Practical reference-frame-independent quantum key distribution systems against the worst relative rotation of reference frames

Chun-Mei Zhang, Jian-Rong Zhu and Qin Wang
1 Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing, 210003, People’s Republic of China
2 Key Lab of Broadband Wireless Communication and Sensor Network Technology, Nanjing University of Posts and Telecommunications, Ministry of Education, Nanjing, 210003, People’s Republic of China
E-mail: qinw@njupt.edu.cn

Keywords: reference-frame-independent, quantum key distribution, decoy state, relative rotation

Abstract
Reference-frame-independent quantum key distribution (RFI-QKD) can generate secret keys with the slow drift of reference frames. However, the performance of practical RFI-QKD systems deteriorates with the increasing drift of reference frames. In this paper, we mathematically demonstrate the worst relative rotation of reference frames for practical RFI-QKD systems and investigate the corresponding performance with optimized system parameters. Simulation results show that practical RFI-QKD systems can achieve quite good performance against the worst relative rotation of reference frames, which exhibit the feasibility of practical QKD systems with free drifting reference frames. Furthermore, we propose a universal estimation method of the secret key rate in practical RFI-QKD systems, which conforms to the nature of RFI-QKD more well than the usual estimation method.

1. Introduction

Based on the theory of quantum physics, quantum key distribution (QKD) [1] provides a way of generating information-theoretic secure keys between two distant parties Alice and Bob, even in the presence of a malicious eavesdropper Eve. Since the first Bennett-Brassard-1984 (BB84) protocol was proposed in 1984, a series of works have been made to improve the practical performance of QKD systems [2–14]. Generally, in most of these systems, the complicated and real-time operation of calibrating reference frames is indispensable to assure the regular running of practical QKD systems [4, 11–14]. However, the calibration of reference frames may complicate QKD systems and reduce key generation rates.

Fortunately, reference-frame-independent QKD (RFI-QKD) [15] can bypass the calibration of reference frames and generate secret keys with the slow drift of reference frames. In RFI-QKD, Alice (Bob) adopts three orthogonal bases $Z$, $X$, and $Y$ to encode (decode) quantum states, and her (his) local bases are denoted as $Z_{A(B)}$, $X_{A(B)}$, and $Y_{A(B)}$, where $Z$, $X$, and $Y$ are three Pauli matrices. The $Z$ basis can be well aligned for common encoding schemes, and the $X$ and $Y$ bases may drift slowly with unknown angle $\beta$. In other words, the $Z$, $X$, and $Y$ bases satisfy $Z_B = Z_A$, $X_B = \cos \beta X_A + \sin \beta Y_A$, and $Y_B = \cos \beta Y_A - \sin \beta X_A$, Alice and Bob can distill secret keys from data in $Z$ basis, and estimate Eve’s information from data in $X$ and $Y$ bases.

To date, there have been a lot of theoretical and experimental reports on RFI-QKD [16–26] due to its immunity against the slow drift of reference frames. However, the performance of practical RFI-QKD systems worsens with the increasing drift of reference frames, and their performance will become the worst when the relative rotation of reference frames reaches its maximum. Hereafter, the maximum relative rotation of reference frames is termed the worst relative rotation of reference frames. Hence, it is vital to investigate the worst relative rotation of reference frames of practical RFI-QKD systems and the corresponding performance.

In this paper, we mathematically demonstrate the worst relative rotation of reference frames for practical RFI-QKD systems, and investigate the corresponding performance with full optimized parameters. Simulation results show that practical RFI-QKD systems can achieve quite good performance even against the worst relative rotation of reference frames.
rotation of reference frames, which obviously exhibit the possibility of practical QKD systems with free drifting reference frames. Moreover, we propose a universal estimation method of the secret key rate in practical RFI-QKD systems, which does not need a good estimation of the relative rotation $\beta$.

