SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

September 2026, Vol. 69, Iss. 9, 192502:1–192502:7
https://doi.org/10.1007/s11432-025-4828-x

From quantum discord to fully reference-frame-independent quantum key distribution

Rong WANG[1,3], Chun-Mei ZHANG[2*] & Zhen-Qiang YIN[4,5*]

[1]*School of Cyberspace, Hangzhou Dianzi University, Hangzhou 310018, China*
[2]*Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China*
[3]*Department of Physics, University of Hong Kong, Hong Kong 999077, China*
[4]*Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China*
[5]*Hefei National Laboratory, University of Science and Technology of China, Hefei 230088, China*

Received 12 November 2025/Revised 7 January 2026/Accepted 2 March 2026/Published online 13 August 2026

Abstract Quantum resource theories provide a powerful and innovative framework for exploring various phenomena in quantum information processing. They reshape our understanding of quantum information, spanning fundamental concepts to practical protocols. In this work, we investigate secure key distribution using quantum discord as a resource. Leveraging the unique properties of discord, we propose a fully reference-frame-independent quantum key distribution protocol capable of generating secret keys without requiring a shared reference frame. Specifically, we construct a 3×3 observed matrix as the security criterion, whose singular values remain invariant under changes in the reference frame. Using the Koashi-Winter relation, we establish the protocol's security against collective attacks in the asymptotic regime. Notably, when the key-generation basis is misaligned, this approach yields a tighter secret key bound compared to previous protocols, and this protocol reduces to previous ones when the key-generation basis is well-calibrated.

Keywords quantum key distribution, fully reference-frame-independent, quantum discord, security analysis, quantum resource

Citation Wang R, Zhang C-M, Yin Z-Q. From quantum discord to fully reference-frame-independent quantum key distribution. Sci China Inf Sci, 2026, 69(9): 192502, https://doi.org/10.1007/s11432-025-4828-x

1 Introduction

In recent years, quantum resource theories (QRTs) [1] have emerged as an active area of research, aiming to quantify desirable quantum effects, develop detection methods, and explore their applications in quantum information processing. From fundamental theory to practical implementation, QRTs have guided the development of novel and impactful quantum protocols. One prominent example is quantum discord (QD) [2–4], which characterizes the quantum correlation of bipartite systems. QD has been proven valuable in various domains, including quantum computing and quantum metrology [4], and its potential in quantum key distribution (QKD) [5] is of particular interest. Based on the principles of quantum physics, QKD allows two distant legitimate parties, Alice and Bob, to exchange information-theoretic secret key bits, in the presence of an eavesdropper, Eve. Notably, QD is considered the minimal resource required to ensure security in QKD [6], and prior studies [7, 8] have demonstrated its practical relevance in specific protocols. However, the exploration of QD's applications in QKD remains relatively underdeveloped. For instance, Ref. [7] investigated a protocol based on quantum states prepared and measured in two bases. This raises a natural question: could the use of three bases provide additional advantages?

In this work, we address this issue by proposing a novel reference-frame-independent QKD (RFI-QKD) protocol. Generally, a shared reference frame, which provides a vital benchmark for Alice and Bob to encode and decode quantum states, is essential for the regular running of practical QKD systems [9–16]. To establish a common reference frame between two distant parties, it is indispensable to perform some real-time calibration, e.g., the alignment of polarization states for polarization coding or the compensation of phase difference for phase coding, which, however, decreases the generation of secret key bits and complicates the operation of QKD systems. Fortunately, RFI-QKD [17, 18] enables secret key distribution between Alice and Bob even with an unknown and slowly drifted reference frame, and has been extensively investigated both theoretically and experimentally [19–25]. However, the key rate performance of RFI-QKD protocol [17, 18] relies heavily on the key-generation basis being well defined and

* Corresponding author (email: cmz@njupt.edu.cn, yinzq@ustc.edu.cn)

stable throughout the key-generation process. Under the premise of a well aligned Z basis, RFI-QKD is robust against the unknown and slow drift of the test bases, denoted as the X and Y bases. Nevertheless, in some practical scenarios, it is tricky to calibrate Alice and Bob's key-generation basis accurately and stably. For example, in the polarization coding scheme of fiber-based or free-space QKD, all polarization states may rotate in the harsh cases of aerial fibers swinging in the wind, cables along the railway, and mobile transmitter or receiver [26–31]. Therefore, a natural question is, can we design a QKD protocol in which the maximal amount of Eve's information is completely independent of the drift of Alice and Bob's reference frame?

Benefitting from the fact that QD is independent of the chosen reference frame, we propose a fully reference-frame-independent (FRFI) QKD protocol. We construct a 3×3 matrix whose singular values remain invariant under variations of Alice and Bob's reference frame. Using these singular values together with the Koashi-Winter relation [32], we derive the secret key rate in the asymptotic case. Furthermore, we numerically demonstrate the performance of the proposed FRFI-QKD protocol, and it reduces to the case of the previous RFI-QKD protocol [17, 18] if the key-generation basis is well calibrated.

