SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

August 2026, Vol. 69, Iss. 8, 182501:1–182501:15
https://doi.org/10.1007/s11432-025-4759-x

Fully passive reference-frame-independent quantum key distribution with finite-key security analysis

Jia-Wei YING[1], Shi-Pu GU[1], Xing-Fu WANG[3], Lan ZHOU[2,3] & Yu-Bo SHENG[1,2*]

[1]*College of Electronic and Optical Engineering and College of Flexible Electronics (Future Technology), Nanjing University of Posts and Telecommunications, Nanjing 210023, China*
[2]*School of Physics, Hangzhou Normal University, Hangzhou 311121, China*
[3]*College of Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China*

Received 24 June 2025/Revised 3 November 2025/Accepted 15 January 2026/Published online 16 July 2026

Abstract Fully passive quantum key distribution (QKD) avoids active modulation of the source and enhances robustness against side-channel attacks. However, existing fully passive QKD systems suffer from low resource efficiency and dependence on precisely calibrated reference frames, limiting their practical applicability. We present a fully passive reference-frame-independent (RFI) QKD protocol that eliminates side channels caused by source-side modulators and fully utilizes the quantum states generated by passive sources to improve efficiency. Our protocol requires calibration of only one axis of the reference frame for secure key transmission, significantly reducing implementation complexity. We developed a system model and conducted parameter optimization, which resulted in a secure key transmission rate improvement of approximately 20% compared to the original fully passive QKD under ideal scenarios. In addition, we analyzed the protocol's performance for finite-length keys. Our fully passive RFI-QKD protocol contributes to the development of practical fully passive QKD systems.

Keywords fully passive, reference-frame-independent, quantum key distribution, quantum communication, finite-key

Citation Ying J-W, Gu S-P, Wang X-F, et al. Fully passive reference-frame-independent quantum key distribution with finite-key security analysis. Sci China Inf Sci, 2026, 69(8): 182501, https://doi.org/10.1007/s11432-025-4759-x

1 Introduction

Quantum key distribution (QKD) enables secure key sharing between two remote users [1]. It ensures unconditional security in communication and has significant applications in quantum communication. Recently, many important protocols have been proposed to advance QKD applications, including: (1) measurement-device-independent (MDI) protocols [2–7], which delegate measurement to a third party to eliminate side channels at the measurement end; (2) twin-field protocols [8–12], which utilize single-photon interference to break the PLOB bound; (3) asynchronous MDI protocols [13–16] and mode-pairing protocols [17–19], which also utilize asynchronous two-photon interference to overcome the PLOB bound while eliminating the phase locking requirement of the twin-field protocol, further enhancing system robustness; (4) device-independent (DI) protocols [20–24], which eliminate side channels at both the source and measurement ends by violating Bell's inequality; and so on [25–35].

Aside from DI protocols, many of the aforementioned protocols may be vulnerable to source-side side-channel risks. Active modulation can generate non-trivial side-channel leakage [36], potentially allowing eavesdroppers (Eve) to conduct sophisticated attacks, such as Trojan-horse attacks [37–43] and unambiguous state discrimination attacks [44, 45], thereby compromising protocol security. To address this issue, Wang et al. [46] proposed a fully passive QKD protocol in 2023, to eliminate active modulation through coherent light interference and combination. This architecture passively generates pulses with random quantum states and intensities, fundamentally bypassing side channels induced by active modulation. The fully passive QKD was experimentally demonstrated in 2023 [47, 48], and the method has been applied to a variety of quantum communication protocols [49–56].

However, the practical implementation of current fully passive QKD faces notable challenges. First, fully passive sources generate quantum states randomly distributed across the Bloch sphere, whereas conventional fully passive QKD protocols utilize only photons in the X and Z bases. This discrepancy results in a significant portion of photons from the passive source being discarded, thereby degrading resource efficiency. Second, fully passive QKD relies on

* Corresponding author (email: shengyb@njupt.edu.cn)

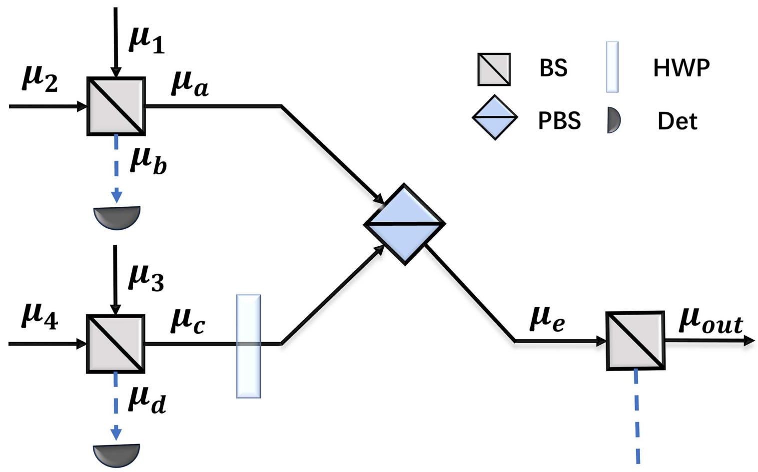

Figure 1 (Color online) Structure of the fully passive source, similar to that in [46]. BS: beam splitter; PBS: polarization beam splitter; HWP: half-wave plate; Det: detector.

rigorous reference frame calibration. In real-world environments, unavoidable disturbances induce fluctuations in the reference frame, making continuous calibration under practical conditions very challenging.

In 2010, Laing et al. [57] proposed the reference-frame-independent (RFI) QKD protocol. In their protocol, the sender Alice employs six quantum states prepared in the Z_A, X_A, and Y_A bases, and the receiver Bob measures these states using the Z_B, X_B, and Y_B bases. Secure key transmission can be achieved as long as one axis of the reference frame is calibrated. The RFI protocol has received extensive research attention, including MDI protocols [58–61], TW protocols [62], fewer states [63–65], and so on [66–71].

Inspired by previous studies [46, 49, 50, 57], we propose a fully passive RFI QKD protocol. Our work makes the following key contributions. (1) We integrate the RFI framework into fully passive QKD systems, effectively eliminating side-channel risks from source-side modulators and fully leveraging quantum states generated by passive sources to enhance efficiency. Notably, our protocol requires calibration of only one direction of the reference frame, significantly reducing the complexity of fully passive QKD systems. (2) We establish a novel system model and perform parameter optimization based on fully passive sources to analyze the performance of the fully passive RFI protocol. By optimizing post-selection intervals and intensities, we obtain the maximum secure key transmission rate achievable by the protocol. (3) We analyze the protocol's performance considering the finite length effect under practical conditions with varying numbers of light source pulses, as well as under different reference frame misalignments.

The remainder of the paper is organized as follows. In Section 2, we introduce the fully passive RFI QKD, including the fully passive source protocol. In Section 3, we describe our estimation of the performance of the fully passive RFI QKD protocol, including the secure key rate, system model, and parameter estimation. In Section 4, we describe the numerical simulations and parameter optimization we conducted in the study. Finally, Section 5 presents a discussion and conclusion.

2 Fully passive RFI QKD

2.1 Fully passive source

In 2023, Wang et al. [46] proposed the first fully passive source. In the same year, Zapatero et al. [49] made several improvements on the fully passive source. The fully passive source and analysis method in our work is based on the above works. Specifically, we refer to [50] and combine the coding strategy in [46] with the analysis method in [49].

The structural diagram of the fully passive source is shown in Figure 1. By inputting four coherent lights with the same intensity and random phases, the device is capable of generating coherent lights with random quantum states and random intensities.

Firstly, the four input coherent pulses can be expressed as

$$\begin{aligned}|\mu_1\rangle &= |\sqrt{v}\mathrm{e}^{\mathrm{i}\alpha}\rangle_H,\ |\mu_2\rangle = |\sqrt{v}\mathrm{e}^{\mathrm{i}\beta}\rangle_H,\\ |\mu_3\rangle &= |\sqrt{v}\mathrm{e}^{\mathrm{i}\gamma}\rangle_H,\ |\mu_4\rangle = |\sqrt{v}\mathrm{e}^{\mathrm{i}\delta}\rangle_H,\end{aligned} \tag{1}$$

where v is the intensity, and α, β, γ, and δ are random phases. The subscript H indicates that all the photons in the pulse are initially in horizontal polarization ($|H\rangle$).