2. The worst relative rotation of reference frames for practical RFI-QKD systems

For simplicity, we demonstrate the worst relative rotation of reference frames for RFI-QKD with the weak coherent source without statistical fluctuations. In order to make the demonstration more practical, we introduce the three-intensity decoy-state method [27–29] into RFI-QKD, where Alice randomly modulates her quantum states into signal states of intensity $\mu$, decoy states of intensity $\nu$, and vacuum states of intensity $\omega$. For signal (decoy) states of intensity $\mu (\nu)$, Alice randomly chooses bases $Z_A, X_A$, or $Y_A$, and for vacuum states of intensity $\omega$, she does not choose any bases. Bob randomly chooses bases $Z_B, X_B$, or $Y_B$ to measure the quantum states he received. After the quantum communication phase, Alice and Bob can obtain a series of gains and quantum bit error rates (QBERs).

Here, we give the related system parameters and models used in this demonstration first. $d (\eta_d)$ denotes the dark count rate (detection efficiency) of single-photon detectors, $\alpha (L)$ represents the loss coefficient (length) of the standard fiber link, $\eta = \eta_d 10^{-\frac{L}{10}}$ denotes the overall transmission efficiency between Alice and Bob, $e_\text{fl}$ characterizes the intrinsic error rate of the optical system, and $f$ measures the inefficiency of the key reconciliation process. In this paper, we use the typical parameters, which are $d = 3 \times 10^{-6}$, $\eta_d = 14.5\%$, $\alpha = 0.2 \text{ dB/km}$, $e_\text{fl} = 1.5\%$, and $f = 1.16$, for simulation. Moreover, two threshold single-photon detectors are adopted at Bob’s side, and the probability of the valid detection events conditional on $j$-photon states is

$$F(j) = \begin{cases} 1 - d, & \text{if } j > 0 \\ d(1 - d), & \text{if } j = 0 \end{cases}$$

(1)

where the valid detection events are those only one detector clicks. As for the double-click events in real-life RFI-QKD systems, Bob assigns a random bit value to one detector. The photon-number distribution of the phase-randomized weak coherent source is $P_\text{fl} = e^{-\lambda} \frac{\lambda^j}{j!}$, where $\lambda$ is the intensity of the weak coherent source, and $i$ is the number of photons.

Obviously, the gain of vacuum states, denoted as $Q^\omega$, is

$$Q^\omega = 2d (1 - d),$$

(2)

and the QBER of vacuum states, denoted as $E^\omega$, is

$$E^\omega = \frac{1}{2}.$$  
(3)

The gain of signal or decoy states of intensity $\lambda$ prepared in basis $\zeta_A$ and measured in basis $\zeta_B$, denoted as $Q^\lambda_{\zeta_A \zeta_B}$, can be given as,

$$Q^\lambda_{\zeta_A \zeta_B} = \frac{1}{2} (P^\lambda_{\zeta_A \zeta_B} + P^\lambda_{\zeta_B \zeta_A} + P^\lambda_{\zeta_A \zeta_A} + P^\lambda_{\zeta_B \zeta_B}),$$

(4)

where $\lambda \in \{\mu, \nu\}$, $\zeta_A, \zeta_B \in \{Z_A, X_A, X_B, Y_A, Y_B\}$, and $\zeta_A$ and $\zeta_B$ consist of basis $\zeta_A, \zeta_B$, and $\zeta_A$ consist of basis $\zeta_B$. $P^\lambda_{\zeta_A \zeta_B}$ denotes the probability of Bob measuring $\zeta_B$ conditional on Alice preparing states $\zeta_A$ with intensity $\lambda$, other parameters ($P^\lambda_{\zeta_B \zeta_A}, P^\lambda_{\zeta_A \zeta_A}$, and $P^\lambda_{\zeta_B \zeta_B}$) have similar meanings, and $\frac{1}{2}$ denotes the probability of Alice preparing quantum states $\zeta_A$ or $\zeta_B$.

