SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

June 2026, Vol. 69, Iss. 6, 162503:1–162503:10
https://doi.org/10.1007/s11432-025-4575-5

Reverse-encoded quantum key distribution with Gaussian-modulated coherent states

Mingxuan GUO[1], Peng HUANG[1,2,3*], Tao WANG[1,2,3] & Guihua ZENG[1,2,3,4*]

[1]*State Key Laboratory of Photonics and Communications, Institute for Quantum Sensing and Information Processing, Shanghai Jiao Tong University, Shanghai 200240, China*
[2]*Shanghai Research Center for Quantum Sciences, Shanghai 201315, China*
[3]*Hefei National Laboratory, Hefei 230088, China*
[4]*Shanghai XunTai Quantech Co., Ltd., Shanghai 200241, China*

Received 17 April 2025/Revised 13 July 2025/Accepted 28 August 2025/Published online 3 March 2026

Abstract The continuous-variable quantum key distribution (CVQKD) is of great value in the practical secure quantum cryptography. However, the signal-to-noise ratio (SNR) of the CVQKD scheme can be extremely low under high channel loss, which greatly affects the performance of key reconciliation algorithms in practical systems, resulting in low reconciliation efficiency and high frame error rate, thus making the secret key rate extremely low. Meanwhile, the low SNR puts higher requirements on the signal processing. In this paper, we present a novel reverse-encoded quantum key distribution (RE-QKD) with Gaussian-modulated coherent states (GMCS) where the encoding of raw keys is implemented by the Gaussian modulation at the Bob site instead of the Alice site, which greatly improves the SNR. We build the prepare-and-measure (PM) scheme and entanglement-based (EB) scheme for the RE-QKD protocol and conduct the security analysis under general collective attacks. The simulation results indicate that the proposed protocol can tolerate higher channel loss and excess noise compared with the conventional GMCS-CVQKD protocol. The RE-QKD protocol inherits the advantages of GMCS-CVQKD while reducing difficulties in high-performance reconciliation, facilitating the signal processing, and improving its ability to tolerate the channel loss and the excess noise, which shows its applicability in quantum communication networks.

Keywords quantum key distribution, Gaussian modulation, coherent state

Citation Guo M X, Huang P, Wang T, et al. Reverse-encoded quantum key distribution with Gaussian-modulated coherent states. Sci China Inf Sci, 2026, 69(6): 162503, https://doi.org/10.1007/s11432-025-4575-5

1 Introduction

Continuous variable quantum key distribution (CVQKD) is an efficient method for two remote users to share secret keys, which is information-theoretically secure even when facing powerful quantum computing. The common CVQKD protocols currently include the Gaussian-modulated coherent-state (GMCS) CVQKD [1–6] and discrete-modulated coherent-state (DMCS) CVQKD [7–11]. The GMCS-CVQKD and DMCS-CVQKD encode the key-related information by modulating the coherent state at the Alice site according to the Gaussian distribution and the discrete probability distribution, respectively. Both GMCS-CVQKD and DMCS-CVQKD protocols have been proved secure against individual [12–15], collective [16–22] and coherent attacks [23–26]. The secret key rates for them when considering the finite-size effect have also been evaluated [27–30]. In practical implementationsl, CVQKD has also made great progress in the long-distance implementation [31–33], the high secret key rate [34–37], and field tests [38–41].

The CVQKD protocols have the advantages of low cost, a high secret key rate, and compatibility with classical coherent optical communication facilities [42]. CVQKD protocols have also shown great potential for application in quantum metropolitan networks [39] and quantum access networks [43]. However, the high-performance reconciliation for both the GMCS-CVQKD and DMCS-CVQKD protocols is difficult due to the low signal-to-noise ratio (SNR), especially when the channel loss is high, which leads to the low reconciliation efficiency and high frame error rate, thus making the secret key rate extremely low. Meanwhile, the low SNR makes signal processing at the Bob site difficult. Moreover, theoretical secret key rates of current CVQKD protocols are sensitive to the channel loss and the excess noise, even for GMCS-CVQKD, which currently has the best performance in terms of tolerable channel loss and excess noise for CVQKD with coherent states. These characteristics limit the current

* Corresponding author (email: huang.peng@sjtu.edu.cn, ghzeng@sjtu.edu.cn)

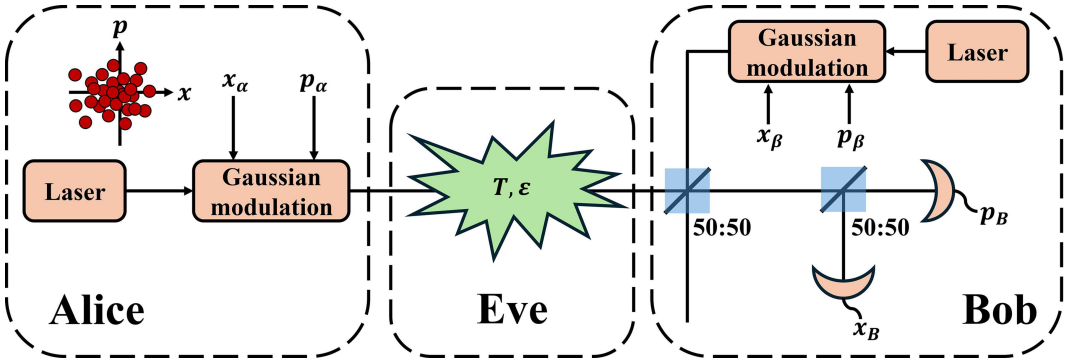

Figure 1 (Color online) The prepare-and-measure scheme for the RE-QKD protocol.

transmission distance of CVQKD protocols, which makes it difficult for CVQKD to adapt to channel environments of the satellite-to-ground channel, the submarine optical fiber channel, and so on. Although many studies have made a great contribution to extending the transmission distance of CVQKD from an engineering perspective, such as controlling the excess noise [32,44], the above physical characteristics of CVQKD protocols still greatly limit the extension of the transmission distance of CVQKD.

To solve these, we propose a reverse-encoded quantum key distribution (RE-QKD) with Gaussian-modulated coherent states, where the raw key encoding is implemented by the Gaussian modulation at the Bob site instead of the Alice site. In the proposed protocol, Alice can obtain raw keys with a high SNR, which remains approximately unchanged as the channel loss increases and is greatly improved compared with conventional CVQKD protocols. It makes the reconciliation for RE-QKD much easier and facilitates the signal processing for Bob. We give out the prepare-and-measure scheme of the RE-QKD protocol. For the security analysis of it, we also develop the entanglement-based scheme that is equivalent to the prepare-and-measure scheme. Based on the equivalent entanglement-based scheme, we analyze the secret key rate of the RE-QKD protocol under general collective attacks. The simulation results show that the RE-QKD protocol can tolerate higher channel loss and excess noise than the conventional GMCS-CVQKD protocol, both in the asymptotic limit of infinitely long keys and when considering the finite size effect.