Then, these four coherent pulses are passed through the $50:50$ beam splitter (BS) in pairs for interference, and the result is

$$\begin{aligned}
|\mu_1\rangle|\mu_2\rangle &= |\sqrt{v}\mathrm{e}^{\mathrm{i}\alpha}\rangle_H|\sqrt{v}\mathrm{e}^{\mathrm{i}\beta}\rangle_H \\
&\overset{\mathrm{BS}}{\rightarrow} \left|\sqrt{\frac{v}{2}}(\mathrm{e}^{\mathrm{i}\alpha}-\mathrm{e}^{\mathrm{i}\beta})\right\rangle_H \left|\sqrt{\frac{v}{2}}(\mathrm{e}^{\mathrm{i}\alpha}+\mathrm{e}^{\mathrm{i}\beta})\right\rangle_H \\
&= \left|\sqrt{2v}\mathrm{e}^{\mathrm{i}\frac{\alpha+\beta+\pi}{2}}\sin\frac{\alpha-\beta}{2}\right\rangle_H \left|\sqrt{2v}\mathrm{e}^{\mathrm{i}\frac{\alpha+\beta}{2}}\cos\frac{\alpha-\beta}{2}\right\rangle_H \\
&= |\mu_a\rangle|\mu_b\rangle,
\end{aligned} \tag{2}$$

$$\begin{aligned}
|\mu_3\rangle|\mu_4\rangle &= |\sqrt{v}\mathrm{e}^{\mathrm{i}\gamma}\rangle_H|\sqrt{v}\mathrm{e}^{\mathrm{i}\delta}\rangle_H \\
&\overset{\mathrm{BS}}{\rightarrow} \left|\sqrt{\frac{v}{2}}(\mathrm{e}^{\mathrm{i}\gamma}-\mathrm{e}^{\mathrm{i}\delta})\right\rangle_H \left|\sqrt{\frac{v}{2}}(\mathrm{e}^{\mathrm{i}\gamma}+\mathrm{e}^{\mathrm{i}\delta})\right\rangle_H \\
&= \left|\sqrt{2v}\mathrm{e}^{\mathrm{i}\frac{\gamma+\delta+\pi}{2}}\sin\frac{\gamma-\delta}{2}\right\rangle_H \left|\sqrt{2v}\mathrm{e}^{\mathrm{i}\frac{\gamma+\delta}{2}}\cos\frac{\gamma-\delta}{2}\right\rangle_H \\
&= |\mu_c\rangle|\mu_d\rangle.
\end{aligned} \tag{3}$$

Then, $|\mu_c\rangle$ passes through a half-wave plate (HWP) to flip the polarization of the photons to vertical polarization ($|V\rangle$). $|\mu_a\rangle$ and $|\mu_c\rangle$ enter the BS for beam combination. After the BS, we can obtain

$$\begin{aligned}
|\mu_a\rangle|\mu_c\rangle &\overset{\mathrm{PBS}}{\rightarrow} |\mu_e\rangle \\
&= \left|\sqrt{2v}\mathrm{e}^{\mathrm{i}\frac{\alpha+\beta+\pi}{2}}\sin\frac{\alpha-\beta}{2}\right\rangle_H \left|\sqrt{2v}\mathrm{e}^{\mathrm{i}\frac{\gamma+\delta+\pi}{2}}\sin\frac{\gamma-\delta}{2}\right\rangle_V \\
&= \exp\left(-v\sin^2\frac{\alpha-\beta}{2}\right)\exp\left(\sqrt{2v}\mathrm{e}^{\mathrm{i}\frac{\alpha+\beta+\pi}{2}}\sin\frac{\alpha-\beta}{2}a_H^\dagger\right) \\
&\quad\cdot\exp\left(-v\sin^2\frac{\gamma-\delta}{2}\right)\exp\left(\sqrt{2v}\mathrm{e}^{\mathrm{i}\frac{\gamma+\delta+\pi}{2}}\sin\frac{\gamma-\delta}{2}a_V^\dagger\right) \\
&= \exp\left(-v\left(\sin^2\frac{\alpha-\beta}{2}+\sin^2\frac{\gamma-\delta}{2}\right)\right) \\
&\quad\cdot\exp\left(\sqrt{2v}\mathrm{e}^{\mathrm{i}\frac{\alpha+\beta+\pi}{2}}(\sin\tfrac{\alpha-\beta}{2}a_H^\dagger+\mathrm{e}^{\mathrm{i}(\frac{\gamma+\delta}{2}-\frac{\alpha+\beta}{2})}\sin\tfrac{\gamma-\delta}{2}a_V^\dagger)\right)|\mathrm{vac}\rangle \\
&= \mathrm{e}^{-\frac{I_e}{2}}\mathrm{e}^{\sqrt{I_e}\mathrm{e}^{\mathrm{i}\psi}a^\dagger(\theta,\phi)}|\mathrm{vac}\rangle \\
&= |\sqrt{I_e}\mathrm{e}^{\mathrm{i}\psi}\rangle_{a^\dagger(\theta,\phi)},
\end{aligned} \tag{4}$$

where

$$\begin{aligned}
&I_e = 2v\left(\sin^2\frac{\alpha-\beta}{2}+\sin^2\frac{\gamma-\delta}{2}\right), \\
&\psi = \frac{\alpha+\beta+\pi}{2}, \\
&a^\dagger(\theta,\phi) = \cos\frac{\theta}{2}a_H^\dagger+\mathrm{e}^{\mathrm{i}\phi}\sin\frac{\theta}{2}a_V^\dagger, \\
&\cos\frac{\theta}{2} = \sin\frac{\alpha-\beta}{2}\Big/\sqrt{\sin^2\frac{\alpha-\beta}{2}+\sin^2\frac{\gamma-\delta}{2}}, \\
&\sin\frac{\theta}{2} = \sin\frac{\gamma-\delta}{2}\Big/\sqrt{\sin^2\frac{\alpha-\beta}{2}+\sin^2\frac{\gamma-\delta}{2}}, \\
&\phi = \frac{\gamma+\delta}{2}-\frac{\alpha+\beta}{2}.
\end{aligned} \tag{5}$$

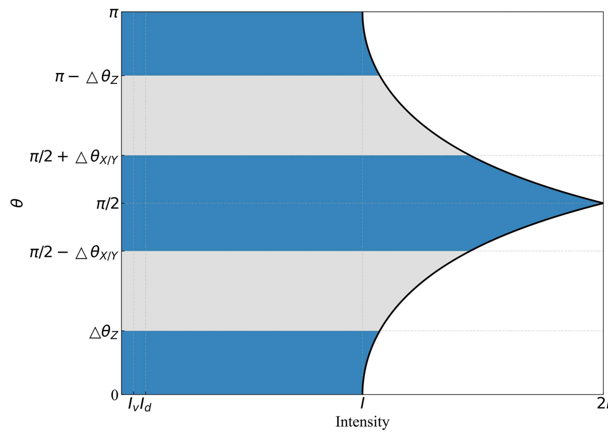

Figure 2 (Color online) Schematic of decoy state interval. The blue regions denote the post-selection interval. When θ is in the intervals $[0, \triangle\theta_Z]$ and $[\pi - \triangle\theta_Z, \pi]$, the output states correspond to the Z basis. When θ is in the interval $[\frac{\pi}{2} - \triangle\theta_{X/Y}, \frac{\pi}{2} + \triangle\theta_{X/Y}]$, the output states correspond to the Y or X basis. When the intensity I is in intervals $[0, I_v]$, $[I_v, I_d]$, and $[I_d, I_s]$, the output states correspond to vacuum, decoy, and signal states, respectively. In the numerical simulation, we set $I_s = I$.

Finally, $|\mu_e\rangle$ is attenuated by a BS with transmittance t much lower than 1, resulting in the output of a weak coherent pulse $|\mu_{out}\rangle$ with the form of

$$|\mu_{out}\rangle = \mathrm{e}^{-\frac{I}{2}} \mathrm{e}^{\sqrt{I}\mathrm{e}^{\mathrm{i}\psi} a^\dagger(\theta,\phi)} |\mathrm{vac}\rangle = |\sqrt{I}\mathrm{e}^{\mathrm{i}\psi}\rangle_{a^\dagger(\theta,\phi)}, \tag{6}$$

where $I = I_e t$.

Since the final output states are randomly distributed on the Bloch sphere, we still need to perform post-selection to select the desired output states. Through heterodyne detection of $|\mu_b\rangle$ and $|\mu_d\rangle$, we can measure their intensities and global phases, thereby obtaining the parameters I, θ, ϕ of the output states. As shown in Figure 2, the post-selection intervals are set as

$$\begin{aligned} S_Z^y =& \{\phi \in [0, 2\pi], \\ & \theta \in \{[\theta_x - \triangle\theta_Z, \theta_x + \triangle\theta_Z] \cap [0, \pi]\}, \\ & y \in \{\mathrm{vac}, d, s\}, \theta_x \in \{0, \pi\}\}, \end{aligned} \tag{7}$$

$$\begin{aligned} S_{X/Y}^y =& \Big\{ \phi \in [\phi_x - \triangle\phi_{X/Y}, \phi_x + \triangle\phi_{X/Y}], \\ & \theta \in \left[\frac{\pi}{2} - \triangle\theta_{X/Y}, \frac{\pi}{2} + \triangle\theta_{X/Y}\right], \\ & y \in \{\mathrm{vac}, d, s\}, \phi_x \in \{0, \pi\} \text{ or } \left\{\frac{\pi}{2}, \frac{3\pi}{2}\right\} \Big\}, \end{aligned} \tag{8}$$

where the subscript $X/Y/Z$ indicates the basis selection, and the superscript y represents the intensity intervals $\{\mathrm{vac}\ (\mathrm{vacuum}), d\ (\mathrm{decoy}), s\ (\mathrm{signal})\}$. $\triangle\theta_Z$, $\triangle\theta_{X/Y}$, and $\triangle\phi_{X/Y}$ characterize the size of the interval. When $\theta_x = 0$ (π), the output state is denoted as $|H\rangle$ $(|V\rangle)$. When ϕ_x takes the values $0, \pi, \frac{\pi}{2}, \frac{3\pi}{2}$, the corresponding output states are denoted as $|D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$, $|A\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$, $|R\rangle = \frac{1}{\sqrt{2}}(|H\rangle + \mathrm{i}|V\rangle)$, and $|L\rangle = \frac{1}{\sqrt{2}}(|H\rangle - \mathrm{i}|V\rangle)$. Among them, $\mathrm{vac} = [0, I_v], d = (I_v, I_d], s = (I_d, I_s]$, and I_v, I_d, I_s are the boundaries of three intervals.

2.2 Fully passive RFI QKD protocol

The fully passive RFI QKD protocol includes the following four steps.

Step 1. Preparation of the initial states. Alice first prepares a large number of the initial states with random quantum states and intensities from a fully passive source. Through post-selection, Alice filters out the photons within the S_Z^y, S_X^y, and S_Y^y intervals and sends them to Bob through a quantum channel.