With equation (4), Alice and Bob can obtain explicit expressions of different gains. We take $Q^\lambda_{X_A X_B}$ for example to show how to get these explicit expressions. First, $P^\lambda_{X_A X_B}$ satisfies

$$P^\lambda_{X_A X_B} = \sum_{i=0}^{\infty} \sum_{j=0}^{i} C_i^j \eta^i (1 - \eta)^{j-i} \left(\langle X_A^i | X_B^0 \rangle > |2\rangle \right)^j F(j)$$

$$= e^{-\lambda \eta} (1 - d) (e^{-\lambda \eta \text{cos} \beta} + d - 1)$$

(5)

Similarly, we can easily get

$$P^\lambda_{X_A Y_B} = e^{-\lambda \eta} (1 - d) (e^{-\lambda \eta \text{cos} \beta} + d - 1),$$

(6)

$$P^\lambda_{Y_A X_B} = e^{-\lambda \eta} (1 - d) (e^{-\lambda \eta \text{cos} \beta} + d - 1),$$

(7)
and

\[ P_{X_i|X_0} = e^{-\lambda_y}(1 - d)(e^{\lambda_y \frac{(1-n_0)}{2}} + d - 1). \]  

(8)

Then, with equations (4)–(8), we can obtain the explicit expression of \( Q_{X_i|X_0} \), which is

\[ Q_{X_i|X_0} = e^{-\lambda_y}(1 - d)(e^{\lambda_y \frac{(1-n_0)}{2}} + e^{\lambda_y \frac{(1-n_0)}{2}} + 2d - 2). \]  

(9)

With the same procedure, we can obtain

\[ Q_{Z_i|Z_0} = e^{-\lambda_y}(1 - d)(e^{\lambda_y} + 2d - 1), \]  

(10)

\[ Q_{X_i|Z_0} = e^{-\lambda_y}(1 - d)(e^{\lambda_y \frac{(1-n_0)}{2}} + e^{\lambda_y \frac{(1-n_0)}{2}} + 2d - 2), \]  

(11)

\[ Q_{Y_i|Z_0} = e^{-\lambda_y}(1 - d)(e^{\lambda_y \frac{(1-n_0)}{2}} + e^{\lambda_y \frac{(1-n_0)}{2}} + 2d - 2), \]  

(12)

and

\[ Q_{Z_i|Y_0} = e^{-\lambda_y}(1 - d)(e^{\lambda_y \frac{(1-n_0)}{2}} + e^{\lambda_y \frac{(1-n_0)}{2}} + 2d - 2). \]  

(13)

Considering the optical intrinsic error rate \( e_\text{in} \), the QBER of signal or decoy states of intensity \( \lambda \) in \( \zeta_A\zeta_B \), denoted as \( E_{\lambda_A\zeta_B} \), is

\[ E_{\lambda_A\zeta_B} = \min \{ E_{\lambda_A\zeta_B}^1, 1 - E_{\lambda_A\zeta_B}^2 \}, \]  

(14)

where \( E_{\lambda_A\zeta_B}^1 = e_d(1 - 2e_{\lambda_A\zeta_B}^1 + e_{\lambda_A\zeta_B}^1) \) and \( e_{\lambda_A\zeta_B}^1 = \frac{P_{X_i|X_0} + P_{X_i|Z_0}}{2Q_{X_i|Z_0}} \) [30, 31]. For simplicity and without loss of generality, we assume \( E_{\lambda_A\zeta_B}^1 \leq 0.5 \) in equation (14). If not, either Alice or Bob flips her or his bit strings to make \( E_{\lambda_A\zeta_B}^1 \leq 0.5 \).

With the above gains and QBERs, they can estimate the lower bound of the single-photon yield [29] in \( \zeta_A\zeta_B \)

\[ Y_{\lambda_A\zeta_B} = \frac{\mu}{\mu + \nu} (e^{\lambda_y} - e^{\lambda_y \frac{(1-n_0)}{2}} - e^{\lambda_y \frac{(1-n_0)}{2}} - \frac{\mu^2 + \nu^2}{\mu^2} Q^2) \],

(15)

and the upper bound of the single-photon error rate [29] in \( \zeta_A\zeta_B \)

\[ e_{\lambda_A\zeta_B}^1 = \min \{ \frac{e^{\lambda_y} - e^{\lambda_y \frac{(1-n_0)}{2}}}{\mu^1_{\lambda_A\zeta_B}}, 0.5 \}. \]  

(16)

Then, the secret key rate of decoy-state RFI-QKD [15, 27, 28] is

\[ R = P_{E}^{\mu} Y_{\lambda_A\zeta_B}^L (1 - I_E) - Q_{Z_i|Y_0}^L \beta H(E_{Z_i|Z_0}), \]  