2 RE-QKD protocol

The prepare-and-measure scheme of the RE-QKD protocol is shown in Figure 1. The specific process is as follows.

(1) Alice prepares n coherent states $|x_\alpha + p_\alpha \mathrm{i}\rangle$ according to two sets of independent Gaussian random numbers $\{x_\alpha\}$ and $\{p_\alpha\}$ with length n, where $x_\alpha, p_\alpha \sim \mathcal{N}(0, V_A^\alpha)$. Then, Alice sends them to Bob through the quantum channel with the channel loss T and the excess noise ε.

(2) Bob also prepares n coherent states $|x_\beta + p_\beta \mathrm{i}\rangle$ according to two sets of independent Gaussian random numbers $\{x_\beta\}$ and $\{p_\beta\}$ with length n, where $x_\beta, p_\beta \sim \mathcal{N}(0, V_A^\beta)$. It is noted that $\{x_\beta\}$ and $\{p_\beta\}$ are the raw key information instead of $\{x_\alpha\}$ and $\{p_\alpha\}$. Then, Bob couples these prepared coherent states with the quantum state received from the quantum channel through a 50:50 beam splitter.

(3) Bob performs heterodyne measurements on the coupled quantum state and publicly announces the measurement results $\{x_B\}$ and $\{p_B\}$.

(4) Bob randomly selects parts of the modulation information $\{x_\beta\}$ and $\{p_\beta\}$ and publishes them. According to the modulation information published by Bob, measurement results, $\{x_\alpha\}$ and $\{p_\alpha\}$, Alice executes the parameter estimation, including the channel loss, the excess noise, and the modulation variance. Then, Alice uses these parameters to estimate the secret key rate.

(5) Alice decodes the raw key information based on $\{x_\alpha\}$, $\{p_\alpha\}$ and Bob's measurement results $\{x_B\}$ and $\{p_B\}$ to obtain $\{2(x_B - \sqrt{0.25T}x_\alpha)\}$ and $\{2(p_B - \sqrt{0.25T}p_\alpha)\}$. Then, Alice and Bob share two sets of correlated raw keys (i.e., $\{2(x_B - \sqrt{0.25T}x_\alpha)\}$ and $\{x_\beta\}$, $\{2(p_B - \sqrt{0.25T}p_\alpha)\}$ and $\{p_\beta\}$).

(6) Alice and Bob discard the raw keys related to the information published in the parameter estimation process. Alice and Bob execute the reconciliation and privacy amplification on the remaining raw keys to distill the final secret keys.

It is worth noting that in order to achieve Gaussian modulation at the Bob site in the RE-QKD process, we do not need to add additional lasers in the actual implementation, because Bob can split the local oscillator light and then perform the Gaussian modulation on it. At the same time, since the light modulated with a Gaussian

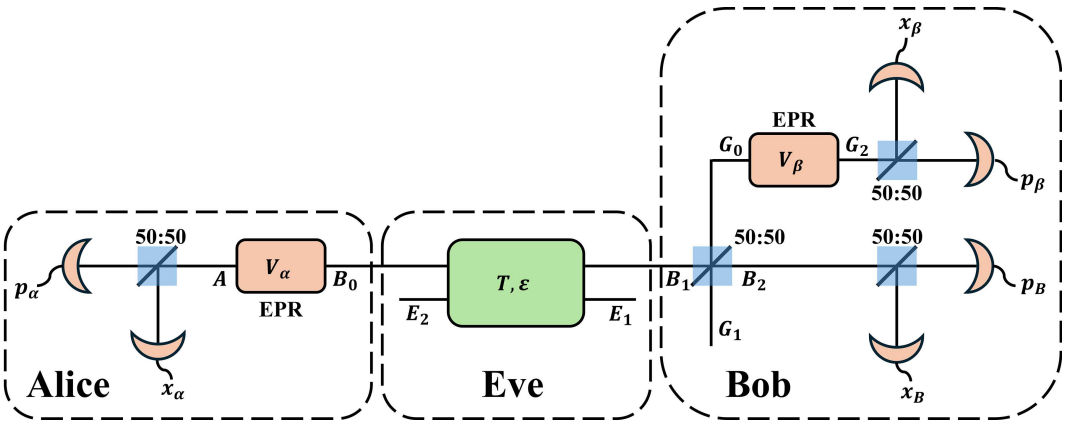

Figure 2 (Color online) The entanglement-based scheme for the RE-QKD protocol.

distribution at Bob site and the local oscillator light used for heterodyne detection are generated from the same light source, there is no rapid phase drift (caused by the laser linewidth and frequency offset) in the proposed scheme. For slow phase drift (caused by fluctuations in optical path length), it can be corrected using mature slow phase drift compensation algorithms [32, 33, 45] during data post-processing.

Although most experimental implementations of QKD adopt PM schemes, theoretical analyses are typically conducted using equivalent entanglement-based schemes, as they simplify the calculation of information leakage (e.g., simplify the calculation of related von Neumann entropy) to Eve. Thus, for calculating the secret key rate of the RE-QKD protocol, we also need to develop the entanglement-based scheme, which is equivalent to the prepare-and-measure scheme, as shown in Figure 2. If the quantum states at the input site of the quantum channel are the same for two schemes, then these two schemes are equivalent for Eve [15], as the quantum states generated by both schemes are indistinguishable for Eve. If the classical information possessed by Alice and Bob is consistent between the PM scheme and the EB scheme, then these two schemes are equivalent for Alice and Bob. If the two schemes are equivalent for Alice, Bob, and Eve, then these two schemes are equivalent. Based on the above principles, we develop the equivalent EB scheme for RE-QKD. The specific process is as follows.

(1) Alice prepares an EPR state (i.e., two-mode squeezed vacuum state (TMSV state)) with the variance $V_\alpha = V_A^\alpha + 1$. Alice performs the heterodyne detection on one mode A of the EPR state, and sends the other mode B_0 to Bob through the quantum channel with the channel loss T and the excess noise ε. After performing heterodyne detection on the mode A of the EPR state, the quantum state at B_0 is projected onto a coherent state where both the X vector and P vector follow a Gaussian distribution with variance V_A^α, which is the same as the quantum state at the input site of the quantum channel in the PM scheme. By performing a classical multiplication on the heterodyne detection result of the mode A in the EB scheme of the RE-QKD protocol, it becomes consistent with the modulation information at the Alice site in the PM scheme. Thus, this process is equivalent to the Gaussian modulation at the Alice site in the PM scheme and makes the two schemes equivalent for Eve and Alice.