Step 2. Measurement. After Bob receives the photons, he randomly measures the received photons using the Z_B, X_B, or Y_B basis. Among them, we assume that the $Z_{A(B)}$ basis used by Alice and Bob is well aligned, and there is a misalignment β between the X and Y bases as

$$Z_B = Z_A,$$

$$\begin{aligned} X_B &= \cos\beta X_A + \sin\beta Y_A, \\ Y_B &= \cos\beta Y_A - \sin\beta X_A. \end{aligned} \tag{9}$$

Step 3. Parameter estimation. Alice and Bob announce the preparation and measurement basis for each photon and perform the basis comparison. In the case where both Alice and Bob choose the Z basis, Bob will randomly select a portion of these measurement results for key generation and use the rest for parameter estimation. The cases where Alice and Bob choose the X or Y basis are used to estimate Eve's eavesdropping. The cases where one party chooses the Z basis, while the other party chooses the X or Y basis, should be discarded. By estimating the security parameters in different cases, Alice and Bob are able to obtain the secure key rate. Alice and Bob repeat the above three steps until they generate enough keys.

Step 4. Error correction and privacy amplification. Alice and Bob conduct error correction and privacy amplification according to the estimated parameters to obtain the final secure keys.

3 Fully passive RFI QKD protocol's performance under practical experimental conditions

3.1 The formula of the secure key rate

In [57], Laing et al. provided the information entropy that the eavesdropper Eve can intercept in the case of a single photon in the RFI QKD as

$$\mathrm{IE}_1 = (1 - e^1_{Z_AZ_B})h\left(\frac{1+u}{2}\right) + e^1_{Z_AZ_B}h\left(\frac{1+v}{2}\right), \tag{10}$$

where $e^1_{Z_AZ_B}$ is the single-photon error rate when Alice sends photons in the Z_A basis and Bob measures them using the Z_B basis, $h(x)$ is defined as the binary Shannon entropy, given by $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$, and

$$u = \min\left(\frac{\sqrt{C/2}}{1 - e^1_{Z_AZ_B}}, 1\right), \tag{11}$$

$$v = \frac{\sqrt{C/2 - (1 - e^1_{Z_AZ_B})^2u^2}}{e^1_{Z_AZ_B}}. \tag{12}$$

Here, C is a β-independent parameter defined as

$$\begin{aligned} C &= \langle X_AX_B\rangle^2 + \langle X_AY_B\rangle^2 + \langle Y_AX_B\rangle^2 + \langle Y_AY_B\rangle^2 \\ &= (1-2e^1_{X_AX_B})^2 + (1-2e^1_{X_AY_B})^2 + (1-2e^1_{Y_AX_B})^2 + (1-2e^1_{Y_AY_B})^2, \end{aligned} \tag{13}$$

where $e^1_{\xi_A\xi_B}$ is the single-photon error rate when Alice sends photons in the ξ_A basis and Bob measures them using the ξ_B basis, and $\xi_A \in \{Z_A, X_A, Y_A\}$, $\xi_B \in \{Z_B, X_B, Y_B\}$. Since $Z_A = Z_B$, we abbreviate them as Z in the following text.

In an ideal situation, the secure key rate of the fully passive RFI QKD protocol with infinite key can be written as

$$R = \langle P\rangle_{S^s_Z} P_Z(\langle P(1)\rangle_{S^s_Z}\langle Y^1_Z\rangle_{S^s_Z}(1 - \mathrm{IE}_1) - f_e\langle Q_Z\rangle_{S^s_Z} h(\langle E_Z\rangle_{S^s_Z})), \tag{14}$$

where $\langle P\rangle_{S^s_Z}$ is the probability that Alice generates photons in the interval S^s_Z and P_Z represents the probability that Bob measures them using the Z basis. $\langle P(1)\rangle_{S^s_Z}\ \langle Y^1_Z\rangle_{S^s_Z}$ is the single-photon gain that Alice generates single-photon states in the interval S^s_Z and Bob selects the Z basis for measurement and obtains a response. f_e is the error correction coefficient. $\langle Q_Z\rangle_{S^s_Z}$ ($\langle E_Z\rangle_{S^s_Z}$) is the overall gain (error rate) when Alice generates states in the interval S^s_Z and Bob selects the Z basis for measurement.

However, in practical experiments, it is not realistic to generate an infinitely long key. It is necessary to analyze the secure key rate of the system under the condition of a finite key length. According to [65, 72], the formula for the secure key length against coherent attack is

$$l = \Bigg\lfloor M^L_{S^s_Z Z,1}(1 - \mathrm{IE}_1) - \lambda_{EC} - \log\left(\frac{2}{\epsilon_{EC}\epsilon^2_{PA}}\right)$$

$$-7M^U_{S^s_Z Z}\sqrt{\frac{\log_2(2/\bar{\epsilon})}{M^L_{S^s_Z Z}}}-30\log_2(N+1)\Bigg\rfloor, \tag{15}$$

where $M^L_{S^s_Z Z,1}$ is the lower bound of the single-photon state response count when generating the key. IE_1 is the information entropy that Eve can obtain from a single-photon state within the framework of the RFI, as shown in (10). λ_{EC} represents the information entropy that needs to be consumed for error correction and $\lambda_{EC} = f_e M^U_{S^s_Z Z} h(E^U_{S^s_Z Z})$. Among them, f_e is the error correction coefficient, and $M^U_{S^s_Z Z}$ ($E^U_{S^s_Z Z}$) is the upper bound of the total response count (error rate) of the key basis (ZZ). ϵ_{EC} (ϵ_{PA}) denotes the probability that error correction (privacy amplification) fails. $\bar{\epsilon}$ denotes the accuracy of smooth min-entropy estimation. N denotes the total number of pulses generated by the fully passive source. Since the key length should be an integer, the entire expression ultimately needs to be rounded down ($\lfloor\rfloor$).

3.2 The overall gain Q and error rate E

Here, we analyze the overall gain Q and error rate E of the protocol under theoretical circumstances. According to Subsection 2.1, the pulse emitted by the light source can be expressed as

$$\rho_{out} = \frac{1}{2\pi}\int_0^{2\pi}|\mu_{out}\rangle\langle\mu_{out}|d\psi = \sum_{n=0}^{\infty}P(I,n)|n\rangle_{a^\dagger(\theta,\phi)}\langle n|. \tag{16}$$

$P(I,n)$ is the probability that the source emits n photons, which follows a Poisson distribution $P(I,n)=\mathrm{e}^{-I}\frac{I^n}{n!}$. Consider a fiber loss channel with a transmission efficiency of $\eta_c = 10^{-\frac{\alpha L}{10}}$, where α is the fiber attenuation coefficient and L is the photon transmission distance. After the output state passes through the channel, it becomes

$$\rho = \sum_{n=0}^{\infty}P(I\eta_c,n)|n\rangle_{a^\dagger(\theta,\phi)}\langle n|. \tag{17}$$

The formula can be understood as that at Bob's end, there is a probability of $P(I\eta_c,n)$ to receive an n-photon state $|n\rangle_{a^\dagger(\theta,\phi)}$. Next, the n-photon state will be measured by projecting in the Z_B, X_B, Y_B bases. Note that the eigenstates of the Z_B, X_B, Y_B bases are $\{|H\rangle,|V\rangle\}$, $\{|D'\rangle=\frac{1}{\sqrt{2}}(|H\rangle+\mathrm{e}^{\mathrm{i}\beta}|V\rangle), |A'\rangle=\frac{1}{\sqrt{2}}(|H\rangle-\mathrm{e}^{\mathrm{i}\beta}|V\rangle)\}$, $\{|R'\rangle=\frac{1}{\sqrt{2}}(|H\rangle+\mathrm{i}\mathrm{e}^{\mathrm{i}\beta}|V\rangle), |L'\rangle=\frac{1}{\sqrt{2}}(|H\rangle-\mathrm{i}\mathrm{e}^{\mathrm{i}\beta}|V\rangle)\}$, respectively. When expanded in these bases, the n-photon state becomes

$$\begin{aligned}
|n\rangle_{a^\dagger(\theta,\phi)} &= \frac{1}{\sqrt{n!}}(a^\dagger(\theta,\phi))^n|\mathrm{vac}\rangle \\
&= \frac{1}{\sqrt{n!}}\left(\cos\frac{\theta}{2}a_H^\dagger+\mathrm{e}^{\mathrm{i}\phi}\sin\frac{\theta}{2}a_V^\dagger\right)^n|\mathrm{vac}\rangle \\
&= \frac{1}{\sqrt{n!}}(f(x)a_x^\dagger+f(y)a_y^\dagger)^n|\mathrm{vac}\rangle \\
&= \frac{1}{\sqrt{n!}}\sum_{m=0}^{n}C_n^m(f(x)a_x^\dagger)^m(f(y)a_y^\dagger)^{n-m}|\mathrm{vac}\rangle \\
&= \frac{1}{\sqrt{n!}}\sum_{m=0}^{n}C_n^m f(x)^m f(y)^{n-m}\sqrt{m!(n-m)!}|m\rangle_x|n-m\rangle_y, && (18)\\
(x,y) &\in \{(H,V),(D',A'),(R',L')\}, && (19)
\end{aligned}$$

