Research
A SCIENCE PARTNER JOURNAL

RESEARCH ARTICLE

Discrete-Modulated Coherent-State Quantum Key Distribution with Basis-Encoding

Mingxuan Guo[1], Peng Huang[1,2,3*], Le Huang[1], Xiaojuan Liao[1], Xueqin Jiang[4,2,3], Tao Wang[1,2,3], and Guihua Zeng[1,2,3,5*]

[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]College of Information Science and Technology, Donghua University, Shanghai 201620, China.[5]Shanghai XunTai Quantech Co., Ltd, Shanghai, 200241, China.

*Address correspondence to: huang.peng@sjtu.edu.cn (P.H.); ghzeng@sjtu.edu.cn (G.Z.)

Citation: Guo M, Huang P, Huang L, Liao X, Jiang X, Wang T, Zeng G. Discrete-Modulated Coherent-State Quantum Key Distribution with Basis-Encoding. *Research* 2025;8:Article 0691. https://doi.org/10.34133/research.0691

Submitted 4 February 2025
Revised 27 March 2025
Accepted 9 April 2025
Published 14 May 2025

Discrete-modulated coherent-state continuous-variable quantum key distribution (DMCS-CVQKD) is of great value for its simple implementation. However, the traditional DMCS-CVQKD scheme cannot tolerate the high channel excess noise and channel loss, compared to the Gaussian-modulated scheme, and its error correction is still difficult. In this paper, we propose a discrete-modulated coherent-state basis-encoding quantum key distribution (DMCS-BE-QKD) protocol, where the secret keys are encoded in the random choice of 2 measurement bases, i.e., the conjugate quadratures X and P of discrete-modulated coherent states, and it only needs simple binary sequence error correction. We analyze the secret key rate of DMCS-BE-QKD protocol under individual and collective attacks in the linear Gaussian channel. The results show that DMCS-BE-QKD can greatly enhance the ability to tolerate the channel loss and excess noise compared to the original DMCS-CVQKD protocol, which can tolerate approximately 40 dB more channel loss compared to the original DMCS-CVQKD for the realistic value of noise. Finally, a proof-of-principle experiment is conducted under a 50.5-km optical fiber to verify the feasibility of DMCS-BE-QKD. It is based on the consistent physical procedures of the traditional DMCS-CVQKD, which makes it perfectly compatible to deployed terminals and can serve as a multiplier for the practical secure quantum cryptography communication in harsh environments.

Introduction

Continuous-variable quantum key distribution (CVQKD) can enable remote trusted parties to share secure secret keys through the untrusted quantum channel with the coherent source and detection, which can be categorized into 2 families, i.e., the Gaussian-modulated coherent-state (GMCS)-CVQKD [1–5] and discrete-modulated coherent-state (DMCS)-CVQKD [6–8] protocols. For the former one, coherent states are modulated according to a Gaussian distribution with an infinite-size constellation. For the latter one, coherent states are modulated according to a discrete probability distribution with a finite-size constellation. The key information is commonly encoded in random amplitudes and phases of coherent states. So far, the security of certain GMCS-CVQKD and DMCS-CVQKD protocols have been proved against individual [9–12], collective [13–19], and coherent attacks [20–23] even when taking into account the finite-size effect [24–29]. Moreover, certain protocols have been experimentally realized in both laboratory [30–35] and field tests [36–39], which show its superior applicability in metropolitan area quantum networks.

As known, the implementations of the above CVQKD protocols, especially the DMCS ones, are well compatible with classical coherent optical communication infrastructures [40]. Moreover, compared to GMCS-CVQKD, DMCS-CVQKD has lower requirements for modulation devices. However, as a cost, DMCS-CVQKD has a low tolerance for the channel loss and the excess noise. Moreover, as far as error correction is concerned, the error correction of conventional DMCS-CVQKD is still similar to that of GMCS-CVQKD, which is difficult and complex to implement, because the values of DMCS-CVQKD's measurement results are continuous. In addition, the DMCS-CVQKD transmits lower power, which corresponds to lower signal-to-noise ratio. Therefore, error correction of conventional DMCS-CVQKD remains difficult.

Huang et al. [41] report a novel protocol with basis-encoding (BE) of Gaussian-modulated coherent states, where the key information is encoded in the random choice of 2 measurement bases, i.e., the choice of conjugate quadratures X and P. This encoding method is different from the encoding method for conventional CVQKD protocols, which encodes the key in the value of conjugate quadratures X and P of the quantum state. The BE method exhibits the higher tolerable excess noise against the typical non-Gaussian individual attack as explored in [41]. Moreover, the raw keys of both Alice and Bob in the BE scheme are binary sequences, and the error correction for them is easier to perform compared to traditional CVQKD protocols. However, this work only analyzes the secret key rate of BE-QKD under a

typical non-Gaussian individual attack. It has marked limitations since the Gaussian channel (i.e., Gaussian attack) is the more general case in reality. Meanwhile, it does not analyze the secret key rate of BE-QKD under collective attacks. No experiment is conducted to verify the feasibility of BE-QKD. Since the publication of [41], the security analysis [16–19,27–29] and experiments [34,35,42–44] of the conventional CVQKD have made significant progress. However, the development of BE-QKD has been rather limited.

Inspired by this, a discrete-modulated coherent-state basis-encoding quantum key distribution (DMCS-BE-QKD) protocol is proposed to improve the tolerance of DMCS-CVQKD for the channel loss and excess noise, and the security analysis of it is further improved compared to the former work [41], where a novel security analysis framework is developed because the analysis framework in [41] is not suitable for analyzing the secret key rate under Gaussian individual or collective attacks. We first focus on 2 typical DMCS-BE-QKD protocols: binary-phase-shift-keying (BPSK) BE-QKD and quadrature-phase-shift-keying (QPSK) BE-QKD protocols. We develop the methods to evaluate the secret key rate of B/QPSK-BE-QKD in the linear Gaussian channel under individual attacks and collective attacks. Moreover, similar analysis can be extended to the arbitrary modulation case. The simulation result shows that B/QPSK-BE-QKD can significantly improve the transmission distance compared to the original B/QPSK-CVQKD scheme and QPSK-BE-QKD performs better than BPSK-BE-QKD. Translating the whole constellation diagram along the $y = x$ axis does not affect the key rate due to the fact that the probability density curves of measurement results corresponding to perform X and P measurements are always the same in this case. Moreover, we realize the proof-of-principle experiment of QPSK-BE-QKD under a 50.5-km optical fiber with the 11-dB channel loss.