2 Protocol description

As illustrated in Figure 1, a reference frame is characterized by three parameters, e.g., the polar angle θ, the azimuthal angle φ, and the relative phase γ between the two computational basis states on the Bloch sphere. Here we use Alice's Z_A-basis states $\{|0\rangle_A, |1\rangle_A\}$ as well as $\{\theta, \varphi, \gamma\}$ to define Bob's Z_B-basis states as $|0\rangle_B = \cos\frac{\theta}{2}|0\rangle_A + \mathrm{e}^{\mathrm{i}\varphi}\sin\frac{\theta}{2}|1\rangle_A$ and $|1\rangle_B = \mathrm{e}^{\mathrm{i}\gamma}(\sin\frac{\theta}{2}|0\rangle_A - \mathrm{e}^{\mathrm{i}\varphi}\cos\frac{\theta}{2}|1\rangle_A)$. The procedure of this FRFI-QKD protocol is shown as follows.

• **State preparation.** Alice randomly chooses a basis ξ_A from her mutually unbiased basis (MUB) set $\{X_A, Y_A, Z_A\}$ and a bit $a \in \{0, 1\}$ to prepare a corresponding orthogonal state, and sends it to Bob through the insecure quantum channel.

• **Measurement.** Bob randomly chooses a basis ξ_B from his MUB set $\{X_B, Y_B, Z_B\}$ to perform a projective measurement on the received state, and records the corresponding classical bit $b \in \{0, 1\}$.

• **Classification.** Alice publicly announces her basis for each preparation, and Bob publicly announces his basis for each measurement. According to their basis information, Alice and Bob classify their events into groups $G_{\xi_A\xi_B}$, where $\xi_A\xi_B$ denotes different combinations of their bases.

• **Parameter estimation.** Alice and Bob randomly sample a part of their raw data to estimate the gains and quantum bit error rates for all groups $G_{\xi_A\xi_B}$.

• **Post-processing.** Alice and Bob perform reverse information reconciliation and privacy amplification on the raw data corresponding to Z_AZ_B to obtain the final secret key bits.

3 Security analysis

We begin with a brief review of QD. Let $\bar{\rho}_{AB}$ be a bipartite quantum state in the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, and let $\bar{\rho}'_{AB} = \sum_b M_b\bar{\rho}_{AB}M_b^\dagger$ be the post-measurement state described by the positive operator-valued measures (POVMs) with elements $E_b = M_b^\dagger M_b$ on $\mathcal{H}_B$. The mutual information of $\bar{\rho}_{AB}$ is defined by $I(A:B) = H(A)+H(B)-H(AB)$, where $H(\cdot)$ is the von Neumann entropy. An alternative mutual information is given by $J(A|B) = H(A) - \min_{E_b} H(A|E_b)$, where $H(A|E_b)$ is the conditional entropy of $\bar{\rho}'_{AB}$ and the minimization is over all possible POVMs. QD is defined as the difference between these two forms of mutual information, which is given by

$$\begin{aligned} D(A|B) &= I(A:B) - J(A|B) \\ &= \min_{\{E_b\}} H(A|E_b) + H(B) - H(AB). \end{aligned} \tag{1}$$

We now employ the equivalent entanglement-based version to analyze the security of the FRFI-QKD protocol. Let ρ_{AB} be a two-qubit state shared by Alice and Bob. In the Pauli representation, it can be expressed as

$$\rho_{AB} = \frac{1}{4}\left(I\otimes I + \sum_i a_i\sigma_i\otimes I + \sum_j b_j I\otimes\sigma_j + \sum_{i,j} T_{ij}\sigma_i\otimes\sigma_j\right), \tag{2}$$

where I is the identity matrix, σ_i and σ_j are the Pauli matrices with $i, j \in \{x, y, z\}$, $a_i = \mathrm{Tr}[\rho_{AB}\sigma_i \otimes I]$ and $b_j = \mathrm{Tr}[\rho_{AB}I\otimes\sigma_j]$ are components of the local Bloch vectors, and $T_{ij} = \mathrm{Tr}[\rho_{AB}\sigma_i\otimes\sigma_j]$ are components of the 3×3