where

$$\begin{aligned}
a^\dagger(\theta,\phi) &= \cos\frac{\theta}{2}a_H^\dagger+\mathrm{e}^{\mathrm{i}\phi}\sin\frac{\theta}{2}a_V^\dagger \\
&= f(H)a_H^\dagger+f(V)a_V^\dagger \\
&= \frac{1}{\sqrt{2}}\left(\cos\frac{\theta}{2}+\mathrm{e}^{\mathrm{i}(\phi-\beta)}\sin\frac{\theta}{2}\right)a_{D'}^\dagger+\frac{1}{\sqrt{2}}\left(\cos\frac{\theta}{2}-\mathrm{e}^{\mathrm{i}(\phi-\beta)}\sin\frac{\theta}{2}\right)a_{A'}^\dagger \\
&= f(D')a_{D'}^\dagger+f(A')a_{A'}^\dagger
\end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{\sqrt{2}}\left(\cos\frac{\theta}{2} - \mathrm{i}\mathrm{e}^{\mathrm{i}(\phi-\beta)}\sin\frac{\theta}{2}\right)a_{R'}^{\dagger} + \frac{1}{\sqrt{2}}\left(\cos\frac{\theta}{2} + \mathrm{i}\mathrm{e}^{\mathrm{i}(\phi-\beta)}\sin\frac{\theta}{2}\right)a_{L'}^{\dagger} \\
&= f(R')a_{R'}^{\dagger} + f(L')a_{L'}^{\dagger},
\end{aligned} \tag{20}
$$

and

$$
\begin{aligned}
&|f(H)|^2 = \frac{1+\cos\theta}{2}, \quad |f(V)|^2 = \frac{1-\cos\theta}{2}, \\
&|f(D')|^2 = \frac{1+\sin\theta\cos(\phi-\beta)}{2}, \\
&|f(A')|^2 = \frac{1-\sin\theta\cos(\phi-\beta)}{2}, \\
&|f(R')|^2 = \frac{1+\sin\theta\sin(\phi-\beta)}{2}, \\
&|f(L')|^2 = \frac{1-\sin\theta\sin(\phi-\beta)}{2}.
\end{aligned} \tag{21}
$$

According to (18), the probability that it generates the state $|m\rangle_x|n-m\rangle_y$ is $P_{m,n-m} = C_n^m\,|f(x)|^{2m}|f(y)|^{2(n-m)}$. Then, the probability that the n-photon state causes the detector x to respond is

$$
\begin{aligned}
Y_{n,x} &= \sum_{m=0}^{n} P_{m,n-m}Y_{m,n-m}^{x} \\
&= \sum_{m=0}^{n} C_n^m|f(x)|^{2m}|f(y)|^{2(n-m)}(1-(1-\eta_d)^m(1-Pd))(1-\eta_d)^{n-m}(1-Pd) \\
&= (1-Pd)(|f(x)|^2+(1-\eta_d)|f(y)|^2)^n - (1-Pd)^2(1-\eta_d)^n \\
&= (1-Pd)(1-\eta_d|f(y)|^2)^n - (1-Pd)^2(1-\eta_d)^n,
\end{aligned} \tag{22}
$$

and the probability that the detector y responds is

$$
Y_{n,y} = (1-Pd)(1-\eta_d|f(x)|^2)^n - (1-Pd)^2(1-\eta_d)^n, \tag{23}
$$

where η_d is the detection efficiency of the detector, and Pd is the dark count rate.

The overall gain Q can be calculated as

$$
\begin{aligned}
Q_{\xi_B} &= Q_x + Q_y, \\
Q_x &= \sum_{n=0}^{\infty} P(I\eta_c, n)Y_{n,x} \\
&= \sum_{n=0}^{\infty} \mathrm{e}^{-I\eta_c}\frac{(I\eta_c)^n}{n!}((1-Pd)(1-\eta_d|f(y)|^2)^n - (1-Pd)^2(1-\eta_d)^n) \\
&= (1-Pd)\mathrm{e}^{-I\eta_c\eta_d|f(y)|^2} - (1-Pd)^2\mathrm{e}^{-I\eta_c\eta_d}, \\
Q_y &= (1-Pd)\mathrm{e}^{-I\eta_c\eta_d|f(x)|^2} - (1-Pd)^2\mathrm{e}^{-I\eta_c\eta_d},
\end{aligned} \tag{24}
$$

where the subscript ξ_B represents the measurement basis of Bob.

Then, the error rate of state $|x\rangle$ will be

$$
E_{\xi_B,x} = \frac{e_dQ_x + (1-e_d)Q_y}{Q_{\xi_B}}, \tag{25}
$$

where e_d is the optical intrinsic error rate.

Since the photons generated by the passive source are not perfect and a certain deviation is allowed, we need to integrate the overall gain and the error rate within the post-selection interval as

$$
\langle Q_{\xi_B}\rangle_{S_{\xi_A}^{y}} = \frac{1}{\langle P\rangle_{S_{\xi_A}^{y}}}\iiint_{S_{\xi_A}^{y}} Q_{\xi_B} f(I,\theta,\phi)dId\theta d\phi, \tag{26}
$$

$$\langle E_{\xi_B}\rangle_{S^y_{\xi_A}} = \frac{1}{\langle P\rangle_{S^y_{\xi_A}}}\iiint_{S^y_{\xi_A}} E_{\xi_B,x} f(I,\theta,\phi) dId\theta d\phi, \tag{27}$$

$$\langle P\rangle_{S^y_{\xi_A}} = \iiint_{S^y_{\xi_A}} f(I,\theta,\phi) dId\theta d\phi, \tag{28}$$

where $\langle P\rangle_{S^y_{\xi_A}}$ is the normalization coefficient. $f(I,\theta,\phi)$ is the probability density function that describes the distribution of the output state on the Bloch sphere, and [49]

$$\begin{aligned} &f(I,\theta,\phi) = f(I,\theta)f(\phi),\\ &f(\phi) = \frac{1}{2\Delta\phi},\\ &f(I,\theta) = \frac{1}{2vt\pi^2\sqrt{1-\frac{I}{2vt}\cos^2\frac{\theta}{2}}\sqrt{1-\frac{I}{2vt}\sin^2\frac{\theta}{2}}}. \end{aligned} \tag{29}$$

3.3 Parameter estimation

In a practical QKD system, we need to estimate the error rate and the overall gain based on the statistical results of the detector responses. Different from the case of an infinitely long key, under the condition of a finite key length, there are usually some fluctuations in this statistical result. Regarding the measurement as a series of Bernoulli random variables, its statistical deviation can be described by Kato's inequality [50], and we have

$$K^L_{N,\epsilon}(\Lambda_N) \overset{\epsilon}{\leqslant} S_N \overset{\epsilon}{\leqslant} K^U_{N,\epsilon}(\Lambda_N), \tag{30}$$

$$K^L_{N,\epsilon}(\Lambda_N) = \Lambda_N - (b + a(2\Lambda_N/N - 1))\sqrt{N}, \tag{31}$$

$$K^U_{N,\epsilon}(\Lambda_N) = \Lambda_N + (d + c(2\Lambda_N/N - 1))\sqrt{N}, \tag{32}$$

where S_N represents the expected value, Λ_N represents the actual statistical value, and ϵ represents the confidence level. Eq. (30) indicates that the probability of S_N being between $K^L_{N,\epsilon}(\Lambda_N)$ and $K^U_{N,\epsilon}(\Lambda_N)$ is more than $1-\epsilon$, and ϵ is usually an extremely small number. N is the total number of statistical counts. a, b, c, and d are coefficients related to N, Λ_N, ϵ, and the specific formula is given in Appendix A.

Similarly, through the expected value, we can also estimate the upper and lower bounds of the statistical values, given by [50]

$$\bar{K}^L_{N,\epsilon}(S_N) \overset{\epsilon}{\leqslant} \Lambda_N \overset{\epsilon}{\leqslant} \bar{K}^U_{N,\epsilon}(S_N), \tag{33}$$

$$\bar{K}^L_{N,\epsilon}(S_N) = (\sqrt{N}S_N + N(e-f))/(2e+\sqrt{N}), \tag{34}$$

$$\bar{K}^U_{N,\epsilon}(S_N) = (\sqrt{N}S_N + N(g-h))/(\sqrt{N}-2g), \tag{35}$$

where e, f, g, and h are coefficients related to N, S_N, ϵ, and the specific formula is given in Appendix A.

According to the above formulas, we can estimate the parameters in (15). The following are the details of the estimation.

3.3.1 *The lower bound of* $M_{S^s_Z Z,1}$

$M_{S^s_Z Z,1}$ is the single-photon response count, and it is defined as

$$M_{S^s_Z Z,1} = N\langle P\rangle_{S^s_Z} P_Z \langle P(I,1)\rangle_{S^s_Z} \langle Y^1_Z\rangle^L_{S^s_Z}, \tag{36}$$

where N is the total number of pulses generated by the fully passive source. $\langle P\rangle_{S^s_Z}$ is the probability that Alice generates photons in the Z basis, and can be calculated with (28). P_Z is the probability that Bob selects the Z basis for measurement. $\langle P(I,1)\rangle_{S^s_Z}$ is the probability that the source generates single photons in the form of

$$\langle P(I,n)\rangle_{S^y_{\xi_A}} = \iiint_{S^y_{\xi_A}} \frac{I^n \mathrm{e}^{-I}}{n!} f(I,\theta,\phi) dId\theta d\phi. \tag{37}$$