Results

DMCS-BE-QKD protocol

The DMCS-BE-QKD protocol executes the following steps.

Quantum communication part:

1. Alice randomly prepares coherent states $|\alpha_k\rangle = |\Re(\alpha_k) + i\Im(\alpha_k)\rangle$ from the set $\{|\alpha_k\rangle\}_{k=0,\ldots,M-1}$, where $\alpha_k \in \mathbb{C}$ and M represents the modulation order. Then, Alice sends them to Bob;
2. Bob randomly chooses a random binary sequence b to decide the measurement basis, i.e., quadrature X (corresponding to $b = 0$) or P (corresponding to $b = 1$), to measure and obtain measurement results X_B or P_B (shot noise unit);
3. Alice and Bob randomly choose a fraction of measurement results to perform the parameter estimation, including the modulation variance, excess noise, and the transmission efficiency.

Key decoding and distillation part:

4. Bob publishes his measurement outcomes β_y of his homodyne detection, i.e., the values X_B or P_B and Alice decoding the secret key b by judging the Bob's measurement basis according to the decoding rules related with her generated coherent states. After these operations, Alice and Bob share a set of correlated binary raw keys.
5. Alice and Bob perform the reconciliation with binary codes and the privacy amplification to distill final secret keys. Intuitively, Bob can also apply the heterodyne detection and publishes randomly one of the 2 basis outcomes according to $b = 0$ or 1.

As depicted in Fig. 1, the decoding rules in step (4) are summarized as follows:

when $\Re(\alpha_k) > \Im(\alpha_k)$ and $\beta_y > \beta_A C_A$, decode key as 0
when $\Re(\alpha_k) > \Im(\alpha_k)$ and $\beta_y < \beta_A C_A$, decode key as 1
when $\Re(\alpha_k) < \Im(\alpha_k)$ and $\beta_y > \beta_A C_A$, decode key as 1
when $\Re(\alpha_k) < \Im(\alpha_k)$ and $\beta_y < \beta_A C_A$, decode key as 0

where $C_A = \frac{1}{2}(2\Re(\alpha_k) + 2\Im(\alpha_k))$, and β_A is the coefficients to give minimum variances of $\Delta X = X_B - \beta_A X_A$ and $\Delta P = P_B - \beta_A P_A$. When Bob uses the homodyne detector, $\beta_A = \sqrt{T\eta}$, where T is the channel trasmission efficiency and η is the efficiency of the detection. When Bob uses the heterodyne detector, $\beta_A = \sqrt{T\eta/2}$. The basic principle of decoding is finding the smaller distance from the Bob's measurement result to the original values of conjugate quadratures. We further discuss several possible situations when Alice conducts the correct and incorrect decoding.

Correct decoding:

when $\Re(\alpha_k) > \Im(\alpha_k)$, $X_B > \beta_A C_A$ or $P_B < \beta_A C_A$
when $\Re(\alpha_k) < \Im(\alpha_k)$, $X_B < \beta_A C_A$ or $P_B > \beta_A C_A$

Incorrect decoding:

when $\Re(\alpha_k) > \Im(\alpha_k)$, $X_B < \beta_A C_A$ or $P_B > \beta_A C_A$
when $\Re(\alpha_k) < \Im(\alpha_k)$, $X_B > \beta_A C_A$ or $P_B < \beta_A C_A$

It should be mentioned that the quantum communication part works the same as the traditional DMCS-CVQKD protocol, while the key decoding and distillation parts run differently.

The security against individual and collective attacks with B/QPSK modulation

We divide the overall channel into subchannels, based on Bob's measurement result β_y. Each subchannel is defined by a specific measurement result β_y. Then, we can analyze the security of each subchannel to obtain its secret key rate. The secret key rates of subchannels are weighted according to the probability of the subchannel occurrence and summed to obtain the final secret key rate. We can use the probability theory to calculate

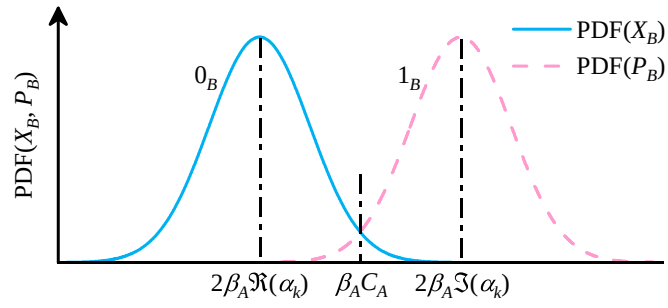

Fig. 1. The decoding rules for Alice. Alice decodes the key based on how "close" is the measurement result β_y to $2\beta_A\Re(\alpha_k)$ and $2\beta_A\Im(\alpha_k)$. When β_y is closer to $2\beta_A\Re(\alpha_k)$, Alice decodes the key as 0. Otherwise, Alice decodes the key as 1.

the classical mutual information between Alice and Bob in the subchannel. For Eve, in the subchannel $\beta_y = m$, the quantum state she obtains when Bob encodes 0 is $\rho_E^{x=m}$, and the quantum state she obtains when Bob encodes 1 is $\rho_E^{p=m}$. Using the density matrix $\rho_E^{x=m}$ and $\rho_E^{p=m}$, we can determine the maximum information Eve can obtain in each subchannel. Then, we can easily calcualte the secret key rate of each subchannel and further obtain the overall key rate.

For each subchannel $\beta_y = m$ (including $X_B = m$ and $P_B = m$), the secret key rate of BE-QKD under individual attacks is given by

$$K_{ind}^{\beta_y=m} = \beta I\left(A;B|\beta_y=m\right) - \max_{\Pi} I\left(b;E,\Pi|\beta_y=m\right) \quad (1)$$

where Π represents any group of Eve's positive-operator valued measurements, $\Pi = \{\Pi_1, \Pi_2, \ldots\}$. For the subchannel, the secret key rate of BE-QKD under collective attacks is given by [45],

$$K_{col}^{\beta_y=m} = \beta I\left(A;B|\beta_y=m\right) - \chi_{bE}^{\beta_y=m} \quad (2)$$

$$\chi_{bE}^{\beta_y=m} = S\left(\rho_E^{\beta_y=m}\right) - p\left(0_B|\beta_y=m\right)S\left(\rho_E^{x=m}\right) - p\left(1_B|\beta_y=m\right)S\left(\rho_E^{p=m}\right) \quad (3)$$

where χ_{bE} represents the Holevo bound, the density matrix of the state at E in the subchannel $\beta_y = m$ is $\rho_E^{\beta_y=m} = p\left(0_B|\beta_y=m\right)\rho_E^{x=m} + p\left(1_B|\beta_y=m\right)\rho_E^{p=m}$, "$0_B$" represents Bob encodes her key as 0, and "1_B" represents Bob encodes her key as 1.