(2) Bob prepares a EPR state with the variance $V_\beta = V_A^\beta + 1$. Bob performs the heterodyne detection on one mode G_2 and sends the other mode G_0 to couple with the mode B_1 received from Alice through a 50:50 beam splitter. Due to the reason similar to the above discussion, this process is equivalent to the Gaussian modulation at the Bob site in the PM scheme and makes the two schemes equivalent for Bob.

(3) Bob performs heterodyne measurements on the mode B_2 and publicly announces the measurement results $\{x_B\}$ and $\{p_B\}$.

(4) Alice and Bob perform the data post-processing similar to the process in the PM scheme, including the parameter estimation, Alice decoding the raw key, the reconciliation, and the privacy amplification.

For the convenience of readers to understand, we have detailed the process of decoding the raw key at the Alice site. In the proposed RE-QKD protocol, the raw key that Alice wants to decode is the Gaussian modulation information of Bob $\{x_\beta\}$ and $\{p_\beta\}$. For Alice, the information she has is the measurement results published by Bob $\{x_B\}$ and $\{p_B\}$, and her local Gaussian modulation information $\{x_\alpha\}$ and $\{p_\alpha\}$. Meanwhile, Figure 3 describes the quantum state before the heterodyne measurement at the Bob site (i.e., mode B_2). As shown in Figure 3, the heterodyne measurement results x_B and p_B of the quantum state at B_2 consist of three parts:

$$x_B = \sqrt{0.25T}x_\alpha + \sqrt{0.25}x_\beta + noise,$$
$$p_B = \sqrt{0.25T}p_\alpha + \sqrt{0.25}p_\beta + noise,$$

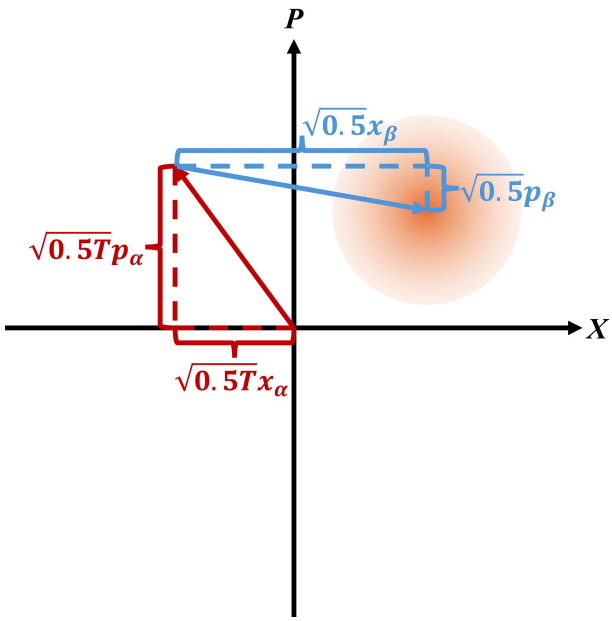

Figure 3 (Color online) The quantum state at the mode B_2.

where $noise \sim \mathcal{N}(0, 1+0.25T\varepsilon)$. Thus, Alice can decode the raw key information by performing $\{2(x_B-\sqrt{0.25T}x_\alpha)\}$ and $\{2(p_B-\sqrt{0.25T}p_\alpha)\}$. Furthermore, since Alice knows the value of x_α and p_α, and x_B and p_B are published by Bob, Alice can obtain raw keys x_β and p_β with the SNR $= \frac{0.25V_A^\beta}{1+0.25T\varepsilon}$ (it is much higher than the SNR of the conventional GMCS-CVQKD (i.e., $\frac{0.5TV_A}{1+0.5T\varepsilon}$) when the channel loss is high). However, Eve does not know the accurate value of x_α and p_α. Thus, Eve can only directly obtain the raw keys x_β and p_β with the SNR $= \frac{0.25V_A^\beta}{1+0.25T\varepsilon+0.25TV_A^\alpha}$ through the classical channel. So, as long as the information obtained from performing the joint optimal POVM for Eve on the quantum state at E_1E_2 is not greater than $\log_2(\frac{0.25V_A^\beta}{1+0.25T\varepsilon}) - \log_2(\frac{0.25V_A^\beta}{1+0.25T\varepsilon+0.25TV_A^\alpha})$, there is an information advantage between legal users against the eavesdropper and the QKD can be performed.

3 Security proof approach

In this section, we give out the security analysis of the RE-QKD protocol under general collective attacks. The basic principle of RE-QKD security analysis is to calculate the secure key rate by subtracting the leaked information to Eve from the mutual information between Alice and Bob. The leaked information to Eve consists of the information directly obtained for Eve from the measurement results published by Bob and the information obtained for Eve from performing the joint optimal POVM on the quantum state at E_1E_2. The information channels related to the above two pieces of leaked information are independent. Therefore, the leaked information is equal to the sum of the leaked information of the above two parts. For the above classical information, we can calculate it based on the SNR. For information obtained for Eve from performing the joint optimal POVM on the quantum state at E_1E_2, we can use the Holevo bound for calculation. For the Holevo bound, we can obtain it by calculating the von Neumann entropy of the quantum state at Eve's site when Bob uses different encoding values and Eve employs the optimal attack. Based on the above discussion, the total secret key rate of RE-QKD in the asymptotic limit of infinitely long keys is given by

$$K^{asy} = \beta I(A;B) - I(B;E) - \chi_{bE}, \tag{1}$$

where β represents the reconciliation efficiency and χ_{bE} represents the Holevo bound. The mutual information between Alice and Bob is given by

$$I(A;B) = \log_2\left(1 + \frac{0.25V_A^\beta}{1+0.25T\varepsilon}\right). \tag{2}$$

The classical information directly leaked from the measurement results published by Bob is given by

$$I(B;E)=\log_2\left(1+\frac{0.25V_A^{\beta}}{1+0.25T\varepsilon+0.25TV_A^{\alpha}}\right). \tag{3}$$