$\langle Y^1_Z\rangle^L_{S^s_Z}$ is the yield of a single-photon state, and can be estimated with the decoy state method. We can solve the following linear programming problem [50]:

$$\langle Y^1_{\xi_B}\rangle^L_{S^s_{\xi_A}} = \min \langle Y^1_{\xi_B}\rangle_{S^s_{\xi_A}}, \tag{38}$$

$$\langle Y^1_{\xi_B}\rangle^U_{S^s_{\xi_A}} = \max\langle Y^1_{\xi_B}\rangle_{S^s_{\xi_A}}, \tag{39}$$

$$\begin{aligned}
\text{s.t.}\quad & \langle\overline{Q_{\xi_B}}\rangle_{S^j_{\xi_A}} \geqslant \sum_{n=0}^{n_{cut}}\langle P(I,n)\rangle_{S^j_{\xi_A}}\langle Y^n_{\xi_B}\rangle_{S^j_{\xi_A}}, \\
& \langle\overline{Q_{\xi_B}}\rangle_{S^j_{\xi_A}} \leqslant \sum_{n=0}^{n_{cut}}\langle P(I,n)\rangle_{S^j_{\xi_A}}\langle Y^n_{\xi_B}\rangle_{S^j_{\xi_A}} + 1 - \sum_{n=0}^{n_{cut}}\langle P(I,n)\rangle_{S^j_{\xi_A}}, \\
& |\langle Y^n_{\xi_B}\rangle_{S^i_{\xi_A}} - \langle Y^n_{\xi_B}\rangle_{S^j_{\xi_A}}| \leqslant D(\sigma^n_{S^i_{\xi_A}}, \sigma^n_{S^j_{\xi_A}}),\ n = 2,\ldots,n_{cut}, \\
& \langle Y^n_{\xi_B}\rangle_{S^i_{\xi_A}} = \langle Y^n_{\xi_B}\rangle_{S^j_{\xi_A}},\ n = 0,1, \\
& 0 \leqslant \langle Y^n_{\xi_B}\rangle_{S^j_{\xi_A}} \leqslant 1,\ n = 0,1,\ldots,n_{cut}, \\
& \frac{K^L_{N_j,\epsilon}(M_{S^j_{\xi_A}\xi_B})}{N\langle P\rangle_{S^s_{\xi_A}}P_{\xi_B}} \leqslant \langle\overline{Q_{\xi_B}}\rangle_{S^j_{\xi_A}} \leqslant \frac{K^U_{N_j,\epsilon}(M_{S^j_{\xi_A}\xi_B})}{N\langle P\rangle_{S^s_{\xi_A}}P_{\xi_B}}, \\
& i,j \in \{v,d,s\},
\end{aligned} \tag{40}$$

where $D(\sigma^n_{S^i_{\xi_A}}, \sigma^n_{S^j_{\xi_A}})$ is the trace distance, and is equal to $\sum|\lambda_i|$. λ_i are the eigenvalues of density matrix $(\sigma^n_{S^i_{\xi_A}} - \sigma^n_{S^j_{\xi_A}})$.

$$\sigma^n_{S^i_{\xi_A}} = \iiint_{S^i_{\xi_A}} |n\rangle\langle n|_{a^\dagger(\theta,\phi)} f(I,\theta,\phi)dId\theta d\phi. \tag{41}$$

$N_j = N\langle P\rangle_{S^j_{\xi_A}}P_{\xi_B}$, and $M_{S^j_{\xi_A}\xi_B} = N\langle P\rangle_{S^j_{\xi_A}}P_{\xi_B}\ \langle Q_{\xi_B}\rangle_{S^j_{\xi_A}}$. When $\xi_A = \xi_B = Z$, and $j = s$, the solution of the linear programming (38) is $\langle Y^1_Z\rangle^L_{S^s_Z}$. Under the infinite-key scenario, the parameter $\langle\overline{Q_{\xi_B}}\rangle_{S^j_{\xi_A}}$ equals $\langle Q_{\xi_B}\rangle_{S^j_{\xi_A}}$. At this point, the solution obtained via linear programming corresponds to the single-photon yield for the infinite-key scenario. In this specific scenario, by leveraging (34) in conjunction with (36), we are able to determine the lower bound of $M_{S^s_Z Z,1}$ under the condition of a finite length as

$$M^L_{S^s_Z Z_B,1} = \bar{K}^L_{N_j,\epsilon}(M_{S^s_Z Z_B,1}). \tag{42}$$

3.3.2 *The upper bound of* IE_1

According to (10)–(12), IE_1 is related to C and e^1_{ZZ}. We need to estimate the upper bound of e^1_{ZZ} and the lower bound of C. According to (13), the lower bound of C can be calculated as

$$C^L = C^L_{X_AX_B} + C^L_{X_AY_B} + C^L_{Y_AX_B} + C^L_{Y_AY_B}, \tag{43}$$

where

$$C^L_{\xi_A\xi_B} = \begin{cases} (1-2e^{1,U}_{\xi_A\xi_B})^2, & \text{if } e^{1,L}_{\xi_A\xi_B} \geqslant 0.5, \\ (1-2e^{1,L}_{\xi_A\xi_B})^2, & \text{if } e^{1,U}_{\xi_A\xi_B} < 0.5, \\ 0, & \text{otherwise,} \end{cases} \tag{44}$$

where $e^{1,U}_{\xi_A\xi_B}$ and $e^{1,L}_{\xi_A\xi_B}$ are respectively the upper bound and the lower bound of $e^1_{\xi_A\xi_B}$, and can be calculated as

$$\begin{aligned} e^{1,U}_{\xi_A\xi_B} &= \frac{m^U_{S^s_Z Z_B,1}}{M^L_{S^s_Z Z_B,1}}, \\ e^{1,L}_{\xi_A\xi_B} &= \frac{m^L_{S^s_Z Z_B,1}}{M^U_{S^s_Z Z_B,1}}, \end{aligned} \tag{45}$$

where $m^U_{S^s_Z Z_B,1}$ and $m^L_{S^s_Z Z_B,1}$ are respectively the upper bound and the lower bound of the single-photon error response count. $M^U_{S^s_Z Z_B,1}$ and $M^L_{S^s_Z Z_B,1}$ are respectively the upper bound and the lower bound of the single-photon response count. And

$$m^{U(L)}_{S^s_{\xi_A}\xi_B,1} = \bar{K}^{U(L)}_{N,\epsilon}(m^{U(L)}),$$

$$
\begin{aligned}
&m^{U(L)} = N\langle P\rangle_{S^s_{\xi_A}} P_{\xi_B} \langle P(I,1)\rangle_{S^s_{\xi_A}} \langle e^1_{\xi_B} Y^1_{\xi_B}\rangle^{U(L)}_{S^s_{\xi_A}},\\
&M^{U(L)}_{S^s_{\xi_A}\xi_B,1} = \bar{K}^{U(L)}_{N,\epsilon}(M^{U(L)}),\\
&M^{U(L)} = N\langle P\rangle_{S^s_{\xi_A}} P_{\xi_B} \langle P(I,1)\rangle_{S^s_{\xi_A}} \langle Y^1_{\xi_B}\rangle^{U(L)}_{S^s_{\xi_A}}.
\end{aligned}
\tag{46}
$$

$\langle Y^1_{\xi_B}\rangle^{U(L)}_{S^s_{\xi_A}}$ can be obtained by solving the linear programming problem of (38) and (39). $\langle e^1_{\xi_B} Y^1_{\xi_B}\rangle^{U(L)}_{S^s_{\xi_A}}$ can be estimated with the following linear programming problem [50]:

$$\langle e^1_{\xi_B} Y^1_{\xi_B}\rangle^{L}_{S^s_{\xi_A}} = \min\langle e^1_{\xi_B} Y^1_{\xi_B}\rangle_{S^s_{\xi_A}}, \tag{47}$$

$$\langle e^1_{\xi_B} Y^1_{\xi_B}\rangle^{U}_{S^s_{\xi_A}} = \max\langle e^1_{\xi_B} Y^1_{\xi_B}\rangle_{S^s_{\xi_A}}, \tag{48}$$

$$
\begin{aligned}
\text{s.t.}\quad &\langle\overline{E_{\xi_B} Q_{\xi_B}}\rangle_{S^j_{\xi_A}} \geqslant \sum_{n=0}^{n_{cut}} \langle P(I,n)\rangle_{S^j_{\xi_A}} \langle e^n_{\xi_B} Y^n_{\xi_B}\rangle_{S^j_{\xi_A}},\\
&\langle\overline{E_{\xi_B} Q_{\xi_B}}\rangle_{S^j_{\xi_A}} \leqslant \sum_{n=0}^{n_{cut}} \langle P(I,n)\rangle_{S^j_{\xi_A}} \langle e^n_{\xi_B} Y^n_{\xi_B}\rangle_{S^j_{\xi_A}} + 1 - \sum_{n=0}^{n_{cut}} \langle P(I,n)\rangle_{S^j_{\xi_A}},\\
&|\langle e^n_{\xi_B} Y^n_{\xi_B}\rangle_{S^i_{\xi_A}} - \langle e^n_{\xi_B} Y^n_{\xi_B}\rangle_{S^j_{\xi_A}}| \leqslant D(\sigma^n_{S^i_x}, \sigma^n_{S^j_x}), n=1,\ldots,n_{cut},\\
&\langle e^0_{\xi_B} Y^0_{\xi_B}\rangle_{S^i_{\xi_A}} = \langle e^0_{\xi_B} Y^0_{\xi_B}\rangle_{S^j_{\xi_A}},\\
&0 \leqslant \langle e^n_{\xi_B} Y^n_{\xi_B}\rangle_{S^j_{\xi_A}} \leqslant 1,\ n=0,1,\ldots,n_{cut},\\
&\frac{K^L_{N_j,\epsilon}(m_{S^j_{\xi_A}\xi_B})}{N\langle P\rangle_{S^s_{\xi_A}} P_{\xi_B}} \leqslant \langle\overline{E_{\xi_B} Q_{\xi_B}}\rangle_{S^j_{\xi_A}} \leqslant \frac{K^U_{N_j,\epsilon}(m_{S^j_{\xi_A}\xi_B})}{N\langle P\rangle_{S^s_{\xi_A}} P_{\xi_B}},\\
&i,j \in \{v,d,s\},
\end{aligned}
\tag{49}
$$

where x is defined in (19), S^j_x represents the post-selection interval of state x, and $m_{S^j_{\xi_A}\xi_B}{=}N\langle P\rangle_{S^j_{\xi_A}} P_{\xi_B}\langle E_{\xi_B} Q_{\xi_B}\rangle_{S^j_{\xi_A}}$. Under the infinite-key scenario, the parameter $\langle\overline{E_{\xi_B} Q_{\xi_B}}\rangle_{S^j_{\xi_A}}$ equals $\langle E_{\xi_B} Q_{\xi_B}\rangle_{S^j_{\xi_A}}$. At this point, the solution obtained via linear programming corresponds to the single-photon error rate for the infinite-key scenario.