(17)

where \( H \) is the binary entropy function given by \( H(x) = -x \log_2(x) - (1 - x) \log_2(1 - x) \), and \( I_E \) denotes Eve’s information. Particularly, Eve’s information is

\[ I_E = (1 - e^{1_{Z_i|Z_0}^L}) H[(1 + u)/2] + e^{1_{Z_i|Z_0}^L} H[(1 + v)/2], \]  

(18)

where

\[ u = \min \{ \sqrt{C/2} / (1 - e^{1_{Z_i|Z_0}^L}), 1 \}, \]  

(19)

\[ v = \sqrt{C/2} / (1 - e^{1_{Z_i|Z_0}^L} \gamma^2 / e^{1_{Z_i|Z_0}^L}), \]  

(20)

and

\[ C = (1 - 2e^{1_{X_i|X_0}^L}) + (1 - 2e^{1_{X_i|X_0}^L})^2 + (1 - 2e^{1_{X_i|X_0}^L})^2 + (1 - 2e^{1_{X_i|X_0}^L})^2. \]  

(21)

As shown in equation (17), the relative rotation of reference frames \( \beta \) only affects Eve’s information \( I_E \). More specifically, \( \beta \) only affects \( C \). Hence, to investigate the performance of practical RFI-QKD systems against the worst relative rotation of reference frames \( \beta \), we only need to investigate the performance of \( C \) against the worst \( \beta \). In our demonstration, we consider RFI-QKD with the slow drift of reference frames, where \( \beta \) can be simply deemed as constant in a short period of time. Interestingly, [22, 24] assume \( \beta \) suffers from certain variation.

To investigate the performance of \( C \) against \( \beta \), we temporarily set \( \mu = 0.6, \nu = 0.1, \) and \( L = 100 \), which obviously will not change the behavior of \( C \) against \( \beta \). First, with equations (16), (21), we can demonstrate \( C \) is a periodic function of \( \beta \) by calculations, and the minimal positive period of \( C \) is \( \frac{\pi}{4} \). In other words, \( C(\beta) = C(\beta + \frac{mn}{4}) \), where \( n = 1, 2, 3, \ldots \). Moreover, in the domain \([0, \frac{\pi}{4}]\), we can demonstrate \( C(\frac{\pi}{4} + \beta) = C(\frac{\pi}{4} - \beta) \), which means the symmetry axis of \( C \) is \( \frac{\pi}{4} \). Figure 1 shows the performance of \( C \) against the relative rotations of reference frames \( \beta \) in two periods. It can be easily seen that the minimal positive period of \( C \) is \( \frac{\pi}{4} \), and the performance of \( C \) reaches its worst at the symmetry axis, where \( \beta = \frac{\pi}{4} \) or \( \frac{\pi}{4} \).
Then, in the domain $\mathbb{P}$, we calculate the derivative of $C$, denoted as $\dot{C}$, and find $\dot{C} = 0$, $\dot{C} = 0$ with $0 < \beta_1 < \frac{\pi}{4}$ and $\dot{C} = 0$ with $\frac{\pi}{4} < \beta_2 < \frac{\pi}{2}$, which illustrates that $C$ reaches the minimum value at $\beta = \frac{\pi}{4}$. Figure 2 shows the performance of $C'$ against the relative rotations of reference frames $\beta$ in $\mathbb{P}$. Hence, considering the periodicity of equations (17) or (21), we demonstrate the worst relative rotation of reference frames for RFI-QKD is $\beta = \frac{m\pi}{4}$, where $m$ is odd.

The physics behind this demonstration can be explained by means of Bloch sphere: 1) $\beta = 0$ means that Alice’s $X_\Lambda$ and $Y_\Lambda$ bases align perfectly with Bob’s $X_B$ and $Y_B$ bases, which is the ideal case; 2) $\beta = \frac{\pi}{4}$ means that Alice’s $X_\Lambda$ is Bob’s $Y_B$ and Alice’s $Y_\Lambda$ is Bob’s $X_B$, which is in essence the ideal case due to the high symmetry of $C$; and 3) $\beta = \frac{\pi}{4}$ means the worst-aligned reference frames between Alice and Bob, which is the worst relative rotation of reference frames for RFI-QKD. Considering the periodicity of equation (17), we can deduce that the performance of RFI-QKD is worst at $\beta = \frac{m\pi}{4}$ ($m$ is odd).