So, the overall key rate of BE-QKD under individual and collective attacks is given by,

$$K_{ind} = \int p\left(\beta_y=m\right)K_{ind}^{\beta_y=m}dm \quad (4)$$

$$K_{col} = \int p\left(\beta_y=m\right)K_{col}^{\beta_y=m}dm \quad (5)$$

We will now discuss the secret key rate of B/QPSK-BE-QKD in the linear Gaussian channel. In the linear Gaussian channel, the channel loss is the coefficient T (i.e., the channel loss can be fully characterized by the coefficient T), and the noise is the additive Gaussian noise that is independent of the input data. The linear Gaussian channel is the most common and important channel in reality, where the attack from Eve is entangling cloner attack [12]. So, we need to discuss the security against individual and collective entangling cloner attacks. The entangling cloner attack is depicted in Fig. 2. Eve first prepares a 2-mode squeezed state (TMSV) with variance $V_E = 1 + \frac{T\varepsilon}{1-T}$, where ε represents the channel excess noise. Then, Eve reserves one mode of TMSV E_2 and coupling another mode E_0 with Alice's outgoing signal B_0 in a beam splitter with transmissivity T. One of the outgoing modes of the beam splitter B_1 is sent to Bob through a lossless channel, and another mode E_1 is reserved by Eve. Finally, Eve performs optimal measurements on the mode E_1E_2.

Mutual information between Alice and Bob

We first discuss the mutual information between Alice and Bob for BPSK-BE-QKD. Here, we discuss the simplest situation, i.e.,

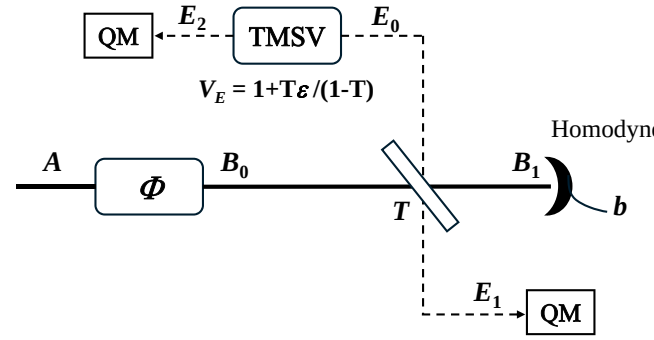

Fig. 2. The operation principle of entangling cloner attacks when Bob uses the homodyne detection while ignoring the detection efficiency and electrical noise.

the modulation constellation ($\alpha_0 = -a + ai, \alpha_1 = a - ai$) shown as Fig. 3A is used, Bob uses the homodyne detection, and the detection efficiency and the electrical noise are ignored. The more complex situations and calculation detail are discussed in Supplementary Note I. First, we can write down the conditional probabilities of Bob's measurement results,

$$\begin{aligned} p\left(\beta_y=m|\alpha_0,0_B\right) &= N_{pdf}\left(m,-2\sqrt{T}a,1+T\varepsilon\right)=p_1,\\ p\left(\beta_y=m|\alpha_1,0_B\right) &= N_{pdf}\left(m,2\sqrt{T}a,1+T\varepsilon\right)=p_2,\\ p\left(\beta_y=m|\alpha_0,1_B\right) &= N_{pdf}\left(m,2\sqrt{T}a,1+T\varepsilon\right)=p_2,\\ p\left(\beta_y=m|\alpha_1,1_B\right) &= N_{pdf}\left(m,-2\sqrt{T}a,1+T\varepsilon\right)=p_1, \end{aligned} \quad (6)$$

where $N_{pdf}(\bullet,\mu,\sigma^2)$ represents the probability density function of the normal distribution with the mean value μ and the standard variance σ. We can also calculate the conditional error rate $p\left(1_A|0_B,\beta_y=m\right)$ when Bob encodes the key "0" and $p\left(0_A|1_B,\beta_y=m\right)$ when Bob encodes the key "1",

$$\begin{aligned} &p\left(1_A|0_B,\beta_y=m\right) =\\ &p\left(0_A|1_B,\beta_y=m\right)=p_{error}^{BPSK}=1/\left(1+\exp\left|\frac{4\sqrt{T}am}{1+T\varepsilon}\right|\right) \end{aligned} \quad (7)$$

Above all, the mutual information between Alice and Bob for BPSK-BE-QKD is given by,

$$\begin{aligned} &I\left(A;B|\beta_y=m\right) =\\ &H\left(A|\beta_y=m\right)-H\left(A|B,\beta_y=m\right)=1-H\left(p_{error}^{BPSK}\right). \end{aligned} \quad (8)$$

Then, we discuss the mutual information between Alice and Bob for QPSK-BE-QKD. We discuss the situation that the modulation constellation ($\alpha_0 = -a + \Delta a + (a+\Delta a)i$, $\Delta b + \alpha_1 = -a + (a+\Delta b)i, \alpha_2 = a + \Delta b + (-a+\Delta b)i, \alpha_3 = a + \Delta a + (-a+\Delta a)i$, $\Delta a > \Delta b$) shown as Fig. 3B is used, Bob uses the homodyne detection, and the detection efficiency and the electrical noise are ignored. The more complex situations and calculation detail are discussed in Supplementary Note I. We can write down the conditional probabilities of Bob's measurement results,