3.3.3 *The upper bound of λ_{EC}*

λ_{EC} is the information entropy that needs to be consumed for error correction and $\lambda_{EC} = f_e M^U_{S^s_Z Z} h(E^U_{S^s_Z Z})$. Through (31) and (32), it is easy for us to conclude that

$$M^U_{S^s_Z Z} = K^U_{N_j,\epsilon}(M_{S^s_Z Z}), \tag{50}$$

$$E^U_{S^s_Z Z} = \frac{m^U_{S^s_Z Z}}{M^L_{S^s_Z Z}}, \tag{51}$$

where $M^U_{S^s_Z Z}$ and $M^L_{S^s_Z Z}$ are respectively the upper bound and the lower bound of the overall response count ($M_{S^s_Z Z}$), and $m^U_{S^s_Z Z}$ is the upper bound of the overall error response count ($m_{S^s_Z Z}$). And

$$
\begin{aligned}
m^U_{S^s_Z Z} &= K^U_{N_j,\epsilon}(m_{S^s_Z Z}),\\
M^L_{S^s_Z Z} &= K^L_{N_j,\epsilon}(M_{S^s_Z Z}),\\
M_{S^s_Z Z} &= N\langle P\rangle_{S^s_Z} P_Z \langle Q_Z\rangle_{S^s_Z},\\
m_{S^s_Z Z} &= N\langle P\rangle_{S^s_Z} P_Z \langle E_Z Q_Z\rangle_{S^s_Z}.
\end{aligned}
\tag{52}
$$

4 Numerical simulation and parameter optimization

We analyze the performance of our protocol under finite-length conditions through numerical simulations. The simulation parameters we used are the same as those in [50], including the detector detection efficiency $\eta_d = 65\%$, the fiber attenuation coefficient $\alpha = 0.2$ dB/km, and the dark count rate $Pd = 10^{-6}$. The optical intrinsic error

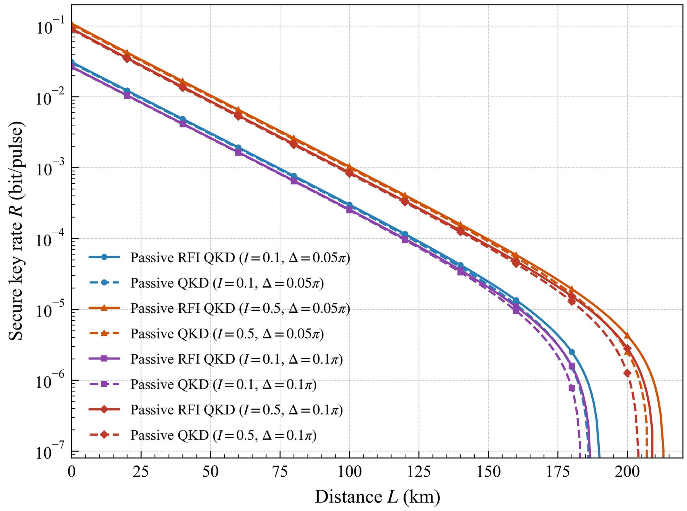

Figure 3 (Color online) Comparison of secure key rates under infinite-key and infinite-decoy-state scenarios with the same parameters for fully passive RFI QKD and fully passive QKD protocols. Solid and dashed lines correspond to fully passive RFI QKD and fully passive QKD, respectively. Different colors correspond to the four parameter sets.

rate e_d is set as 1.5%. In the decoy-state analysis, it can be seen from Figure 2 that the blue regions correspond to the post-selection interval. However, when the light source intensity exceeds a certain threshold intensity I, the probability density function $f(I,\theta)$ within this post-selection interval contains numerous singular points, which pose challenges to parameter optimization. Furthermore, the interval where intensity exceeds I is dominated by states in the X basis and Y basis; in the RFI protocol, these states are only used for parameter estimation and do not directly participate in information transmission. Thus, we choose to abandon the use of X-basis and Y-basis states when intensity exceeds I, and define the three decoy-state intervals as vac $= [0, I_v], d = (I_v, I_d], s = (I_d, I_s]$, and $I_v = 0.05I$, $I_d = 0.1I$, $I_s = I$. We set the probability that Bob chooses the Z basis for measurement as $\frac{1}{2}$, and the probabilities of choosing the X basis and the Y basis for measurement are both set as $\frac{1}{4}$. In the finite-length analysis, ϵ_{PA}, ϵ_{EC}, and $\bar{\epsilon}$ are set as 10^{-20}.

In Figure 3, we compare the secure key rates of the fully passive RFI QKD and fully passive QKD protocols under the infinite-key and infinite-decoy-state scenario with the same parameters. We set $\triangle\theta_Z = \triangle\theta_{X/Y} = \triangle\phi_{X/Y} = \triangle$, and selected two values each for the intensity I and post-selection interval $\triangle$, forming four parameter sets for the comparison. Specifically, the values of I are 0.1 and 0.5, while the values of $\triangle$ are 0.1π and 0.05π. As can be observed from the figure, under the same parameter conditions, the secure key rate of the fully passive RFI QKD protocol is consistently slightly higher than that of the fully passive QKD protocol. This is primarily because the RFI protocol utilizes more bases for eavesdropping estimation. Under the same conditions, the information entropy that Eve can obtain is lower than that of the fully passive QKD protocol.

Figure 4(a) presents the optimal performance of the fully passive RFI QKD protocol under two scenarios: one with infinite decoy states, and the other with three decoy states. Additionally, it compares our protocol with four reference protocols: the ideal actively modulated QKD protocol, the ideal RFI QKD protocol, the fully passive QKD protocol with three decoy states, and the fully passive QKD protocol with infinite decoy states. The six protocols are under an infinite-length key scenario. We define a secure key transmission rate as $R_s = \langle P\rangle_{S_Z^s} P_Z R$, which represents the amount of key that the protocol can generate using a source with a pulse frequency of 1 Hz. Here, $\langle P\rangle_{S_Z^s} P_Z$ is the probability that Alice and Bob can form a key, and R represents the information entropy of a single signal pulse which is equal to $\frac{l}{N\langle P\rangle_{S_Z^s} P_Z}$.

We optimized the intervals and intensities of these protocols, and obtained the maximum secure key transmission rate of the protocols as shown in Figure 4(a). It can be observed from the figure that the optimal secure key transmission rate of the RFI protocol is very close to that of the QKD protocol. The RFI protocol uses multiple sets of bases for parameter estimation, which can further restrict Eve's eavesdropping. Compared with the actively modulated QKD protocol, its transmission rate can be increased by approximately 5%, and its transmission distance is also improved. A similar trend applies to fully passive protocols. However, the transmission rate improvement of the fully passive RFI QKD protocol is slightly more significant compared with the fully passive QKD protocol, at around 20%. This is mainly because the RFI protocol enables stricter restrictions on Eve's eavesdropping, which in turn allows it to adopt a broader post-selection range and consequently boosts the post-selection success rate.

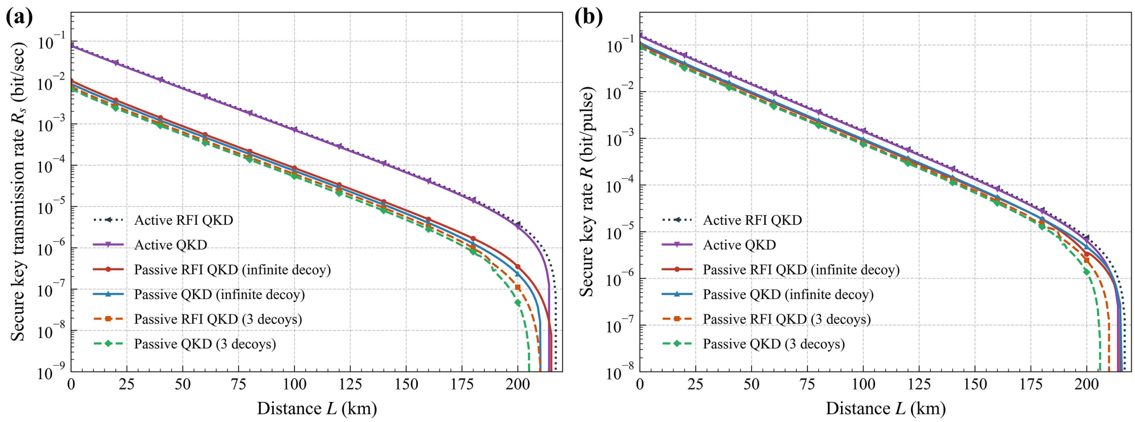

Figure 4 (Color online) Optimal performance of the fully passive RFI QKD protocol under two scenarios: one with infinite decoy states, the other with three decoy states. The comparison includes four reference protocols: the ideal actively modulated QKD protocol, the ideal RFI QKD protocol, the fully passive QKD protocol with three decoy states, and the fully passive QKD protocol with infinite decoy states. All protocols are assessed under an infinite-length key scenario. (a) The maximum secure key transmission rate R_s (in bits per second) achievable using a source with a pulse frequency of 1 Hz under optimal interval sizes and light source intensities. (b) Key transmission rate R for a single pulse when the optimal transmission rate in (a) is achieved.