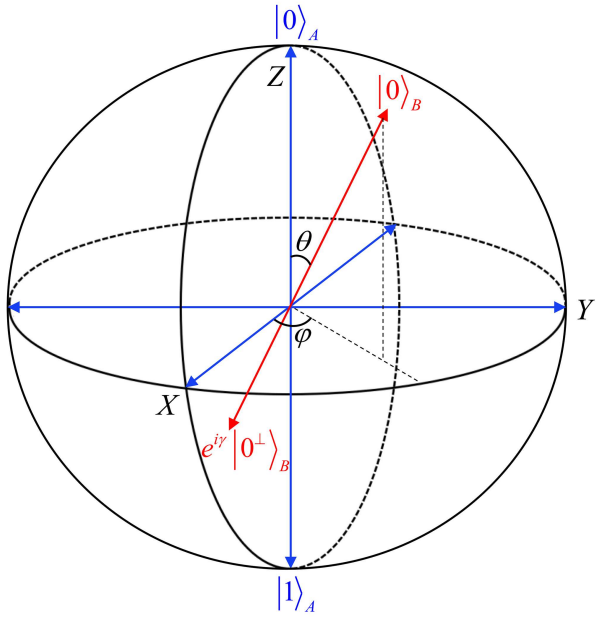

Figure 1 (Color online) Characterization of a reference frame based on the Bloch sphere, where $|0\rangle_A$ and $|1\rangle_A$ denote Alice's two computational basis states, $|0\rangle_B$ and $|1\rangle_B = e^{i\gamma}|0^\perp\rangle_B$ denote Bob's two computational basis states.

correlation tensor matrix denoted as $\hat{T}$. Following previous studies [33–35], we reduce ρ_{AB} to a Bell diagonal one without limiting Eve's power and changing the observable statistics. Refs. [36,37] have shown that, by applying an appropriate local unitary transformation $U_A \otimes U_B$ on ρ_{AB}, where $U_{A,B} \in SU(2)$, we can obtain

$$\rho'_{AB} = U_A \otimes U_B \rho_{AB} U_A^\dagger \otimes U_B^\dagger, \tag{3}$$

which has a diagonal correlation tensor matrix denoted as $\hat{T}'$. Since there must exist a unique rotation $O \in SO(3)$ corresponding to any unitary transformation $U \in SU(2)$, the correlation tensor matrix of ρ'_{AB} can be written as

$$\hat{T}' = O_A \hat{T} O_B^t = \mathrm{diag}[T'_{zz}, T'_{xx}, T'_{yy}], \tag{4}$$

where $O_{A(B)}$ denotes the unique rotation corresponding to $U_{A(B)}$. Without loss of generality, we assume $T'_{zz} \geqslant T'_{xx} \geqslant |T'_{yy}| \geqslant 0$, as proved in [8]. For completeness, we outline the proof here. To order these elements, we follow these steps: (1) apply $(\sigma_z + \sigma_x)/\sqrt{2}$ to both qubits if $|T'_{zz}| \leqslant |T'_{xx}|$, yielding $|T'_{zz}| \geqslant |T'_{xx}|$; (2) apply $(\sigma_y + \sigma_z)/\sqrt{2}$ to both qubits if $|T'_{zz}| \leqslant |T'_{yy}|$, yielding $|T'_{zz}| \geqslant |T'_{yy}|$; (3) apply $(\sigma_x + \sigma_y)/\sqrt{2}$ to both qubits if $|T'_{xx}| \leqslant |T'_{yy}|$, yielding $|T'_{xx}| \geqslant |T'_{yy}|$. These three steps ensure that $|T'_{zz}| \geqslant |T'_{xx}| \geqslant |T'_{yy}|$. Next, (4) do nothing if $T'_{zz} \geqslant 0$ and $T'_{xx} \geqslant 0$; (5) apply σ_z to Bob's qubit if $T'_{zz} \geqslant 0$ and $T'_{xx} \leqslant 0$; (6) apply σ_x to Bob's qubit if $T'_{zz} \leqslant 0$ and $T'_{xx} \geqslant 0$; (7) apply σ_y to Bob's qubit if $T'_{zz} \leqslant 0$ and $T'_{xx} \leqslant 0$.

We introduce a more mixed state

$$\sigma_{AB} = \frac{1}{4}\left(\rho'_{AB} + \sum_i \sigma_i \otimes \sigma_i \rho'_{AB} \sigma_i \otimes \sigma_i\right). \tag{5}$$