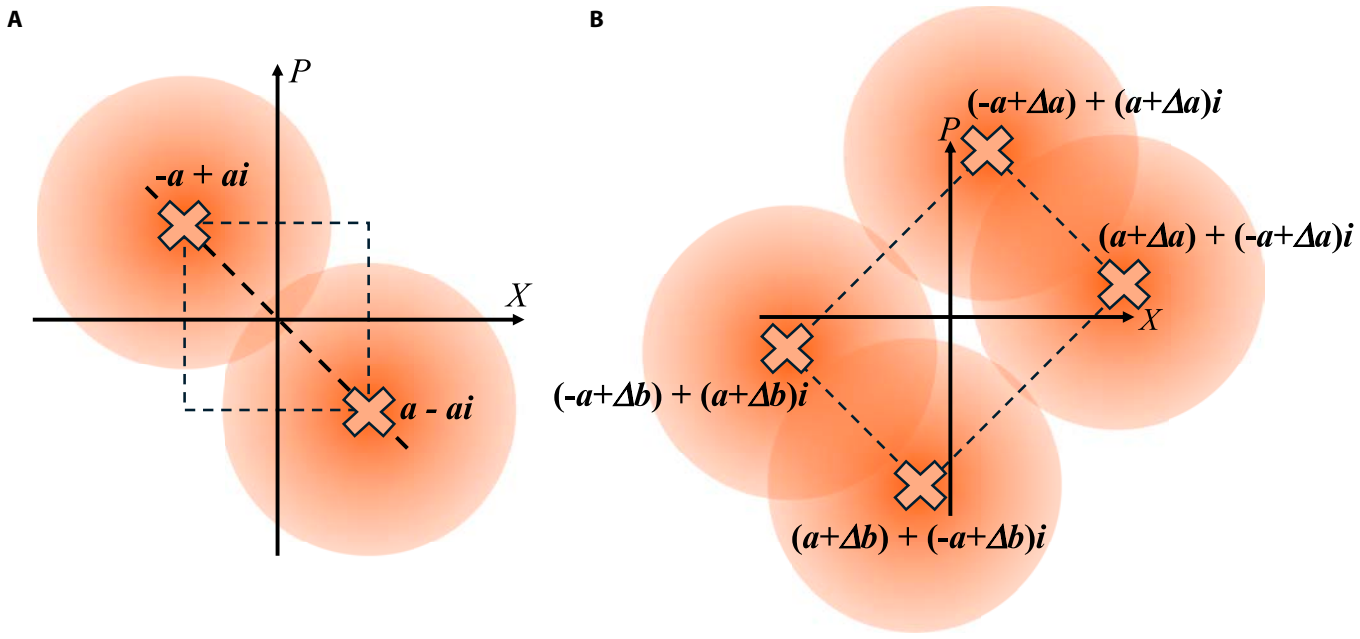

Fig. 3. The modulation constellation for (A) BPSK-BE-QKD and (B) QPSK-BE-QKD.

$$
\begin{aligned}
p\left(\beta_y=m|\alpha_0,0_B\right)&=N_{pdf}\left(m,2\sqrt{T}(-\alpha+\Delta\alpha),1+T\varepsilon\right)=p_1\\
p\left(\beta_y=m|\alpha_1,0_B\right)&=N_{pdf}\left(m,2\sqrt{T}(-\alpha+\Delta b),1+T\varepsilon\right)=p_2\\
p\left(\beta_y=m|\alpha_2,0_B\right)&=N_{pdf}\left(m,2\sqrt{T}(\alpha+\Delta b),1+T\varepsilon\right)=p_3\\
p\left(\beta_y=m|\alpha_3,0_B\right)&=N_{pdf}\left(m,2\sqrt{T}(\alpha+\Delta\alpha),1+T\varepsilon\right)=p_4\\
p\left(\beta_y=m|\alpha_0,1_B\right)&=N_{pdf}\left(m,2\sqrt{T}(\alpha+\Delta\alpha),1+T\varepsilon\right)=p_4\\
p\left(\beta_y=m|\alpha_1,1_B\right)&=N_{pdf}\left(m,2\sqrt{T}(\alpha+\Delta b),1+T\varepsilon\right)=p_3\\
p\left(\beta_y=m|\alpha_2,1_B\right)&=N_{pdf}\left(m,2\sqrt{T}(-\alpha+\Delta b),1+T\varepsilon\right)=p_2\\
p\left(\beta_y=m|\alpha_3,1_B\right)&=N_{pdf}\left(m,2\sqrt{T}(-\alpha+\Delta\alpha),1+T\varepsilon\right)=p_1.
\end{aligned}
\tag{9}
$$

Similarly, we can also give out the conditional error rate $p\left(1_A|0_B,\beta_y=m\right)$ and $p\left(0_A|1_B,\beta_y=m\right)$ for QPSK-BE-QKD,

$$
p\left(1_A|0_B,\beta_y=m\right)=p\left(0_A|1_B,\beta_y=m\right)=p_{error}^{QPSK}=
\begin{cases}
\dfrac{p_1+p_2}{p_1+p_2+p_3+p_4}, m>2\sqrt{T}\Delta a\\
\dfrac{p_2+p_4}{p_1+p_2+p_3+p_4}, 2\sqrt{T}\Delta b<m<2\sqrt{T}\Delta a\\
\dfrac{p_3+p_4}{p_1+p_2+p_3+p_4}, m<2\sqrt{T}\Delta b
\end{cases}
\tag{10}
$$

Above all, the mutual information between Alice and Bob for QPSK-BE-QKD is given by,

$$
\begin{aligned}
&I\left(A;B|\beta_y=m\right)=\\
&H\left(A|\beta_y=m\right)-H\left(A|B,\beta_y=m\right)=1-H\left(p_{error}^{QPSK}\right)
\end{aligned}
\tag{11}
$$

Leaked key information to Eve

In this part, we try to calculate the leaked key information to Eve in the linear Gaussian channel under individual attacks $\left(\max_{\Pi} I\left(b;E,\Pi|\beta_y=m\right)\right)$ and under collective attacks $\left(\chi_{bE}^{\beta_y=m}\right)$. In order to achieve this, we first need to figure out the density matrix of the conditional quantum state $\rho_E^{x=m}$ and $\rho_E^{p=m}$ when using the homodyne detection and ignoring the detection efficiency and the electrical noise.

We can first express the state at B_0 and two-mode squeezed vacuum state (TSMV) state $|E_0E_2\rangle$:

$$
\rho_{B_0}=\sum_{k=0}^{M-1}p_k|\alpha_k\rangle\langle\alpha_k| \tag{12}
$$

$$
|E_0E_2\rangle=\frac{1}{\cosh r_E}\sum_{n=0}^{\infty}\left(\tanh r_E\right)^n|n,n\rangle, \tag{13}
$$

where $r_E=\left(\cosh^{-1}V_E\right)/2$ and $M=2$ or 4 when the protocol is B/QPSK-BE-QKD protocol. The operator of the beam splitter with transmissivity T can be given by [46],

$$
R_{B_0E_0}=\exp\left(\cos^{-1}\sqrt{T}\left(\hat{a}_{B_0}\otimes\hat{a}_{E_0}^{\dagger}-\hat{a}_{B_0}^{\dagger}\otimes\hat{a}_{E_0}\right)\right) \tag{14}
$$

Then, we can calculate the density matrix of the state at $B_1E_1E_2$,

$$
\rho_{B_1E_1E_2}=\left(R_{B_0E_0}\otimes I_{E_2}\right)\left(\rho_{B_0}\otimes|E_0E_2\rangle\langle E_0E_2|\right)\left(R_{B_0E_0}^{\dagger}\otimes I_{E_2}\right) \tag{15}
$$