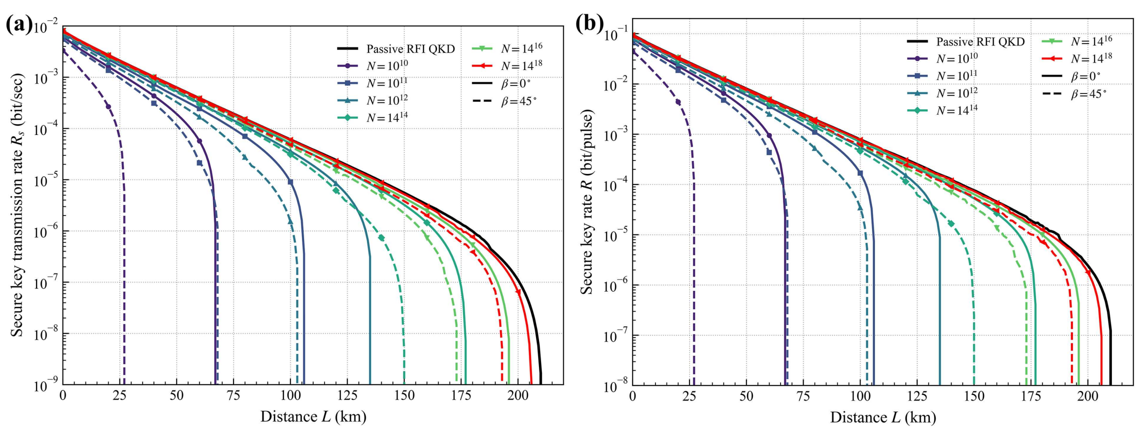

Figure 5 (Color online) Performance of our fully passive RFI QKD protocol under different numbers of pulse rounds N (total number of pulses emitted by the fully passive source). (a) Maximum secure key rate achievable using a source with a pulse frequency of 1 Hz under optimal interval sizes and light source intensities. (b) Secure key rate when the optimal transmission rate in (a) is achieved. Solid lines and dashed lines correspond to reference frame misalignment β is 0° and 45°, respectively. The red curve represents the performance of the three-decoy-state fully passive RFI QKD under the infinite-key scenario. Other colors correspond to different pulse round numbers N (i.e., $N = 10^{10}$, 10^{11}, 10^{12}, 10^{14}, 10^{16}, 10^{18}).

Additionally, its maximum transmission distance can reach 215 km, which is slightly lower than that of the actively modulated RFI QKD protocol. However, there is a large gap in transmission rate between the fully passive RFI QKD and the actively modulated RFI QKD protocols. This is mainly due to the post-selection during the light source preparation process. Since the states generated by the fully passive source are randomly distributed on the Bloch sphere, most quantum states are discarded due to post-selection failure, resulting in significant resource consumption.

Furthermore, when using three decoy states, the performance of the fully passive RFI QKD protocol decreases significantly, making it very close to the fully passive QKD protocol with three decoy states. This is primarily because the RFI protocol needs to estimate the single-photon error rates under five base combinations to calculate parameter C for eavesdropping estimation, while the QKD protocol only requires the X-basis error rate for eavesdropping estimation. At this point, the error in decoy state estimation is amplified, leading to a significant decline in the protocol's performance. In addition, as can be observed from Figure 4(b), the secure key rate of the fully passive protocol is slightly lower than that of the actively modulated protocol. This is primarily because the post-selection interval itself introduces a certain level of error rate, which in turn leads to a reduction in the key rate. However, at the optimal transmission rate, the secure key rates of the fully passive RFI protocol and the fully passive QKD protocol are comparable, with minor deviations attributed to fluctuations in parameter estimation and optimization accuracy.

We also considered the performance under finite-key scenarios. As shown in Figure 5, we compared the performance for different numbers of source pulses N. The secure key transmission rate of the fully passive protocol is jointly influenced by both the transmission distance and the number of pulse rounds N emitted by the light source. For short distances, a relatively small N is sufficient to approach the performance of the infinite-key scenario; for long distances, however, the rate decays rapidly with increasing distance. Specifically, at 50 km, when $N = 10^{11}$, the transmission rate is approximately 66.54% of that in the infinite-key scenario; when N is increased to 10^{12}, this proportion can rise to 84.64%. When N is 10^{10}, 10^{11}, and 10^{12}, respectively, the maximum transmission distances of the protocol are 67, 106, and 135 km in sequence. As the transmission distance increases, at 150 km, N must reach 10^{16} to achieve 79.00% of the infinite-key scenario's performance; even when N is increased to 10^{18} at 200 km, the rate only reaches 53.62% of that scenario's performance. The core reason for this performance decay lies in the fact that, as the communication distance increases, the post-selection interval must be gradually reduced to maintain basic performance. This in turn leads to a rapid decrease in the number of effective pulses available for parameter estimation, ultimately resulting in a significant decline in the protocol's performance under the finite-key scenario.

In addition, we present the optimal secure key transmission rate curve of the protocol when the reference frame misalignment is 45° as the dashed lines shown in Figure 5(a). Theoretically, we use the β-independent statistic C to estimate eavesdropping, and the performance of the protocol should be independent of the reference frame misalignment value. However, due to the fact that the decoy state method fails to accurately estimate the single-photon error rate, and with the influence of the finite length, the actual value of C exhibits a periodicity related to β. When the reference frame misalignment is 45°, C reaches its minimum value, and at this time, the amount of information Eve obtains is the largest. As N decreases, both the maximum communication distance and the secure key transmission rate experience significant drops. When N is 10^{10}, 10^{11}, and 10^{12}, the maximum communication distances are 27, 68, and 103 km, respectively. Figure 5(b) characterizes the secure key rate R when the optimal transmission rate in Figure 5(a) is achieved.

5 Discussion and conclusion

We currently focus on a relatively simplified scenario, assuming the reference frame remains stable over a certain period. If the reference frame undergoes continuous slow variation, as discussed in [72], the protocol's performance may change. Future research can explore how reference frames with different temporal variation characteristics affect the protocol. In addition, further investigation into accurate decoy state estimation methods and robust optimization algorithms is necessary to enhance the protocol's performance. Furthermore, MDI QKD is a highly promising research area due to its ability to resist attacks on the detector side. Previous studies have proposed a high-security MDI QKD protocol capable of resisting modulation errors and fluctuations [73]. However, this protocol still faces attack risks due to its reliance on decoy state modulation [74]. Fully passive MDI QKD [51, 52] has been proposed to address this issue. Applying the RFI framework to fully passive MDI QKD to enhance its security in mobile communication scenarios is also a promising research direction. Moreover, side channels at the source are prevalent in many quantum tasks. Thus, extending the application of fully passive sources to other quantum tasks (e.g., quantum digital signatures [75–77], quantum random number generation [78, 79]) and analyzing their specific performance in these tasks is also a promising research direction.

In conclusion, we propose a fully passive RFI QKD protocol that effectively resists side-channel attacks targeting source-side modulators by passively generating initial states. Our protocol requires that only one axis of the reference frame be aligned, which significantly reduces complexity while fortifying overall communication security. A major limitation of fully passive QKD is the inherent waste of quantum states. In the original fully passive QKD protocol, only two sets of bases are required for communication. Following post-selection, many quantum states must be discarded, which diminishes the protocol's efficiency. Our protocol employs the X and Y bases for eavesdropping estimation and the Z basis for key generation and parameter estimation, thus maximizing the utilization of quantum states produced by the fully passive source. Consequently, our protocol effectively curtails potential eavesdropping by Eve, and enhances the secure key transmission rate R_s. Under ideal circumstances, our protocol achieves a 20% improvement in secure key transmission rate compared with fully passive QKD. Under practical conditions, we must consider the finite-length effects. When the number of pulses generated by the source reaches 10^{12}, the maximum communication distances can reach 135 and 103 km at $\beta = 0°$ and $\beta = 45°$, respectively. For a GHz source, this data volume can be achieved in a matter of minutes. Our protocol contributes to the development of practical fully passive QKD systems.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 12574393, 92365110, 12175106) and Postgraduate Research & Practice Innovation Program of Jiangsu Province (Grant No. KYCX25-1129).