The information obtained for Eve from performing the joint optimal POVM on the quantum state at E_1E_2 (i.e., the Holevo bound) is given by

$$\begin{aligned}\chi_{bE}&=\int p(x_B,p_B)\chi_{bE}^{x_B,p_B}\mathrm{d}x_B\mathrm{d}p_B\\&=\int p(x_B,p_B)\left(S(\rho_E^{ther,x_B,p_B})-\int p(\nu)S(\rho_E^{\nu,x_B,p_B})\mathrm{d}\nu\right)\mathrm{d}x_B\mathrm{d}p_B,\end{aligned} \tag{4}$$

where $\chi_{bE}^{x_B,p_B}$ represents the Holevo bound in the sub-channel where the heterodyne measurement results for the mode B_2 are (x_B,p_B), ρ_E^{ther,x_B,p_B} represents the density matrix of the overall (i.e., the quantum state at the mode G_0 is a thermal state with the variance $V_\beta=V_A^{\beta}+1$) conditional quantum state at Eve when the heterodyne measurement results for the mode B_2 are (x_B,p_B) and ρ_E^{ν,x_B,p_B} represents the density matrix of the conditional quantum state at Eve when Bob encodes raw keys as $(2\Re(\nu),2\Im(\nu))$ (SNU, shot noise units) (i.e., the quantum state at the mode G_0 is a coherent state $|\nu\rangle$) and the heterodyne measurement results for the mode B_2 are (x_B,p_B). Since all the operations in the entanglement-based scheme of the RE-QKD protocol are Gaussian operations, states prepared at the Alice and Bob sites are Gaussian states, and the key information is encoded in the X and P components, the optimal attack for the RE-QKD protocol is the Gaussian attack [46] according to the optimality of Gaussian attacks. Thus, $S(\rho_E^{ther,x_B,p_B})$ and $S(\rho_E^{\nu,x_B,p_B})$ only depend on their corresponding covariance matrices. Furthermore, $S(\rho_E^{ther,x_B,p_B})$ and $S(\rho_E^{\nu,x_B,p_B})$ remain unchanged for all x_B, p_B and ν. Meanwhile, because E is the purification of AB_1, $S(\rho_E^{ther,x_B,p_B})=S(\rho_{G_1G_2A}^{ther,x_B,p_B})$ and $S(\rho_E^{\nu,x_B,p_B})=S(\rho_{G_1G_2A}^{\nu,x_B,p_B})$. Thus, Eq. (4) can be simplified as

$$\begin{aligned}\chi_{bE}&=\int p(x_B,p_B)\left(S(\rho_E^{ther,x_B,p_B})-\int p(\nu)S(\rho_E^{\nu,x_B,p_B})\mathrm{d}\nu\right)\mathrm{d}x_B\mathrm{d}p_B\\&=\int p(x_B,p_B)(S(\rho_E^{ther,x_B,p_B})-S(\rho_E^{\nu,x_B,p_B}))\mathrm{d}x_B\mathrm{d}p_B\\&=S(\rho_E^{ther,x_B,p_B})-S(\rho_E^{\nu,x_B,p_B})\\&=S(\rho_{G_1G_2A}^{ther,x_B,p_B})-S(\rho_{G_1G_2A}^{\nu,x_B,p_B}).\end{aligned} \tag{5}$$

In order to calculate the $S(\rho_{G_1G_2A}^{ther,x_B,p_B})$ and $S(\rho_{G_1G_2A}^{\nu,x_B,p_B})$, we need to obtain the covariance matrices for $\rho_{G_1G_2A}^{ther,x_B,p_B}$ and $\rho_{G_1G_2A}^{\nu,x_B,p_B}$. We can first give out covariance matrices for states at AB_1 and G_0G_2, and the symplectic matrix for the beamsplitters operation of transmittance T,

$$\gamma_{AB_1}=\begin{pmatrix}V_\alpha I_2 & \sqrt{T(V_\alpha^2-1)}\sigma_z\\ \sqrt{T(V_\alpha^2-1)}\sigma_z & (1+TV_A^{\alpha}+T\varepsilon)I_2\end{pmatrix}, \tag{6}$$

$$\gamma_{G_0G_2}^{ther}=\begin{pmatrix}V_\beta I_2 & \sqrt{V_\beta^2-1}\sigma_z\\ \sqrt{V_\beta^2-1}\sigma_z & V_\beta I_2\end{pmatrix}, \tag{7}$$

$$\gamma_{G_0G_2}^{\nu}=I_2\oplus I_2, \tag{8}$$

$$S(T)=\begin{pmatrix}\sqrt{T}I_2 & \sqrt{1-T}I_2\\ -\sqrt{1-T}I_2 & \sqrt{T}I_2\end{pmatrix}, \tag{9}$$

where $\sigma_z=\mathrm{diag}(1,-1)$. We can then further obtain covariance matrices for the state at $B_2G_1G_2A$,

$$\gamma_{AB_2G_1G_2}^{ther}=(I_A\oplus S(T=0.5)\oplus I_{G_2})(\gamma_{AB_1}\oplus\gamma_{G_0G_2}^{ther})(I_A\oplus S(T=0.5)\oplus I_{G_2})^{\mathrm{T}}, \tag{10}$$

$$\gamma_{AB_2G_1G_2}^{\nu}=(I_A\oplus S(T=0.5)\oplus I_{G_2})(\gamma_{AB_1}\oplus\gamma_{G_0G_2}^{\nu})(I_A\oplus S(T=0.5)\oplus I_{G_2})^{\mathrm{T}}, \tag{11}$$

$$\gamma_{B_2G_1G_2A}^{ther}=\begin{pmatrix}\gamma_{AB_2G_1G_2}^{ther}(3{:}8,3{:}8) & \gamma_{AB_2G_1G_2}^{ther}(3{:}8,1{:}2)\\ \gamma_{AB_2G_1G_2}^{ther}(1{:}2,3{:}8) & \gamma_{AB_2G_1G_2}^{ther}(1{:}2,1{:}2)\end{pmatrix}, \tag{12}$$

$$\gamma^{\nu}_{B_2G_1G_2A}=\begin{pmatrix}\gamma^{\nu}_{AB_2G_1G_2}(3{:}8,3{:}8) & \gamma^{\nu}_{AB_2G_1G_2}(3{:}8,1{:}2)\\ \gamma^{\nu}_{AB_2G_1G_2}(1{:}2,3{:}8) & \gamma^{\nu}_{AB_2G_1G_2}(1{:}2,1{:}2)\end{pmatrix}. \tag{13}$$

After Bob performs the heterodyne measurement on the mode B_2, we can obtain

$$\begin{aligned}\gamma^{ther,x_B,p_B}_{G_1G_2A}&=\gamma^{ther}_{B_2G_1G_2A}(3{:}8,3{:}8)\\&\quad-\gamma^{ther}_{B_2G_1G_2A}(3{:}8,1{:}2)[\gamma^{ther}_{B_2G_1G_2A}(1{:}2,1{:}2)+I_{B_2}]^{-1}[\gamma^{ther}_{B_2G_1G_2A}(3{:}8,1{:}2)]^{\mathrm{T}},\end{aligned} \tag{14}$$

$$\begin{aligned}\gamma^{\nu,x_B,p_B}_{G_1G_2A}&=\gamma^{\nu}_{B_2G_1G_2A}(3{:}8,3{:}8)\\&\quad-\gamma^{\nu}_{B_2G_1G_2A}(3{:}8,1{:}2)[\gamma^{\nu}_{B_2G_1G_2A}(1{:}2,1{:}2)+I_{B_2}]^{-1}[\gamma^{\nu}_{B_2G_1G_2A}(3{:}8,1{:}2)]^{\mathrm{T}}.\end{aligned} \tag{15}$$