A straightforward calculation shows that the correlation tensor matrix of σ_{AB} is identical to that of ρ'_{AB}, while the local Bloch vectors of σ_{AB} vanish. Consequently, σ_{AB} is Bell diagonal. By performing inverse transformation on σ_{AB}, we obtain

$$U_A^\dagger \otimes U_B^\dagger \sigma_{AB} U_A \otimes U_B = \frac{1}{4}\left(I \otimes I + \sum_{i,j} T_{ij} \sigma_i \otimes \sigma_j\right), \tag{6}$$

whose correlation tensor matrix is exactly the same as that of ρ_{AB}. Notably, the states $U_A^\dagger \otimes U_B^\dagger \sigma_{AB} U_A \otimes U_B$ and ρ_{AB} produce identical observable statistics, while $U_A^\dagger \otimes U_B^\dagger \sigma_{AB} U_A \otimes U_B$ is more mixed than ρ_{AB}. Therefore, Eve can gain at least the same knowledge or even more if Alice and Bob share σ_{AB} [33–35]. Since σ_{AB} is Bell diagonal,

we rewrite it as

$$\sigma_{AB} = \sum_{k=1}^{4} \lambda_k \left|\Phi_k\right\rangle \left\langle\Phi_k\right|, \tag{7}$$

where $\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 = 1$, $\lambda_1 \geqslant \lambda_2 \geqslant \lambda_3 \geqslant \lambda_4 \geqslant 0$, $|\Phi_{1,2}\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}$, and $|\Phi_{3,4}\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}$. From the two representations of σ_{AB} in (5) and (7), we obtain the following relations:

$$\begin{aligned} &\lambda_1 + \lambda_2 - \lambda_3 - \lambda_4 = T'_{zz}, \\ &\lambda_1 - \lambda_2 + \lambda_3 - \lambda_4 = T'_{xx}, \\ &\lambda_1 - \lambda_2 - \lambda_3 + \lambda_4 = -T'_{yy}. \end{aligned} \tag{8}$$

We now apply QD to compute Eve's conditional entropy of Bob's classical bit. Using the Koashi-Winter relation [32] and similar technique in [7], we obtain

$$\min_{Z_B} H(Z_B|E) = D(A|B), \tag{9}$$

where the minimization is over all possible projective measurement basis Z_B [38]. For the Bell diagonal state σ_{AB} in (7), Refs. [39, 40] have demonstrated that its QD is given by

$$D(A|B) = 1 - (\lambda_1 + \lambda_2) h\left(\frac{\lambda_2}{\lambda_1 + \lambda_2}\right) - (\lambda_3 + \lambda_4) h\left(\frac{\lambda_4}{\lambda_3 + \lambda_4}\right), \tag{10}$$

where $h(x)$ denotes the Shannon entropy. To derive $\{\lambda_k\}$ from the observable statistics, we focus on the observable tensor correlation matrix

$$\hat{T} = \begin{bmatrix} \langle\sigma_x \otimes \sigma_x\rangle & \langle\sigma_x \otimes \sigma_y\rangle & \langle\sigma_x \otimes \sigma_z\rangle \\ \langle\sigma_y \otimes \sigma_x\rangle & \langle\sigma_y \otimes \sigma_y\rangle & \langle\sigma_y \otimes \sigma_z\rangle \\ \langle\sigma_z \otimes \sigma_x\rangle & \langle\sigma_z \otimes \sigma_y\rangle & \langle\sigma_z \otimes \sigma_z\rangle \end{bmatrix}, \tag{11}$$

where $\langle\sigma_i \otimes \sigma_j\rangle = T_{ij}$. After performing standard singular value decomposition (SVD) for $\hat{T}$, we can obtain the corresponding singular values in decreasing order as $\{T_1, T_2, T_3\}$. From (4), we obtain

$$T_1 = T'_{zz}, \quad T_2 = T'_{xx}, \quad T_3 = |T'_{yy}|. \tag{12}$$

Consequently, combining (8) and (12), the QD of σ_{AB} in (10) can be rewritten as

$$D(A|B) = 1 - \frac{1+T_1}{2} h\left(\frac{1+T_1-T_2-T_3}{2(1+T_1)}\right) - \frac{1-T_1}{2} h\left(\frac{1-T_1-T_2+T_3}{2(1-T_1)}\right). \tag{13}$$

Applying the Devetak-Winter bound [41], the secret key rate of FRFI-QKD in the asymptotic scenario is given by

$$R \geqslant \min_{Z_B} H(Z_B|E) - h(Q), \tag{14}$$

where Q is the quantum bit error rate of the key-generation basis. Finally, substituting (9) and (13) into (14) yields

$$R \geqslant 1 - \frac{1+T_1}{2} h\left(\frac{1+T_1-T_2-T_3}{2(1+T_1)}\right) - \frac{1-T_1}{2} h\left(\frac{1-T_1-T_2+T_3}{2(1-T_1)}\right) - h(Q). \tag{15}$$

Notably, the security can be lifted from collective attacks to coherent attacks using the postselection technique in [42].