We define eigenvalue sets of the $\hat{x}$ and $\hat{p}$ operator [the definitions of $\hat{x}$ and $\hat{p}$ are $\hat{x}=\hat{a}+\hat{a}^{\dagger}$ and $\hat{p}=i\left(\hat{a}^{\dagger}-\hat{a}\right)$, where $\hat{a}^{\dagger}$ is the creation operator and $\hat{a}$ is the annihilation operator] as Λ_x and Λ_p, respectively. To get numerical results, we cut off the space of B_i and

E_i by the space spanned by the first N Fock states. Thus, we know that these 2 eigenvalue sets are completely the same and both of them have the size N. So, we define that $\Lambda = \Lambda_x = \Lambda_p = \{\lambda_1, \ldots, \lambda_N\}$, $\hat{x}\left|x_{\lambda_i}\right\rangle = \lambda_i\left|x_{\lambda_i}\right\rangle$, and $\hat{p}\left|p_{\lambda_i}\right\rangle = \lambda_i\left|p_{\lambda_i}\right\rangle$. For convenience, we abbreviate $\left|x_{\lambda_i}\right\rangle$ as $|x_i\rangle$ and abbreviate $\left|p_{\lambda_i}\right\rangle$ as $|p_i\rangle$. Then, we can define that,

$$M_{x=\lambda_i} = M_{x_i} = \left(|x_i\rangle\langle x_i|\right) \otimes I_{E_1E_2} \tag{16}$$

$$M_{p=\lambda_i} = M_{p_i} = \left(|p_i\rangle\langle p_i|\right) \otimes I_{E_1E_2} \tag{17}$$

Furthermore, we can calculate conditional probabilities of each measurement results and the probability of the subchannel occurrence,

$$p\left(\beta_y = \lambda_i|0_B\right) = Tr\left(M_{x_i}^{\dagger} M_{x_i} \rho_{B_1E_1E_2}\right) \tag{18}$$

$$p\left(\beta_y = \lambda_i|1_B\right) = Tr\left(M_{p_i}^{\dagger} M_{p_i} \rho_{B_1E_1E_2}\right) \tag{19}$$

$$p\left(\beta_y = \lambda_i\right) = p\left(0_B\right)p\left(\beta_y = \lambda_i|0_B\right) + p\left(1_B\right)p\left(\beta_y = \lambda_i|1_B\right) \tag{20}$$

Then, we give out the density matrix of the conditional quantum state $\rho_E^{x=\lambda_i}$ and $\rho_E^{p=\lambda_i}$,

$$\rho_E^{x=\lambda_i} = \rho_{E_1E_2}^{x=\lambda_i} = Tr_{B_1}\frac{M_{x_i}\rho_{B_1E_1E_2}M_{x_i}^{\dagger}}{p\left(\beta_y = \lambda_i|0_B\right)} \tag{21}$$

$$\rho_E^{p=\lambda_i} = \rho_{E_1E_2}^{p=\lambda_i} = Tr_{B_1}\frac{M_{p_i}\rho_{B_1E_1E_2}M_{p_i}^{\dagger}}{p\left(\beta_y = \lambda_i|1_B\right)} \tag{22}$$

The calculation methods for the density matrixes of the states $\rho_E^{x=\lambda_i}$ and $\rho_E^{p=\lambda_i}$ when using the heterodyne detection and in the cases with the imperfect detection are shown in Supplementary Note II. We can find that the calculation process involves the calculation about 3 state spaces, which will largely slow down our calculation speed. To solve this, we can derive the specific expression of $\rho_E^{x=\lambda_i}$ and $\rho_E^{p=\lambda_i}$ involving only about 2 state spaces to accelerate the speed for calculating, which is detailed in Supplementary Note III.

After we obtain the density matrixes of the states $\rho_E^{x=\lambda_i}$ and $\rho_E^{p=\lambda_i}$, we can calculate the leaked key information to Eve in the linear Gaussian channel under individual attacks and under collective attacks. Under individual attacks, we can use a non-convex optimization method [47] to calculate the $\max_{\Pi} I\left(b; E, \Pi|\beta_y = \lambda_i\right)$ since $\max_{\Pi} I\left(b; E, \Pi|\beta_y = \lambda_i\right)$ is a convex function and finding its maximum value is a non-convex optimization problem. The detail is described in Supplementary Note IV. Then, we can use Eqs. 1, 4, 6 to 8, and 12 to 22 to calculate the key rate for BPSK-BE-QKD and use Eqs. 1, 4, and 9 to 22 for QPSK-BE-QKD under individual attacks. Under collective attacks, we just need to calculate the related von Neumann entropy, which is easy to be calculated. Thus, we can use Eqs. 2, 3, 5 to 8, and 12 to 22 to calculate the key rate for BPSK-BE-QKD and use Eqs. 2, 3, 5, and 9 to 22 for QPSK-BE-QKD under collective attacks. It is worth noting that under the condition of the photon number cutoff, Eqs. 4 and 5 need to be rewritten as follows,

$$K_{ind} = \int p\left(\beta_y = m\right)K_{ind}^{\beta_y=m}dm \approx \sum_{i=1}^{N} p\left(\beta_y = \lambda_i\right)K_{ind}^{\beta_y=\lambda_i} \tag{23}$$

$$K_{col} = \int p\left(\beta_y = m\right)K_{col}^{\beta_y=m}dm \approx \sum_{i=1}^{N} p\left(\beta_y = \lambda_i\right)K_{col}^{\beta_y=\lambda_i} \tag{24}$$

The security against individual and collective attacks with an arbitrary modulation

In this section, we discuss the secret key rate of DMCS-BE-QKD in the linear Gaussian channel under individual and collective attacks with an arbitrary modulation. A modulation with M coherent state $\left\{|\alpha_k\rangle\right\}_{k=0,..,M-1}$ is prepared with probabilities $\left\{p_k\right\}_{k=0,\ldots,M-1}$. Then, we calculate the average value of real and imagine parts for coherent states and sort them from small to large to form the set $\Upsilon = \left\{\Delta_k^C\right\}_{k=0,\ldots,M_1-1}$ while removing the same elements (thus, $M_1 \leq M$), where $\Delta_k^C = \frac{1}{2}\left(\Re\left(\alpha_k\right) + \Im\left(\alpha_k\right)\right)$. We also define the set $K_{x>p}$ that includes all the indices whose corresponding coherent states' X value is larger than P value. We define the set $K_{x<p}$ that includes all the indices whose corresponding coherent states' X value is samller than P value. We define the set Ω_k^1 that includes all the indices whose corresponding coherent state's Δ^C is $\leq \Delta_k^C$, and define the set Ω_k^2 that includes all the indices whose corresponding coherent state's Δ^C is $\geq \Delta_k^C$.