Then, we can calculate the symplectic eigenvalues λ_1^{ther}, λ_2^{ther} and λ_3^{ther} for $\gamma^{ther,x_B,p_B}_{G_1G_2A}$ and λ_1^{ν}, λ_2^{ν} and λ_3^{ν} for $\gamma^{\nu,x_B,p_B}_{G_1G_2A}$,

$$\lambda^{ther}_{1,2}=\sqrt{\frac{1}{2}(\Delta_{ther}\pm\sqrt{\Delta^2_{ther}-4D^2_{ther}})},\quad \lambda^{ther}_3=1, \tag{16}$$

$$\lambda^{\nu}_{1,2}=\sqrt{\frac{1}{2}(\Delta_{\nu}\pm\sqrt{\Delta^2_{\nu}-4D^2_{\nu}})},\quad \lambda^{\nu}_3=1, \tag{17}$$

$$\begin{aligned}\Delta_{ther}=&(T^2(V_A^{\alpha})^2(V_A^{\beta})^2+6T^2(V_A^{\alpha})^2V_A^{\beta}+T^2(V_A^{\alpha})^2\varepsilon^2-2T^2(V_A^{\alpha})^2\varepsilon+10T^2(V_A^{\alpha})^2+2T^2V_A^{\alpha}(V_A^{\beta})^2\varepsilon\\&+12T^2V_A^{\alpha}V_A^{\beta}\varepsilon+2T^2V_A^{\alpha}\varepsilon^2+16T^2V_A^{\alpha}\varepsilon+T^2(V_A^{\beta})^2\varepsilon^2+6T^2V_A^{\beta}\varepsilon^2+10T^2\varepsilon^2-2T(V_A^{\alpha})^2(V_A^{\beta})^2\\&+2T(V_A^{\alpha})^2V_A^{\beta}\varepsilon-14T(V_A^{\alpha})^2V_A^{\beta}+8T(V_A^{\alpha})^2\varepsilon-24T(V_A^{\alpha})^2-2TV_A^{\alpha}(V_A^{\beta})^2+4TV_A^{\alpha}V_A^{\beta}\varepsilon\\&-12TV_A^{\alpha}V_A^{\beta}+16TV_A^{\alpha}\varepsilon-16TV_A^{\alpha}+2T(V_A^{\beta})^2\varepsilon+16TV_A^{\beta}\varepsilon+32T\varepsilon+(V_A^{\alpha})^2(V_A^{\beta})^2+8(V_A^{\alpha})^2V_A^{\beta}\\&+16(V_A^{\alpha})^2+2V_A^{\alpha}(V_A^{\beta})^2+16V_A^{\alpha}V_A^{\beta}+32V_A^{\alpha}+2(V_A^{\beta})^2+16V_A^{\beta}+32)/(V_A^{\beta}+TV_A^{\alpha}+T\varepsilon+4)^2,\end{aligned} \tag{18}$$

$$\begin{aligned}\Delta_{\nu}=&(T^2(V_A^{\alpha})^2\varepsilon^2-2T^2(V_A^{\alpha})^2\varepsilon+10T^2(V_A^{\alpha})^2+2T^2V_A^{\alpha}\varepsilon^2+16T^2V_A^{\alpha}\varepsilon+10T^2\varepsilon^2+8T(V_A^{\alpha})^2\varepsilon\\&-24T(V_A^{\alpha})^2+16TV_A^{\alpha}\varepsilon-16TV_A^{\alpha}+32T\varepsilon+16(V_A^{\alpha})^2+32V_A^{\alpha}+32)/(TV_A^{\alpha}+T\varepsilon+4)^2,\end{aligned} \tag{19}$$

$$D_{ther}=\frac{4V_A^{\alpha}+V_A^{\beta}-3TV_A^{\alpha}+V_A^{\alpha}V_A^{\beta}+3T\varepsilon-TV_A^{\alpha}V_A^{\beta}+3TV_A^{\alpha}\varepsilon+TV_A^{\beta}\varepsilon+TV_A^{\alpha}V_A^{\beta}\varepsilon+4}{V_A^{\beta}+TV_A^{\alpha}+T\varepsilon+4}, \tag{20}$$

$$D_{\nu}=\frac{4V_A^{\alpha}-3TV_A^{\alpha}+3T\varepsilon+3TV_A^{\alpha}\varepsilon+4}{TV_A^{\alpha}+T\varepsilon+4}. \tag{21}$$

Finally, we can obtain the value of the required von Neumann entropy,

$$S(\rho^{ther,x_B,p_B}_{G_1G_2A})=G\left(\frac{\lambda_1^{ther}-1}{2}\right)+G\left(\frac{\lambda_2^{ther}-1}{2}\right)+G\left(\frac{\lambda_3^{ther}-1}{2}\right), \tag{22}$$

$$S(\rho^{\nu,x_B,p_B}_{G_1G_2A})=G\left(\frac{\lambda_1^{\nu}-1}{2}\right)+G\left(\frac{\lambda_2^{\nu}-1}{2}\right)+G\left(\frac{\lambda_3^{\nu}-1}{2}\right), \tag{23}$$

where $G(x)=(x+1)\log_2(x+1)-x\log_2 x$. Then, we can use (1)–(3), (5), (16)–(23) to calculate the secret key rate of the RE-QKD protocol in the asymptotic limit of infinitely long keys. We can also give the secret key rate of the RE-QKD protocol when considering the finite-size effect [48],

$$T'=\left(\sqrt{T}-z_{\epsilon_{\mathrm{PE}}/2}\sqrt{\frac{1+T\varepsilon}{(N-n)V_A^{\alpha}}}\right)^2, \tag{24}$$

$$\varepsilon'=\left[T\varepsilon+z_{\epsilon_{\mathrm{PE}}/2}(1+T\varepsilon)\sqrt{\frac{2}{N-n}}\right]\Big/T', \tag{25}$$

$$\Delta(n)=7\sqrt{\frac{\log_2(2/\bar{\epsilon})}{n}}+\frac{2}{n}\log_2(1/\epsilon_{\mathrm{PA}}), \tag{26}$$

$$K^{fin}=\frac{n}{N}(K^{asy}(T',\varepsilon')-\Delta(n)), \tag{27}$$

where $z_{\epsilon_{\mathrm{PE}}/2}$ follows the equation $(1-\mathrm{erf}(z_{\epsilon_{\mathrm{PE}}/2}/\sqrt{2}))/2=\epsilon_{\mathrm{PE}}/2$, $\mathrm{erf}(x)=\frac{2}{\sqrt{\pi}}\int_0^x \mathrm{e}^{-t^2}\mathrm{d}t$, ϵ_{PE} and ϵ_{PA} represent the failure probability of the parameter estimation and the privacy amplification process, $\bar{\epsilon}$ is a smoothing parameter, n represents the block length for the final key distillation, and N represents the whole block size.