4 Simulation

In the simulation, we assume the dark count rate of single-photon detectors is 10^{-6}, and the intrinsic error rate is 1.5%. To demonstrate the robustness against reference frame variations, we investigate the performance of FRFI-QKD under different θ, φ and γ with respect to the tolerable loss (including the detection efficiency of single-photon detectors) between Alice and Bob. Note that θ, φ and γ are actually unknown to Alice and Bob, which are set

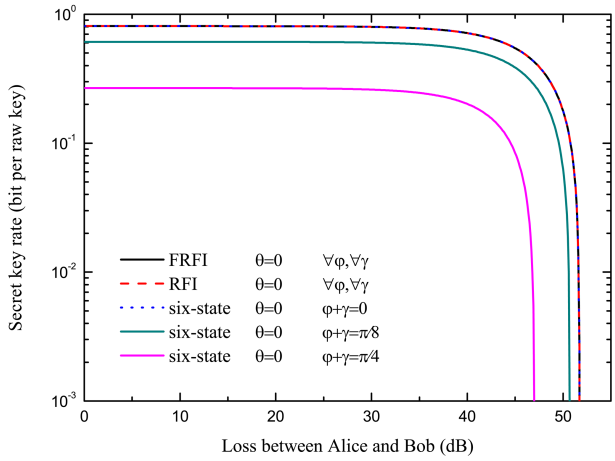

Figure 2 (Color online) Secret key rate (bit per raw key) of FRFI-QKD, RFI-QKD and six-state QKD under different φ and γ in the case of $\theta = 0$. The curves of FRFI-QKD and RFI-QKD with arbitrary φ and γ coincide exactly with the curve of six-state QKD with $\varphi + \gamma = 0$.

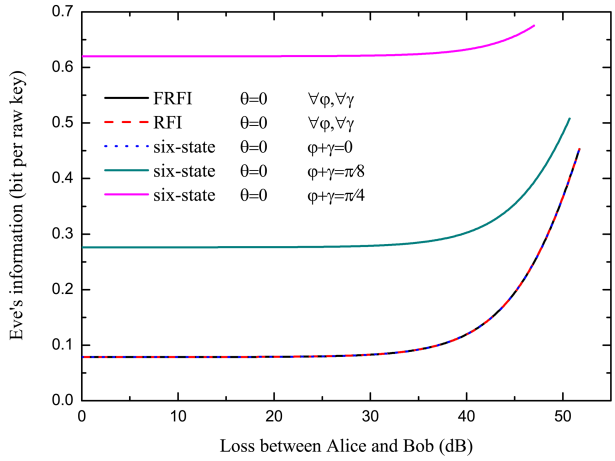

Figure 3 (Color online) Eve's information (bit per raw key) of FRFI-QKD, RFI-QKD and six-state QKD under different φ and γ in the case of $\theta = 0$. The curves of FRFI-QKD and RFI-QKD with arbitrary φ and γ coincide exactly with the curve of six-state QKD with $\varphi + \gamma = 0$.

to be known just for ease of simulation. We also compare the performance of FRFI-QKD with RFI-QKD [18] and six-state QKD [43].

First, we investigate the performance of FRFI-QKD, RFI-QKD and six-state QKD with a well aligned key-generation basis, that is, $\theta = 0$ while φ and γ drift. Figures 2 and 3 demonstrate that, with a well aligned key-generation basis, FRFI-QKD and RFI-QKD exhibit the same secret key rate and tolerable loss, since Eve's information in both FRFI-QKD and RFI-QKD is irrelevant to the variation of φ and γ when $\theta = 0$. In contrast, with the deterioration of φ and γ, the secret key rate and tolerable loss of six-state QKD are severely depressed due to the increasing amount of Eve's information.

Then, we examine the performance of FRFI-QKD, RFI-QKD and six-state QKD when the key-generation basis Z is misaligned, e.g., $\theta = \pi/8$, and the corresponding results are shown in Figures 4 and 5. We can find that the misalignment of the key-generation basis ($\theta = \pi/8$) has the most severe impact on six-state QKD, followed by RFI-QKD, and the least on FRFI-QKD. Moreover, the drift of φ and γ does not affect the secret key rate, tolerable loss, or Eve's information of FRFI-QKD and RFI-QKD, but does affect those of six-state QKD, exhibiting trends similar to those in Figures 2 and 3. Notably, in the case of $\theta = \pi/8$, the secret key rate and tolerable loss of FRFI-QKD are significantly higher than those of RFI-QKD, because the estimation of Eve's information in FRFI-QKD is independent of θ, φ and γ, and is tighter than that of RFI-QKD.

Finally, we investigate the performance of FRFI-QKD and RFI-QKD with the variation of the key-generation basis, e.g., $\theta = 0, \pi/8, \pi/4, 3\pi/8$ with arbitrary φ and γ, and the corresponding results are shown in Figures 6 and 7. As θ increases, the secret key rate and tolerable loss of FRFI-QKD remain substantially higher than those of RFI-QKD. As shown in Figure 7, in FRFI-QKD, the misalignment of the key-generation basis does not help Eve to obtain more information on the raw key, due to the constructed 3×3 matrix whose singular values are irrelevant to the choice of the reference frame between Alice and Bob. However, the misalignment of the key-generation basis increases the quantum bit error rate of the raw data, reducing the secret key rate of both FRFI-QKD and RFI-QKD. Remarkably, when the key generation basis experiences significant misalignment (e.g., $\theta = 3\pi/8$), FRFI-QKD continues to generate considerable key bits, while RFI-QKD fails to produce any positive key bits. This clearly demonstrates that FRFI-QKD is more robust against the reference frame drift and can substantially relax the real-time calibration requirement of the reference frame in practical QKD systems.