3. Simulation

With the above demonstration, we consider the reasonable data set $N = 10^{14}$ for statistical fluctuations [31] in practical RFI-QKD systems, and investigate its performance in $\mathbb{P}$ by the full parameter optimization method [32]. Notice that the domain $\mathbb{P}$ is ample to study the performance of practical RFI-QKD systems due to the periodicity of equations (17) or (21). For comparison purpose, we investigate the performance of practical RFI-QKD with $\beta = 0, \frac{\pi}{8}, \frac{3\pi}{8}, \frac{5\pi}{8}$. Simulation results are shown in figure 3. In figure 3, the solid lines from right to left denote the secret key rate of RFI-QKD with $\beta = 0, \frac{\pi}{8}, \frac{3\pi}{8}$, respectively, and the dotted lines
from right to left denote the secret key rate of RFI-QKD with $b = \frac{\pi}{8}, \frac{3\pi}{8}$, respectively. It can be easily seen that the performance of practical RFI-QKD at the worst relative rotation of reference frames $b = \frac{\pi}{4}$ is always the worst, and the perfectly overlapped lines of $b = 0, \frac{\pi}{8}, \frac{3\pi}{8}$ illustrate the symmetry of equation (17).

Moreover, even with the worst relative rotation of reference frames $b = \frac{\pi}{4}$, practical RFI-QKD systems can still achieve very good performance.

We emphasize that the kernel of RFI-QKD is that Alice and Bob do not know the relative rotation of reference frames. Usually, Alice and Bob can give a rough estimation of the relative rotation (say $b = \frac{\pi}{8}$), and study the performance of practical RFI-QKD systems with the estimated $b$. However, since the reference frames between Alice and Bob suffer from the unknown and slow drifting, it is difficult for them to give a relatively good estimation of $b$. Hence, experimenters and engineers should investigate the performance of RFI-QKD against the worst relative rotation of reference frames, and then use the optimized parameters against the worst relative rotation of reference frames scenario to all relative rotations of reference frames. Denote the former doing as the usual method, and the latter as the new method.

With full optimized parameters, we make a comparison of the two methods in $[0, \frac{\pi}{8}]$ at $100$ km of the standard fiber link, and results are shown in figure 4, where the circles denote results of the usual method, and the triangles denote results of the new method.

![Figure 3. Secret key rates per pulse of RFI-QKD against different relative rotations of reference frames with $N = 10^{11}$ with full optimized parameters. The solid lines from right to left denote the performance with $\beta = 0, \frac{\pi}{4}, \frac{3\pi}{4}$, respectively, and the dotted lines from right to left denote the performance with $\beta = \frac{\pi}{8}, \frac{3\pi}{8}, \frac{5\pi}{8}$, respectively.](image1)

![Figure 4. Comparison of the usual method and the new method in RFI-QKD against the relative rotations of reference frames $\beta$ in $[0, \frac{\pi}{8}]$ at $100$ km with $N = 10^{11}$ by the full parameter optimization method. The circles denote the results of the usual method, and the triangles denote the results of the new method.](image2)
be noted that, to clearly show the performance of RFI-QKD against the worst relative rotation of reference frames, results in figure 3 are simulated with the usual method.

4. Conclusions

In conclusion, we have demonstrated the worst relative rotation of reference frames for practical RFI-QKD, and investigated its performance with optimized parameters. Simulation results show that RFI-QKD can achieve quite good performance against the worst relative rotation of reference frames, which clearly demonstrates the possibility of practical QKD systems with free drifting reference frames. We believe practical QKD systems with free drifting reference frames will easily find a place in the satellite-to-ground QKD scenario [11, 12] or other scenarios where it is difficult to calibrate the reference frames. Furthermore, we propose a universal estimation method of the secret key rate in practical RFI-QKD systems, which conforms to the nature of RFI-QKD more well than the usual estimation method.