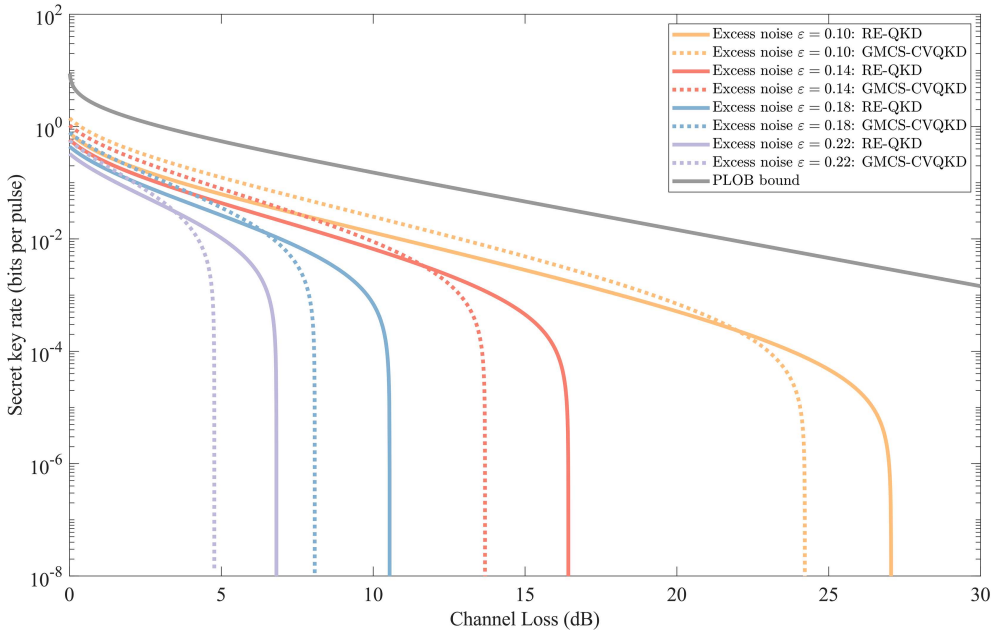

Figure 4 (Color online) Secret key rates for the RE-QKD protocol as a function of the channel loss under different excess noises in the asymptotic limit of infinitely long keys. The modulation variance is set as $V_A^{\alpha} = V_A^{\beta} = 30$ for RE-QKD. The modulation variance for the conventional GMCS-CVQKD is also set as 30. The gray solid curve shows the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound [47].

4 The simulation performance

In this section, we perform the numerical simulation for the secret key rate of the RE-QKD protocol. Since we are mainly concerned with the physical characteristics of the proposed protocol, we set the reconciliation efficiency as 1 for the RE-QKD protocol and the conventional GMCS-CVQKD protocol in the simulation. Moreover, the units for the excess noise and the modulation variance in this paper are fixed as the SNU. Figures 4 and 5 show secret key rates for the RE-QKD protocol against the channel loss under different excess noises in the asymptotic limit of infinitely long keys and when considering the finite-size effect, respectively. It indicates that the RE-QKD protocol can tolerate larger channel loss and higher excess noise than the conventional GMCS-CVQKD, both in the asymptotic limit and when considering the finite-size effect. This is because the raw key-related information is not directly transmitted through the quantum channel, which is assumed to be completely controlled by Eve. Thus, it is easier for the legal users in the RE-QKD protocol to build an information advantage against Eve. Therefore, RE-QKD has advantages over the conventional GMCS-CVQKD in adapting to complex and harsh real channel environments.

Figure 6 shows secret key rates for the RE-QKD protocol as a function of the modulation variance at the Alice site V_A^{α} and the modulation variance at the Bob site V_A^{β} when considering the finite-size effect. It can be seen that whether for the modulation variance at the Alice site or at the Bob site, the key rate of RE-QKD increases with the modulation variance. Therefore, the performance advantage of RE-QKD is more obvious at larger modulation variance. As depicted in Figure 7, the tolerable excess noise for the RE-QKD protocol can achieve a high level under different channel losses. The tolerable excess noise for the proposed protocol can still be larger than 0.04 SNU when the channel loss is up to 80 dB and the modulation variance is larger than 30 SNU in the asymptotic limit. At the relatively small channel loss, e.g., 10 dB, the tolerable excess noise for RE-QKD can be as high as 0.18 SNU. The tolerable excess noise of RE-QKD increases with the modulation variance. After the modulation variance is greater than 30 SNU, the increase in the tolerable excess noise becomes extremely slow.

As depicted in Figure 8, the figure shows the tolerable channel loss for the RE-QKD protocol against the modulation variance in the asymptotic limit of infinitely long keys. The tolerable channel loss for RE-QKD becomes larger as the modulation variance increases. It also indicates that the tolerable channel loss for RE-QKD is higher than that of the conventional GMCS-CVQKD at any modulation variance, which further proves the advantages of the RE-QKD protocol over the conventional GMCS-CVQKD in terms of the transmission distance.

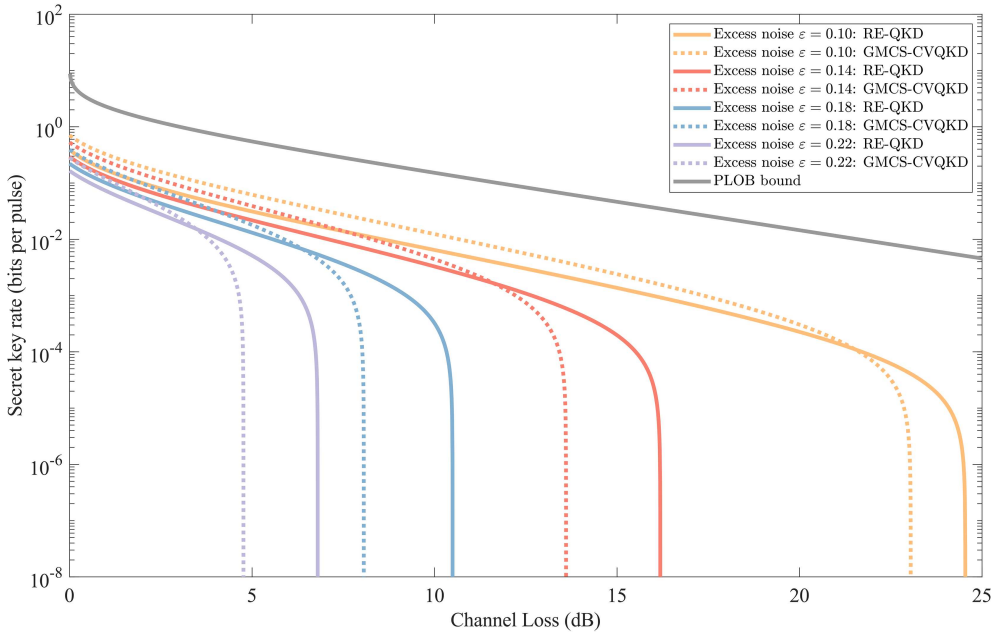

Figure 5 (Color online) Secret key rates for the RE-QKD protocol as a function of the channel loss under different excess noise when considering the finite-size effect. The modulation variance is set to the optimal value of 0–30 for RE-QKD and the conventional GMCS-CVQKD. n and N are set as 10^{12} and 2×10^{12}, respectively. We set $\epsilon_{\mathrm{PA}} = \epsilon_{\mathrm{PE}} = \bar{\epsilon} = 10^{-10}$ for typical values [48]. The gray solid curve shows the PLOB bound [47].