5 Conclusion

In summary, based on the constructed $\hat{T}$-matrix and Koashi-Winter relation, we have employed QD to analyze the security for an FRFI-QKD protocol. Owing to the intrinsic properties of QD, this protocol is robust against the slow drift of the reference frame characterized by θ, φ and γ. Numerical simulation results show that Eve's information in FRFI-QKD is completely independent of θ, φ and γ; Eve's information in RFI-QKD is only independent of φ and γ; and Eve's information in six-state QKD is dependent on θ, φ and γ. On the other hand, since the drift of θ

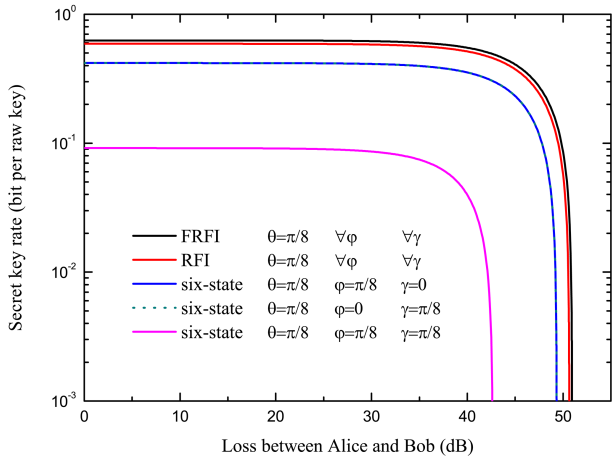

Figure 4 (Color online) Secret key rate (bit per raw key) of FRFI-QKD, RFI-QKD and six-state QKD under different φ and γ in the case of $\theta = \pi/8$. The curve of six-state QKD with $\varphi = \pi/8$ and $\gamma = 0$ coincides exactly with that of six-state QKD with $\varphi = 0$ and $\gamma = \pi/8$.

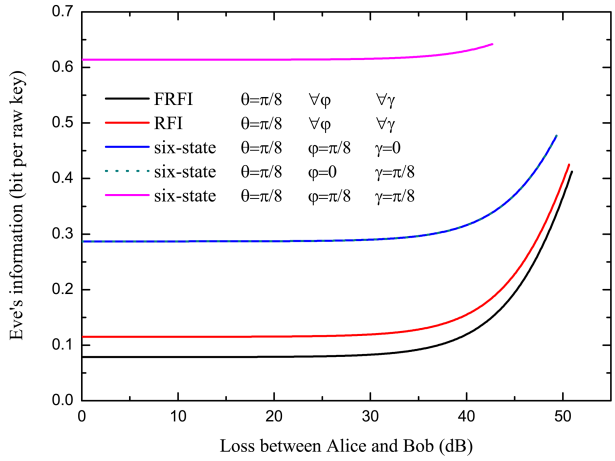

Figure 5 (Color online) Eve's information (bit per raw key) of FRFI-QKD, RFI-QKD and six-state QKD under different φ and γ in the case of $\theta = \pi/8$. The curve of six-state QKD with $\varphi = \pi/8$ and $\gamma = 0$ coincides exactly with that of six-state QKD with $\varphi = 0$ and $\gamma = \pi/8$.

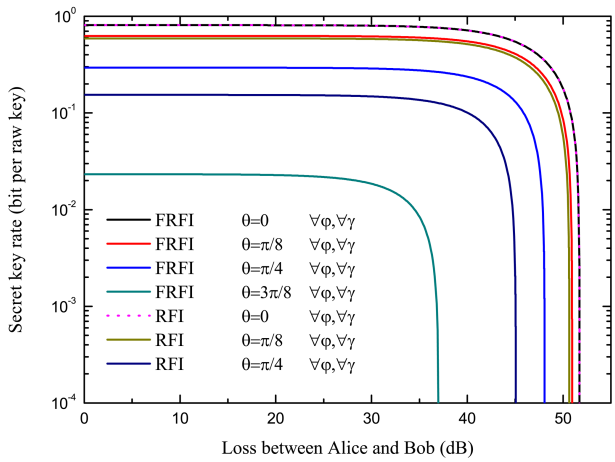

Figure 6 (Color online) Secret key rate (bit per raw key) of FRFI-QKD and RFI-QKD under different θ in the case of arbitrary φ and γ. In the case of $\theta = 0$, the curves of FRFI-QKD and RFI-QKD with arbitrary φ and γ coincide exactly.