Acknowledgments

We gratefully acknowledge the financial support from the National Key Research and Development Program of China through Grant No. 2017YFA0304100, the National Natural Science Foundation of China through Grants Nos. 61475197, 61590932, 11774180, 61705110, the Natural Science Foundation of Jiangsu Province through Grant No. BK20170902, the Natural Science Foundation of the Jiangsu Higher Education Institutions through Grant Nos. 15KJA120002, 17KJB140016, and the Outstanding Youth Project of Jiangsu Province through Grant No. BK20150039.

ORCID iDs

Chun-Mei Zhang @ https://orcid.org/0000-0002-4682-0384

References

[1] Bennett C H and Brassard G 1984 Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing (New York) 175–9
[2] Adachi Y, Yamamoto T, Koashi M and Imoto N 2007 Phys. Rev. Lett. 99 180503
[3] Lo H K, Curty M and Qi B 2012 Phys. Rev. Lett. 108 130503
[4] Yin H L et al 2016 Phys. Rev. Lett. 117 190501
[5] Sasaki T, Yamamoto Y and Koashi M 2014 Nature 509 475
[6] Yin Z Q, Fung C-H F, Ma X, Zhang C M, Li H W, Chen W, Wang S, Guo G C and Han Z F 2014 Phys. Rev. A 90 052319
[7] Li H W, Yin Z Q, Chen W, Wang S, Guo G C and Han Z F 2014 Phys. Rev. A 89 032302
[8] Zhou Y H, Yu Z W and Wang X B 2016 Phys. Rev. A 93 042324
[9] Frohlich B, Dynes J F, Lucamarini M, Sharpe A W, Yuan Z and Shields A J 2013 Nature 501 69
[10] Wang S, Yin Z Q, Chen W, He D Y, Song X T, Li H W, Zhang L J, Zhou Z, Guo G C and Han Z F 2015 Nature Photon. 9 832
[11] Yin J et al 2017 Phys. Rev. Lett. 119 200501
[12] Liao S K et al 2017 Nature 549 43
[13] Ji L, Gao J, Yang A L, Feng Z, Lin X F, Li Z G and Jin X M 2017 Opt. Express 25 19795
[14] Bourgoin J P, Higgins B L, Gogov N, Holloway C, Pugh C J, Kaiser S, Cranmer M and Jennewein T 2015 Opt. Express 23 33347
[15] Laing A, Scarani V, Rarity J G and O’Brien J L 2010 Phys. Rev. A 82 012304
[16] Walting J, Bittau D, Li H W, Laing A, O’Brien J L and Niskanen A O 2013 New. J. Phys. 15 073001
[17] 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 2014 Sci. Rep. 4 03617
[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] Zhang P et al 2014 Phys. Rev. Lett. 112 130501
[20] 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
[21] Wang C, Sun S H, Ma X C, Tang G Z and Liang L M 2015 Phys. Rev. A 92 042319
[22] Wang F, Zhang P, Wang X and Li F 2016 Phys. Rev. A 94 062330
[23] Zhang C M, Zhu J R and Wang Q 2017 Phys. Rev. A 95 032309
[24] Pramanik T, Park B K, Cho Y W, Han S W, Kim Y S and Moon S 2017 Phys. Lett. A 381 2497
[25] Zhang C M, Zhu J R and Wang Q 2017 J. Lightwave Technol. 35 4574
[26] Wang C, Yin Z Q, Wang S, Chen W, Guo G C and Han Z F 2017 Optica 4 1016
[27] Wang X B 2005 Phys. Rev. Lett. 94 230503
[28] Lo H K, Ma X and Chen K 2005 Phys. Rev. Lett. 94 230504
[29] Ma X, Qi B, Zhao Y and Lo H K 2005 Phys. Rev. A 72 012326
[30] Wang Q and Wang X B 2014 Sci. Rep. 4 04612
[31] Ma X, Fung C-H F and Razavi M 2012 Phys. Rev. A 86 052305
[32] Xu F, Xu H and Lo H K 2014 Phys. Rev. A 89 052333