First, we try to calculate the mutual information between Alice and Bob for DMCS-BE-QKD with an arbitrary modulation. We can easily write down all the conditional probabilities of Bob's meansurement results when using the homodyne detection and ignoring the detection efficiency and the electrical noise,

$$\begin{aligned} p\left(\beta_y = m|\alpha_k, 0_B\right) &= N_{pdf}\left(m, 2\sqrt{T}\Re\left(\alpha_k\right), 1 + T\varepsilon\right) \\ p\left(\beta_y = m|\alpha_k, 1_B\right) &= N_{pdf}\left(m, 2\sqrt{T}\Im\left(\alpha_k\right), 1 + T\varepsilon\right), \end{aligned} \tag{25}$$

Then, we can calculate the probabilities of the subchannel occurrence and probabilities of Bob encoding the key "0" and "1" under the subchannel,

$$p\left(\beta_y = m\right) = \sum_{k,n} p\left(\alpha_k, n_B\right)p\left(\beta_y = m|\alpha_k, n_B\right) \tag{26}$$

$$p\left(0_B|\beta_y = m\right) = \frac{\sum_k p\left(\alpha_k, 0_B\right)p\left(\beta_y = m|\alpha_k, 0_B\right)}{p\left(\beta_y = m\right)} \tag{27}$$

$$p\left(1_B|\beta_y=m\right)=\frac{\sum_k p(\alpha_k,1_B)p\left(\beta_y=m|\alpha_k,1_B\right)}{p\left(\beta_y=m\right)} \quad (28)$$

We try to calculate the conditional error rate $p\left(1_A|0_B,\beta_y=m\right)$ and $p\left(0_A|1_B,\beta_y=m\right)$. We will divide the situation into M_1+1 types, namely, $m<2\sqrt{T}\Delta_0^C$, $2\sqrt{T}\Delta_0^C<m<2\sqrt{T}\Delta_1^C$, $2\sqrt{T}\Delta_1^C<m<2\sqrt{T}\Delta_2^C$,..., $2\sqrt{T}\Delta_{M_1-2}^C<m<2\sqrt{T}\Delta_{M_1-1}^C$, $m>2\sqrt{T}\Delta_{M_1-1}^C$.

When $m<2\sqrt{T}\Delta_0^C$, we can obtain that,

$$p\left(1_A|0_B,\beta_y=m\right)=\frac{\sum_{k\in K_{x>p}} p(\alpha_k,0_B)p\left(\beta_y=m|\alpha_k,0_B\right)}{p\left(\beta_y=m\right)p\left(0_B|\beta_y=m\right)} \quad (29)$$

$$p\left(0_A|1_B,\beta_y=m\right)=\frac{\sum_{k\in K_{x<p}} p(\alpha_k,1_B)p\left(\beta_y=m|\alpha_k,1_B\right)}{p\left(\beta_y=m\right)p\left(1_B|\beta_y=m\right)} \quad (30)$$

When $2\sqrt{T}\Delta_k^C<m<2\sqrt{T}\Delta_{k+1}^C$ $(0\le k\le M_1-2)$, we can obtain that,

$$p(1_A|0_B,\beta_y=m)=\frac{\sum_{k\in\left(\Omega_{k+1}^2\cap K_{x>p}\right)\cup\left(\Omega_k^1\cap K_{x<p}\right)} p(\alpha_k,0_B)p(\beta_y=m|\alpha_k,0_B)}{p(\beta_y=m)p(0_B|\beta_y=m)} \quad (31)$$

$$p(0_A|1_B,\beta_y=m)=\frac{\sum_{k\in\left(\Omega_{k+1}^2\cap K_{x<p}\right)\cup\left(\Omega_k^1\cap K_{x>p}\right)} p(\alpha_k,1_B)p(\beta_y=m|\alpha_k,1_B)}{p(\beta_y=m)p(1_B|\beta_y=m)} \quad (32)$$

When $m>2\sqrt{T}\Delta_{M_1-1}^C$, we can obtain that,

$$p\left(1_A|0_B,\beta_y=m\right)=\frac{\sum_{k\in K_{x<p}} p(\alpha_k,0_B)p\left(\beta_y=m|\alpha_k,0_B\right)}{p\left(\beta_y=m\right)p\left(0_B|\beta_y=m\right)} \quad (33)$$

$$p\left(0_A|1_B,\beta_y=m\right)=\frac{\sum_{k\in K_{x>p}} p(\alpha_k,1_B)p\left(\beta_y=m|\alpha_k,1_B\right)}{p\left(\beta_y=m\right)p\left(1_B|\beta_y=m\right)} \quad (34)$$

and thus, we can obtain that,

$$p\left(0_A|\beta_y=m\right)=\sum_k p\left(k_B|\beta_y=m\right)p\left(0_A|k_B,\beta_y=m\right) \quad (35)$$

$$p\left(1_A|\beta_y=m\right)=\sum_k p\left(k_B|\beta_y=m\right)p\left(1_A|k_B,\beta_y=m\right) \quad (36)$$

Above all, the mutual information between Alice and Bob for DMCS-BE-QKD with an arbitrary modulation is given by,

$$I\left(A;B|\beta_y=m\right)=H\left(A|\beta_y=m\right)-H\left(A|B,\beta_y=m\right) \quad (37)$$

When keeping the modulation constellation unchanged, just changing the detecting method as heterodyne detecting or considering the detection efficiency and the electrical noise, we can just obey the rule discussed in Supplementary Note I to replace T and ϵ in Eqs. 25 to 37.

We can use the completely same process discussed above to calculate the leaked information to Eve under individual and collective attacks with an arbitrary modulation. Finally, we are able to calculate the secret key rate in this situation according to Eqs. 23 and 24.

The simulation performance

In this section, we perform the numerical simulation of secret key rates for the B/QPSK-BE-QKD protocol in the linear Gaussian channel under individual and collective attacks by the method described above. We calculate secret key rates for the original B/QPSK-CVQKD in the linear channel under collective attacks according to [6]. Since we mainly focus on the physical characteristics of the proposed protocol, the reconciliation efficiency is set to 1 for both the BE scheme and the original scheme in the following simulations. It is noted that the photon number cutoff and the finite number of subchannels have an impact on the security. We observe that the secret key rate does not depend on the specific value of the photon number cutoff parameter N and the number of subchannels provided that they are both larger than 8. Figure 4 shows the secret key rates of B/QPSK-BE-QKD via the channel loss for different channel excess noises in the linear Gaussian channel under individual attacks. Both BPSK and QPSK BE-QKD protocols show high performance in the noise tolerance and the transmission distance. Meanwhile, QPSK-BE-QKD performs better than the BPSK-BE-QKD under individual attacks.

