci. Rep.* **4** 3617
[12] Wang C, Sun S H, Ma X C, Tang G Z and Liang L M 2015 *Phys. Rev. A* **92** 042319
[13] Wang F M, Zhang P, Wang X L and Li F L 2016 *Phys. Rev. A* **94** 062330
[14] Liu H W, Wang J P, Ma H Q and Sun S H 2019 *Phys. Rev. Appl* **12** 034039
[15] Zhang C M, Wang W B, Li H W and Wang Q 2019 *Opt. Lett.* **44** 1226
[16] Sun S H 2021 *Phys. Rev. A* **104** 022423
[17] Zhu J R, Wang R and Zhang C M 2022 *Opt. Lett.* **47** 4219
[18] Wang J P, Liu H W, Ma H Q and Sun S H 2019 *Phys. Rev. A* **99** 032309
[19] Bae J, Acín, A 2007 *Phys. Rev. A* **75** 012334
[20] Gottesman D and Lo H K 2003 *IEEE Trans. Inf. Theory* **49** 457
[21] Li H W, Zhang C M, Jiang M S and Cai Q Y 2022 *Commun. Phys.* **5** 53
[22] Jiang X L, Wang Y, Li J J, *et al.* 2023 *Opt. Express* **31** 9196
[23] Liu X, Luo D, Zhang Z R and Wei K J 2023 *Phys. Rev. A* **107** 062613
[24] Wang R Q, Zhang C M, Yin Z Q, *et al.* 2023 *New J. Phys.* **24** 073049
[25] Chau H F 2002 *Phys. Rev. A* **66** 060302
[26] Ma X F, Fung C H F, Dupuis F, Chen K, Tamaki K and Lo H K 2006 *Phys. Rev. A* **74** 032330
[27] Tan Y G and Liu Q 2016 *Chin. Phys. Lett.* **33** 090303
[28] Xu H, Yu Z W, Jiang C, Hu X L and Wang X B 2020 *Phys. Rev. A* **101** 042330
[29] Ma X F, Qi B, Zhao Y and Lo H K 2005 *Phys. Rev. A* **72** 012326
[30] Chernoff H 1952 *Ann. Math. Stat.* **23** 493
[31] Zhang Z, Zhao Q, Razavi M and Ma X F 2017 *Phys. Rev. A* **95** 012333
[32] Gobby C, Yuan Z L and Shields A J 2004 *Appl. Phys. Lett.* **84** 3762
[33] Xu F H, Xu H and Lo H K 2014 *Phys. Rev. A* **89** 052333