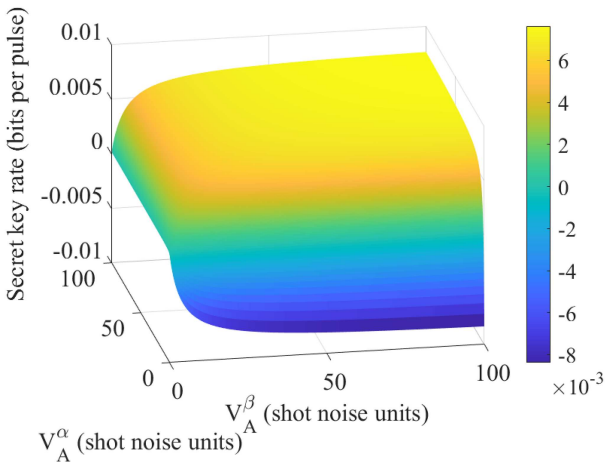

Figure 6 (Color online) Secret key rates for the RE-QKD protocol as a function of the modulation variance at the Alice site V_A^{α} and the modulation variance at the Bob site V_A^{β} when considering the finite-size effect. The channel loss and the excess noise are set as 10 dB and 0.01 shot noise units, respectively. n and N are set as 10^{12} and 2×10^{12}, respectively. We set $\epsilon_{\mathrm{PA}} = \epsilon_{\mathrm{PE}} = \bar{\epsilon} = 10^{-10}$ for typical values [48].

5 Conclusion

In this paper, we propose a reverse-encoded quantum key distribution with Gaussian-modulated coherent states and develop its prepare-and-measure scheme and entanglement-based scheme. The secret key rate for the proposed protocol is evaluated under general collective attacks. The simulation results indicate that the RE-QKD protocol is able to tolerate higher channel loss and larger excess noise than the conventional GMCS-CVQKD protocol, making it highly promising for application in the practical quantum encryption and quantum networks. The proposed RE-QKD protocol can increase the transmission distance while improving the reconciliation efficiency and reducing the frame error rate, thereby increasing the key rate of QKD. This helps improve the performance of QKD and has potential applications in typical quantum network applications such as quantum signatures [49], quantum e-commerce [50]. In addition, it reduces the difficulty of reconciliation, which helps reduce post-processing

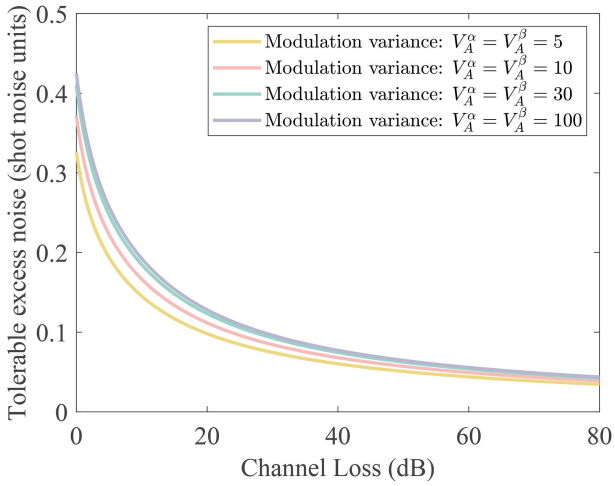

Figure 7 (Color online) Tolerable excess noise for the RE-QKD protocol as a function of the channel loss under different modulation variances in the asymptotic limit of infinitely long keys.

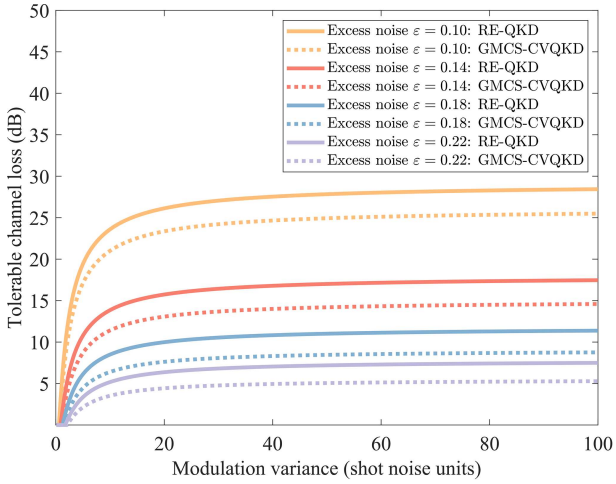

Figure 8 (Color online) Tolerable channel loss for the RE-QKD protocol as a function of the modulation variance under different excess noises in the asymptotic limit of infinitely long keys. The modulation variance at the Alice site and the Bob site is set to be the same for RE-QKD.

costs and facilitates its widespread deployment in quantum networks. Future work will include the experimental demonstration of the RE-QKD protocol.

Acknowledgements This work was supported by Quantum Science and Technology-National Science and Technology Major Project (Grant No. 2021ZD0300703), Shanghai Municipal Science and Technology Major Project (Grant No. 2019SHZDZX01), Key R&D Program of Guangdong Province (Grant No. 2020B0303040002), and National Natural Science Foundation of China (Grant No. 62101320).