As depicted in Fig. 5, the BPSK-BE-QKD both for homodyne and heterodyne detections can withstand the approximately 30- and 7-dB channel loss under collective attacks when the excess noises ϵ are 0.02 and 0.05, respectively. However, when the excess noise ϵ is 0.02 or 0.05, the original BPSK-CVQKD cannot code even when the channel loss is 0 dB. Meanwhile, Fig. S4 shows similar results when considering the effect of the detection efficiency and the electrical noise. Key rate curve for BPSK-BE-QKD with more excess noise selections is shown in Supplementary Note VI. It can be seen that BPSK-BE-QKD is less sensitive to the excess noise compared to the original BPSK-CVQKD.

As shown in Fig. 6, QPSK-BE-QKD can withstand the approximately 50- and 10-dB channel loss under collective attacks when the excess noise ϵ is 0.02 and 0.05, respectively. QPSK-BE-QKD can tolerate approximately 40 dB and 10 more channel loss compared to the original QPSK-CVQKD when excess noises ϵ are 0.02 and 0.05, respectively (for standard optical fibers, it is equivalent to extending the distance for about 200 and 50 km, respectively). It shows similar results when considering the imperfection of the detection according to Fig. S5. Key rate curve for QPSK-BE-QKD with more excess noise

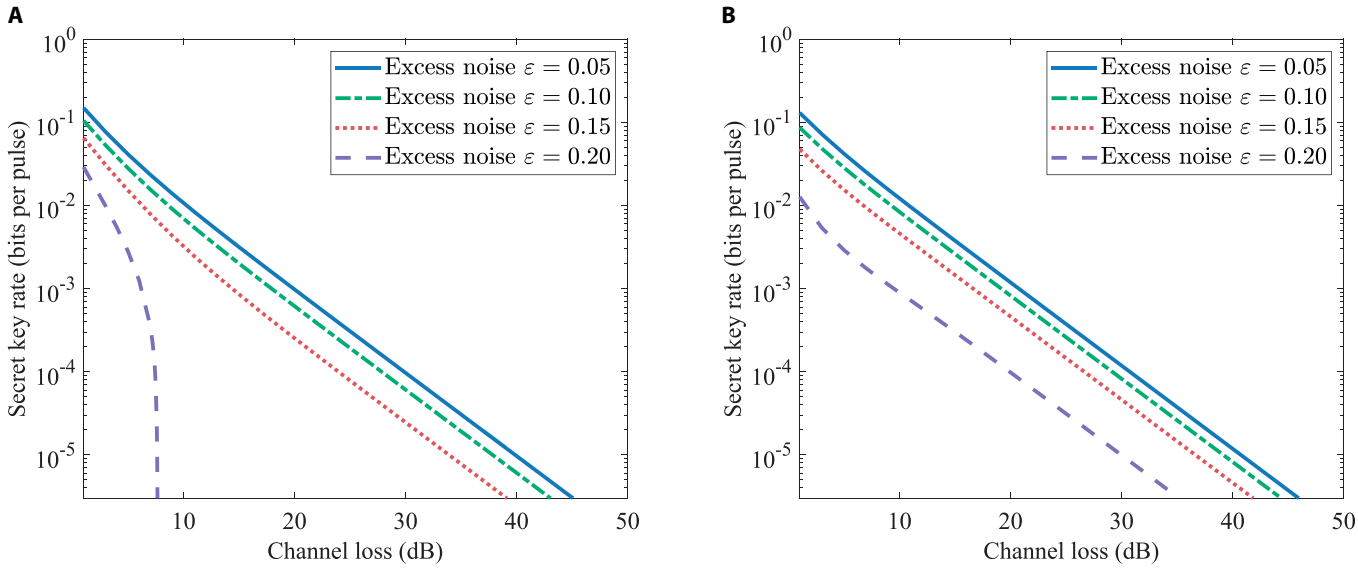

Fig. 4. Secret key rates of (A) BPSK-BE-QKD or (B) QPSK-BE-QKD via the channel loss for different channel excess noises in the linear Gaussian channel under individual attacks. The modulation variance is (A) $V_A = 0.5$ or (B) $V_A = 1$.

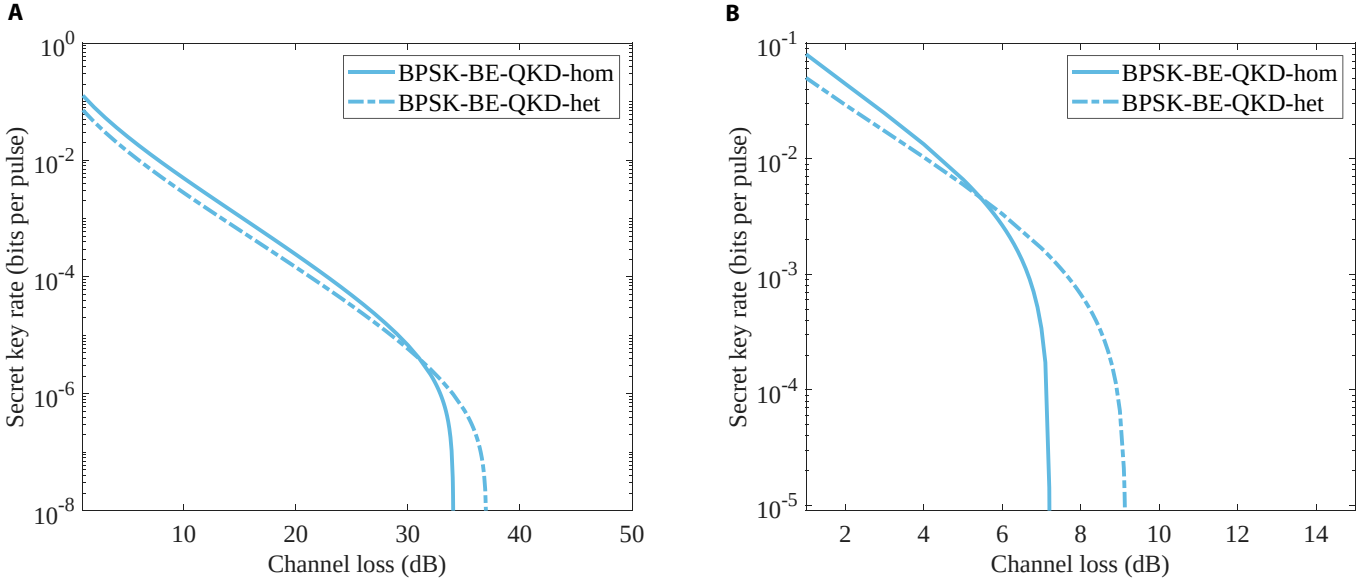

Fig. 5. Secret key rates of BPSK-BE-QKD via the channel loss for the excess noise (A) $\varepsilon = 0.02$ or (B) $\varepsilon = 0.05$ in the linear Gaussian channel under collective attacks. Here, we ignore the detection efficiency and the electrical noise. The modulation variance is $V_A = 0.5$ for BPSK-BE-QKD.