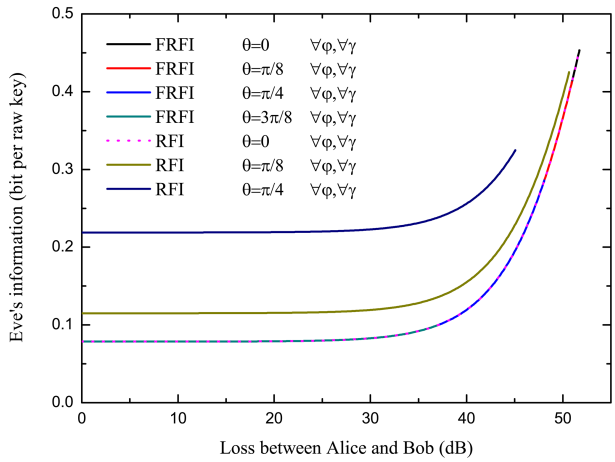

Figure 7 (Color online) Eve's information (bit per raw key) of FRFI-QKD and RFI-QKD under different θ in the case of arbitrary φ and γ. The curves of Eve's information for FRFI-QKD under different θ coincide exactly except that their tolerable losses differ.

affects the quantum bit error rate of the raw data, the secret key rate of FRFI-QKD decreases with the deterioration of θ. When the key-generation basis suffers from significant variation, FRFI-QKD continues to produce substantial key data, greatly relaxing the real-time calibration requirement of a reference frame and enabling applications in more complex reference frame scenarios. Conversely, when the key-generation basis is well aligned, FRFI-QKD exhibits performance identical to that of RFI-QKD. Moreover, given the scarcity of ideal single-photon sources, the decoy-state method [44,45] can be naturally incorporated into our protocol. In future work, it would be interesting to extend the approach of our protocol to other quantum cryptographic schemes [46–48].

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 62501220, 62371244, 62531023) and Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0300700).

References

1 Chitambar E, Gour G. Quantum resource theories. Rev Mod Phys, 2019, 91: 025001
2 Henderson L, Vedral V. Classical, quantum and total correlations. J Phys A-Math Gen, 2001, 34: 6899–6905
3 Ollivier H, Zurek W H. Quantum discord: a measure of the quantumness of correlations. Phys Rev Lett, 2001, 88: 017901
4 Modi K, Brodutch A, Cable H, et al. The classical-quantum boundary for correlations: discord and related measures. Rev Mod Phys, 2012, 84: 1655–1707
5 Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 1984. 175–179