References

1 Grosshans F, Grangier P. Continuous variable quantum cryptography using coherent states. Phys Rev Lett, 2002, 88: 057902
2 Grosshans F, Van Assche G, Wenger J, et al. Quantum key distribution using Gaussian-modulated coherent states. Nature, 2003, 421: 238–241
3 Weedbrook C, Lance A M, Bowen W P, et al. Quantum cryptography without switching. Phys Rev Lett, 2004, 93: 170504
4 Lance A M, Symul T, Sharma V, et al. No-switching quantum key distribution using broadband modulated coherent light. Phys Rev Lett, 2005, 95: 180503
5 Weedbrook C, Pirandola S, García-Patrón R, et al. Gaussian quantum information. Rev Modern Phys, 2021, 84: 621–669
6 Wang P, Tian Y, Li Y M. Advances in continuous variable measurement-device-independent quantum key distribution. Sci China Inf Sci, 2025, 68: 180501
7 Leverrier A, Grangier P. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. Phys Rev Lett, 2009, 102: 180504
8 Zhao Y B, Heid M, Rigas J, et al. Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks. Phys Rev A, 2009, 79: 012307
9 Sych D, Leuchs G. Coherent state quantum key distribution with multi letter phase-shift keying. New J Phys, 2016, 12: 053019
10 Papanastasiou P, Lupo C, Weedbrook C, et al. Quantum key distribution with phase-encoded coherent states: asymptotic security analysis in thermal-loss channels. Phys Rev A, 2018, 98: 012340
11 Liao Q, Xiao G, Xu C G, et al. Discretely modulated continuous-variable quantum key distribution with an untrusted entanglement source. Phys Rev A, 2020, 102: 032604
12 Lütkenhaus N. Security against eavesdropping in quantum cryptography. Phys Rev A, 1996, 54: 97–111
13 Slutsky B A, Rao R, Sun P C, et al. Security of quantum cryptography against individual attacks. Phys Rev A, 1998, 57: 2383–2398
14 Bechmann-Pasquinucci H. Eavesdropping without quantum memory. Phys Rev A, 2006, 73: 044305
15 Grosshans F, Cerf N, Wenger J, et al. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. Quantum Inform Comput, 2003, 3: 535–552
16 Biham E, Mor T. Security of quantum cryptography against collective attacks. Phys Rev Lett, 1997, 78: 2256–2259
17 García-Patrón R, Cerf N J. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. Phys Rev Lett, 2006, 97: 190503
18 Navascués M, Grosshans F, Acén A. Optimality of Gaussian attacks in continuous-variable quantum cryptography. Phys Rev Lett, 2006, 97: 190502
19 Ghorai S, Grangier P, Diamanti E, et al. Asymptotic security of continuous-variable quantum key distribution with a discrete modulation. Phys Rev X, 2019, 9: 021059
20 Lin J, Upadhyaya T, Lütkenhaus N. Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution. Phys Rev X, 2019, 9: 041064
21 Denys A, Brown P, Leverrier A. Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. Quantum, 2021, 5: 540
22 Kaur E, Guha S, Wilde M M. Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution. Phys Rev A, 2021, 103: 012412
23 Kraus B, Gisin N, Renner R. Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. Phys Rev Lett, 2005, 95: 080501
24 Renner R, Gisin N, Kraus B. Information-theoretic security proof for quantum-key-distribution protocols. Phys Rev A, 2005, 72: 012332
25 Renner R, Cirac J I. de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. Phys Rev Lett, 2009, 102: 110504

26 Coles P J, Metodiev E M, Lütkenhaus N. Numerical approach for unstructured quantum key distribution. Nat Commun, 2016, 7: 11712
27 Scarani V, Renner R. Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way postprocessing. Phys Rev Lett, 2008, 100: 200501
28 Leverrier A, García-Patrón R, Renner R, et al. Security of continuous-variable quantum key distribution against general attacks. Phys Rev Lett, 2013, 110: 030502
29 Leverrier A. Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction. Phys Rev Lett, 2017, 118: 200501
30 Matsuura T, Maeda K, Sasaki T, et al. Finite-size security of continuous-variable quantum key distribution with digital signal processing. Nat Commun, 2021, 12: 252
31 Jouguet P, Kunz-Jacques S, Leverrier A, et al. Experimental demonstration of long-distance continuous-variable quantum key distribution. Nat Photonic, 2013, 7: 378–381
32 Huang D, Huang P, Lin D, et al. Long-distance continuous-variable quantum key distribution by controlling excess noise. Sci Rep, 2016, 6: 19201
33 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
34 Wang T, Huang P, Li L, et al. High key rate continuous-variable quantum key distribution using telecom optical components. New J Phys, 2024, 26: 023002
35 Ji F, Huang P, Wang T, et al. Gbps key rate passive-state-preparation continuous-variable quantum key distribution within an access-network area. Photon Res, 2024, 12: 1485–1493
36 Liao Q, Fei Z, Liu J, et al. High-rate discretely-modulated continuous-variable quantum key distribution using quantum machine learning. Chaos Solitons Fract, 2025, 196: 116331
37 Zhang K, Hou J, Jiang X Q, et al. Effective rate-adaptive reconciliation for CV-QKD using QC-MET-LDPC codes. Sci China Inf Sci, 2025, 68: 180510
38 Jouguet P, Kunz-Jacques S, Debuisschert T, et al. Field test of classical symmetric encryption with continuous variables quantum key distribution. Opt Express, 2012, 20: 14030–14041
39 Huang D, Huang P, Li H, et al. Field demonstration of a continuous-variable quantum key distribution network. Optim Lett, 2016, 41: 3511–3514
40 Karinou F, Brunner H H, Fung C H F, et al. Toward the integration of CV quantum key distribution in deployed optical networks. IEEE Photon Technol Lett, 2018, 30: 650–653
41 Zhang Y, Li Z, Chen Z, et al. Continuous-variable QKD over 50 km commercial fiber. Quantum Sci Technol, 2019, 4: 035006
42 Kumar R, Qin H, Alléaume R. Coexistence of continuous variable QKD with intense DWDM classical channels. New J Phys, 2015, 17: 043027
43 Xu Y, Wang T, Zhao H, et al. Round-trip multi-band quantum access network. Photon Res, 2023, 11: 1449–1464
44 Wang T, Huang P, Zhou Y, et al. Pilot-multiplexed continuous-variable quantum key distribution with a real local oscillator. Phys Rev A, 2018, 97: 012310
45 Wang T, Huang P, Zhou Y, et al. High key rate continuous-variable quantum key distribution with a real local oscillator. Opt Express, 2018, 26: 2794–2806
46 Pirandola S, Braunstein S L, Lloyd S. Characterization of collective Gaussian attacks and security of coherent-state quantum cryptography. Phys Rev Lett, 2008, 101: 200504
47 Pirandola S, Laurenza R, Ottaviani C, et al. Fundamental limits of repeaterless quantum communications. Nat Commun, 2017, 8: 15043
48 Leverrier A, Grosshans F, Grangier P. Finite-size analysis of a continuous-variable quantum key distribution. Phys Rev A, 2010, 81: 062343
49 Zeng G, Keitel C H. Arbitrated quantum-signature scheme. Phys Rev A, 2002, 65: 042312
50 Liu S, Zhang Y, Ren S, et al. Experimental demonstration of complete quantum e-commerce based on an efficient quantum digital payment. Photon Res, 2025, 13: 572–582