Supporting information Appendixes A and B. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, 1984
2 Lo H K, Curty M, Qi B. Measurement-device-independent quantum key distribution. Phys Rev Lett, 2012, 108: 130503
3 Curty M, Xu F, Cui W, et al. Finite-key analysis for measurement-device-independent quantum key distribution. Nat Commun, 2014, 5: 3732
4 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
5 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
6 Shukla C, Shukla A, Chatzinotas S, et al. Orthogonal-state-based measurement device independent quantum communication: a noise-resilient approach. AAPPS Bull, 2025, 35: 20
7 Wang P, Tian Y, Li Y M. Advances in continuous variable measurement-device-independent quantum key distribution. Sci China Inf Sci, 2025, 68: 180501
8 Curty M, Azuma K, Lo H K. Simple security proof of twin-field type quantum key distribution protocol. npj Quantum Inf, 2019, 5: 64
9 Cui C, Yin Z Q, Wang R, et al. Twin-field quantum key distribution without phase postselection. Phys Rev Appl, 2019, 11: 034053
10 Liu Y, Yu Z W, Zhang W, et al. Experimental twin-field quantum key distribution through sending or not sending. Phys Rev Lett, 2019, 123: 100505
11 Lu F Y, Yin Z Q, Wang R, et al. Practical issues of twin-field quantum key distribution. New J Phys, 2019, 21: 123030
12 Wang S, Yin Z Q, He D Y, et al. Twin-field quantum key distribution over 830-km fibre. Nat Photonics, 2022, 16: 154–161
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 Zhou L, Lin J, Xie Y M, et al. Experimental quantum communication overcomes the rate-loss limit without global phase tracking. Phys Rev Lett, 2023, 130: 250801
15 Shao S F, Zhou L, Lin J P, et al. High-rate measurement-device-independent quantum communication without optical reference light. Phys Rev X, 2025, 15: 021066
16 Luo D, Liu X, Qin K, et al. Practical asynchronous measurement-device-independent quantum key distribution with advantage distillation. Phys Rev A, 2024, 110: 022605
17 Zeng P, Zhou H, Wu W, et al. Mode-pairing quantum key distribution. Nat Commun, 2022, 13: 3903
18 Zhu H T, Huang Y, Liu H, et al. Experimental mode-pairing measurement-device-independent quantum key distribution without global phase locking. Phys Rev Lett, 2023, 130: 030801
19 Liu X, Luo D, Zhang Z, et al. Mode-pairing quantum key distribution with advantage distillation. Phys Rev A, 2023, 107: 062613
20 Acín A, Brunner N, Gisin N, et al. Device-independent security of quantum cryptography against collective attacks. Phys Rev Lett, 2007, 98: 230501
21 Pironio S, Acín A, Brunner N, et al. Device-independent quantum key distribution secure against collective attacks. New J Phys, 2009, 11: 045021
22 Nadlinger D P, Drmota P, Nichol B C, et al. Experimental quantum key distribution certified by Bell's theorem. Nature, 2022, 607: 682–686
23 Zhang W, van Leent T, Redeker K, et al. A device-independent quantum key distribution system for distant users. Nature, 2022, 607: 687–691
24 Liu W Z, Zhang Y Z, Zhen Y Z, et al. Toward a photonic demonstration of device-independent quantum key distribution. Phys Rev Lett, 2022, 129: 050502
25 Zhang Y, Chen Z, Pirandola S, et al. Long-distance continuous-variable quantum key distribution over 202.81 km of fiber. Phys Rev Lett, 2020, 125: 010502
26 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
27 Zhang G W, Chen W, Fan-Yuan G J, et al. Polarization-insensitive quantum key distribution using planar lightwave circuit chips. Sci China Inf Sci, 2022, 65: 200506
28 Ren S Y, Wang Y, Su X L. Hybrid quantum key distribution network. Sci China Inf Sci, 2022, 65: 200502
29 Feng Y, Qiu R H, Zhang K, et al. Secret key rate of continuous-variable quantum key distribution with finite codeword length. Sci China Inf Sci, 2023, 66: 180511
30 Ma L, Yang J, Zhang T, et al. Practical continuous-variable quantum key distribution with feasible optimization parameters. Sci China Inf Sci, 2023, 66: 180507
31 Yu Y, Li W, Wang L, et al. Interfering-or-not-interfering quantum key distribution. Phys Rev A, 2024, 109: 052609
32 Tian X H, Yang R, Liu H Y, et al. Experimental demonstration of drone-based quantum key distribution. Phys Rev Lett, 2024, 133: 200801
33 Xu J X, Ma X, Liu J Y, et al. Automatically identifying imperfections and attacks in practical quantum key distribution systems via machine learning. Sci China Inf Sci, 2024, 67: 202501
34 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
35 Shukla C, Rehman J, Chatzinotas S. Quantum network applications in 6G paradigm. AAPPS Bull, 2025, 35: 28
36 Gnanapandithan A, Qian L, Lo H K. Hidden multidimensional modulation side channels in quantum protocols. Phys Rev Lett, 2025, 134: 130802
37 Vakhitov A, Makarov V, Hjelme D R. Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography. J Modern Opt, 2001, 48: 2023–2038
38 Gisin N, Fasel S, Kraus B, et al. Trojan-horse attacks on quantum-key-distribution systems. Phys Rev A, 2006, 73: 022320
39 Jain N, Anisimova E, Khan I, et al. Trojan-horse attacks threaten the security of practical quantum cryptography. New J Phys, 2014, 16: 123030
40 Jain N, Stiller B, Khan I, et al. Risk analysis of Trojan-horse attacks on practical quantum key distribution systems. IEEE J Sel Top Quantum Electron, 2015, 21: 6600710
41 Lucamarini M, Choi I, Ward M B, et al. Practical security bounds against the Trojan-horse attack in quantum key distribution. Phys Rev X, 2015, 5: 031030
42 Navarrete Á, Curty M. Improved finite-key security analysis of quantum key distribution against trojan-horse attacks. Quantum Sci Technol, 2022, 7: 3

43 Luo T, Liu Q, Sun X, et al. Security analysis against the Trojan horse attack on practical polarization-encoding quantum key distribution systems. Phys Rev A, 2024, 109: 042608
44 Ivanovic I D. How to differentiate between non-orthogonal states. Phys Lett A, 1987, 123: 257–259
45 Lorenzo G C, Pereira M, Kato G, et al. A security framework for quantum key distribution implementations. ArXiv:2305.05930
46 Wang W, Wang R, Hu C, et al. Fully passive quantum key distribution. Phys Rev Lett, 2023, 130: 220801
47 Hu C, Wang W, Chan K S, et al. Proof-of-principle demonstration of fully passive quantum key distribution. Phys Rev Lett, 2023, 131: 110801
48 Lu F Y, Wang Z H, Zapatero V, et al. Experimental demonstration of fully passive quantum key distribution. Phys Rev Lett, 2023, 131: 110802
49 Zapatero V, Wang W, Curty M. A fully passive transmitter for decoy-state quantum key distribution. Quantum Sci Technol, 2023, 8: 025014
50 Zapatero V, Curty M. Finite-key security of passive quantum key distribution. Phys Rev Appl, 2024, 21: 014018
51 Li J, Wang W, Lo H K. Fully passive measurement-device-independent quantum key distribution. Phys Rev Appl, 2024, 21: 064056
52 Wang X, Lu F Y, Wang Z H, et al. Fully passive measurement-device-independent quantum key distribution. Phys Rev Appl, 2024, 21: 064067
53 Tannous R, Wu W, Vinet S, et al. Towards fully passive time-bin quantum key distribution over multi-mode channels. ArXiv:2302.05038
54 Wang W Y, Wang R, Lo H K. Fully-passive twin-field quantum key distribution. ArXiv:2304.12062
55 Li J J, Wang W Y, Chau H F. Fully passive quantum conference key agreement. ArXiv:2407.15761
56 Ying J W, Zhang Q, Gu S P, et al. Quantum secure direct communication based on fully passive source. ArXiv:2502.12652
57 Laing A, Scarani V, Rarity J G, et al. Reference-frame-independent quantum key distribution. Phys Rev A, 2010, 82: 012304
58 Zhang C M, Zhu J R, Wang Q. Practical decoy-state reference-frame-independent measurement-device-independent quantum key distribution. Phys Rev A, 2017, 95: 032309
59 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
60 Zhou Y, Ding H J, Liu J Y, et al. Finite-key security analysis against the Trojan-horse attack on practical reference-frame-independent measurement-device-independent quantum key distribution. Phys Rev Appl, 2025, 23: 024007
61 Liu J Y, Zhou X Y, Wang Q. Reference-frame-independent measurement-device-independent quantum key distribution using fewer states. Phys Rev A, 2021, 103: 022602
62 Yin H L, Fu Y. Measurement-device-independent twin-field quantum key distribution. Sci Rep, 2019, 9: 3045
63 Liu H, Wang J, Ma H, et al. Reference-frame-independent quantum key distribution using fewer states. Phys Rev Appl, 2019, 12: 034039
64 Wang J, Liu H, Ma H, et al. Experimental study of four-state reference-frame-independent quantum key distribution with source flaws. Phys Rev A, 2019, 99: 032309
65 Xie Z, Tian Z, Fan X, et al. Four-state reference-frame-independent quantum key distribution over 200 km. Phys Rev Appl, 2024, 22: 064037
66 Wang C, Sun S H, Ma X C, et al. Reference-frame-independent quantum key distribution with source flaws. Phys Rev A, 2015, 92: 042319
67 Zhang P, Aungskunsiri K, Martín-López E, et al. Reference-frame-independent quantum-key-distribution server with a telecom tether for an on-chip client. Phys Rev Lett, 2014, 112: 130501
68 Xue Y, Shi L, Chen W, et al. Improving the performance of reference-frame-independent quantum key distribution through a turbulent atmosphere. Phys Rev A, 2020, 102: 062602
69 Jin A, Zeng P, Penty R V, et al. Reference-frame-independent design of phase-matching quantum key distribution. Phys Rev Appl, 2021, 16: 034017
70 Tian Z, Xie Z, 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
71 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
72 Sheridan L, Le T P, Scarani V. Finite-key security against coherent attacks in quantum key distribution. New J Phys, 2010, 12: 123019
73 Lu F Y, Wang Z H, Yin Z Q, et al. Unbalanced-basis-misalignment-tolerant measurement-device-independent quantum key distribution. Optica, 2022, 9: 8
74 Lu F Y, Ye P, Wang Z H, et al. Hacking measurement-device-independent quantum key distribution. Optica, 2023, 10: 4
75 Yin H L, Fu Y, Li C L, et al. Experimental quantum secure network with digital signatures and encryption. Natl Sci Rev, 2022, 10: nwac228
76 Cao X Y, Li B H, Wang Y, et al. Experimental quantum e-commerce. Sci Adv, 2024, 10: eadk3258
77 Du Y, Li B H, Hua X, et al. Chip-integrated quantum signature network over 200 km. Light Sci Appl, 2025, 14: 108
78 Lin X, Wang R, Wang S, et al. Certified randomness from untrusted sources and uncharacterized measurements. Phys Rev Lett, 2022, 129: 050506
79 Du Y, Hua X, Zhao Z, et al. Source-independent quantum random number generators with integrated silicon photonics. Commun Phys, 2025, 8: 9