6 Pirandola S. Quantum discord as a resource for quantum cryptography. Sci Rep, 2014, 4: 6956
7 Wang R, Fan-Yuan G J, Yin Z Q, et al. Secure key from quantum discord. ArXiv:2304.05880
8 Wang R, Yao Y, Yin Z Q. Quantum discord witness with uncharacterized devices. Phys Rev Appl, 2025, 23: 064019
9 Wang S, Yin Z Q, Chen W, et al. Experimental demonstration of a quantum key distribution without signal disturbance monitoring. Nat Photon, 2015, 9: 832–836
10 Yin H L, Chen T Y, Yu Z W, et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. Phys Rev Lett, 2016, 117: 190501
11 Boaron A, Boso G, Rusca D, et al. Secure quantum key distribution over 421 km of optical fiber. Phys Rev Lett, 2018, 121: 190502
12 Comandar L C, Lucamarini M, Fröhlich B, et al. Quantum key distribution without detector vulnerabilities using optically seeded lasers. Nat Photon, 2016, 10: 312–315
13 Xie Y M, Lu Y S, Weng C X, et al. Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon interference. PRX Quantum, 2022, 3: 020315
14 Lu F Y, Wang Z H, Zapatero V, et al. Experimental demonstration of fully passive quantum key distribution. Phys Rev Lett, 2023, 131: 110802
15 Lu Q H, Wang F X, Chen W, et al. Quantum key distribution over a mimicked dynamic-scattering channel. Sci China Inf Sci, 2024, 67: 142503
16 Wang P, Tian Y, Li Y M. Advances in continuous variable measurement-device-independent quantum key distribution. Sci China Inf Sci, 2025, 68: 180501
17 Laing A, Scarani V, Rarity J G, et al. Reference-frame-independent quantum key distribution. Phys Rev A, 2010, 82: 012304
18 Zhu J R, Wang R, Zhang C M. Improved reference-frame-independent quantum key distribution. Opt Lett, 2022, 47: 4219–4222
19 Yin Z Q, Wang S, Chen W, et al. Reference-free-independent quantum key distribution immune to detector side channel attacks. Quantum Inf Process, 2014, 13: 1237–1244
20 Zhang C M, Zhu J R, Wang Q. Practical reference-frame-independent quantum key distribution systems against the worst relative rotation of reference frames. J Phys Commun, 2018, 2: 055029
21 Lu F Y, Yin Z Q, Fan-Yuan G J, et al. Efficient decoy states for the reference-frame-independent measurement-device-independent quantum key distribution. Phys Rev A, 2020, 101: 052318
22 Jiang X L, Wang Y, Li J J, et al. Improving the performance of reference-frame-independent quantum key distribution with advantage distillation technology. Opt Express, 2023, 31: 9196
23 Wang C, Song X T, Yin Z Q, et al. Phase-reference-free experiment of measurement-device-independent quantum key distribution. Phys Rev Lett, 2015, 115: 160502
24 Liu X, Luo D, Luo Z, et al. Reference-frame-independent quantum key distribution over 250 km of optical fiber. Phys Rev Appl, 2024, 22: 064018
25 Tian Z Y, Xie Z R, Chen Y, et al. Reference-frame-independent quantum key distribution based on machine-learning-enhanced qubit-based synchronization. Sci China-Phys Mech Astron, 2025, 68: 270312
26 Xavier G B, Walenta N, Vilela de Faria G, et al. Experimental polarization encoded quantum key distribution over optical fibres with real-time continuous birefringence compensation. New J Phys, 2009, 11: 045015
27 Ferreira da Silva T, Vitoreti D, Xavier G B, et al. Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. Phys Rev A, 2013, 88: 052303
28 Tang Z, Liao Z, Xu F, et al. Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. Phys Rev Lett, 2014, 112: 190503
29 Ding Y Y, Chen H, Wang S, et al. Polarization variations in installed fibers and their influence on quantum key distribution systems. Opt Express, 2017, 25: 27923–27936
30 Li D D, Gao S, Li G C, et al. Field implementation of long-distance quantum key distribution over aerial fiber with fast polarization feedback. Opt Express, 2018, 26: 22793
31 Tian X H, Yang R, Liu H Y, et al. Experimental demonstration of drone-based quantum key distribution. Phys Rev Lett, 2024, 133: 200801
32 Koashi M, Winter A. Monogamy of quantum entanglement and other correlations. Phys Rev A, 2004, 69: 022309
33 Renner R. Security of quantum key distribution. Int J Quantum Inform, 2008, 06: 1–127
34 Acín A, Brunner N, Gisin N, et al. Device-independent security of quantum cryptography against collective attacks. Phys Rev Lett, 2007, 98: 230501
35 Pironio S, Acín A, Brunner N, et al. Device-independent quantum key distribution secure against collective attacks. New J Phys, 2009, 11: 045021
36 Horodecki R, Horodecki P. Perfect correlations in the Einstein-Podolsky-Rosen experiment and Bell's inequalities. Phys Lett A, 1996, 210: 227–231
37 Horodecki R, Horodecki M. Information-theoretic aspects of inseparability of mixed states. Phys Rev A, 1996, 54: 1838–1843
38 Datta A. Studies on the role of entanglement in mixed-state quantum computation. Dissertation for Ph.D. Degree. Albuquerque: The University of New Mexico, 2008
39 Luo S. Quantum discord for two-qubit systems. Phys Rev A, 2008, 77: 042303
40 Lang M D, Caves C M. Quantum discord and the geometry of bell-diagonal states. Phys Rev Lett, 2010, 105: 150501
41 Devetak I, Winter A. Distillation of secret key and entanglement from quantum states. Proc Royal Soc A Math Phys Eng Sci, 2005, 461: 207–235
42 Christandl M, König R, Renner R. Postselection technique for quantum channels with applications to quantum cryptography. Phys Rev Lett, 2009, 102: 020504
43 Bruß D. Optimal eavesdropping in quantum cryptography with six states. Phys Rev Lett, 1998, 81: 3018–3021
44 Wang X B. Beating the photon-number-splitting attack in practical quantum cryptography. Phys Rev Lett, 2005, 94: 230503
45 Lo H K, Ma X, Chen K. Decoy state quantum key distribution. Phys Rev Lett, 2005, 94: 230504
46 Liu H W, Liu Z P, Yin H L, et al. Quantum-enhanced blockchain federated learning via quantum Byzantine agreement. Sci China Inf Sci, 2025, 68: 180503
47 Lu Y S, Yin H L, Xie Y M, et al. Repeater-like asynchronous measurement-device-independent quantum conference key agreement. Rep Prog Phys, 2025, 88: 067901
48 Xiao Y R, Yin H L, Hua W J, et al. Experimental efficient source-independent quantum secret sharing against coherent attacks. Phys Rev Lett, 2025, 135: 150801