selections is shown in Supplementary Note VI. It is noted that the low bound of the key rate obtained in [6] is not tight enough, and both the BE protocol itself and the security analysis method may contribute to these observed improvements in terms of the tolerable channel loss and excess noise. The exact proportion of the contribution that the above 2 factors make is still unknown and requires further study. In addition, it is noted that Lin et al. [17] reflected the best performance of the current QPSK-CVQKD scheme under the general collective attack. According to the above results, QPSK-BE-QKD with linear Gaussian channel assumption can tolerate several dB more channel loss compared to the result in [17]. We will broadly discuss the performance potential of QPSK-BE-QKD if they are all under general collective attack conditions. Under the general collective attack, we need to traverse all possible states at AB_1 and all possible purification of ρ_{AB_1} (since the state at Eve can be any purification of ρ_{AB_1}), and then the secret key rate is calculated using the maximum corresponding leaked information. We prove that the leaked information for DMCS-BE-QKD remains unchanged for different purification of ρ_{AB_1} in Supplementary Note V and conduct the partly traverse for possible ρ_{AB_1} by the semi-definite programming [17]. As shown in Fig. S6, it can be seen that all the secret key rates for QPSK-BE-QKD under possible collective attacks we partly traversed are not less than the secret key rate under the collective entangling clone attack. This suggests that QPSK-BE-QKD has some potential to have a performance advantage over conventional QPSK-CVQKD under general collective attacks. It can also be seen from Fig. 6 that QPSK-BE-QKD can achieve the higher secret key rate and the longer distance than the BPSK-BE-QKD

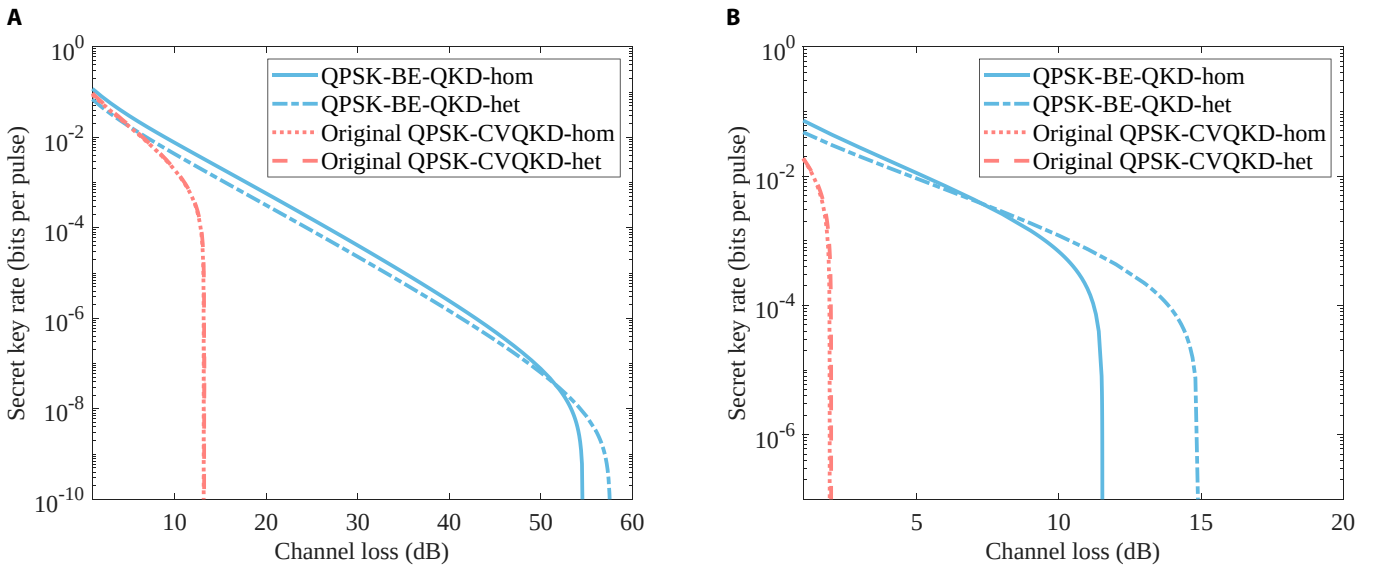

Fig. 6. Secret key rates of QPSK-BE-QKD via the channel loss for the excess noise (A) $\varepsilon = 0.02$ or (B) $\varepsilon = 0.05$ in the linear Gaussian channel under collective attacks. Here, we ignore the detection efficiency and the electrical noise. The modulation variance is $V_A = 1$ for QPSK-BE-QKD. For original QPSK-CVQKD, we set its modulation variance V_A to the optimal value obtained through traversal.

under collective attacks, which is consistent with the conclusion obtained under individual attacks. This is because the overall mutual information between Alice and Bob for QPSK-BE-QKD and BPSK-BE-QKD can be considered approximately equal (because the overall average bit error rates between Alice and Bob for these 2 protocols are completely the same, where the bit error rate only depends on the absolute value of the difference between the X and P components of each constellation point). At the same time, the constellation diagram of QPSK-BE-QKD will decrease the orthogonality between the conditional quantum states $\rho_E^{x=m}$ and $\rho_E^{p=m}$ while making it more difficult for Eve to conduct the maximum mutual information discrimination of $\rho_E^{x=m}$ and $\rho_E^{p=m}$. Above all, B/QPSK-BE-QKD can quite improve the secure transmission distance and the tolerable channel excess noise.

Figure 7 shows secret key rates of B/QPSK-BE-QKD via the modulation variance in the linear Gaussian channel under collective attacks. The result shows that the modulation variance V_A has its best value for B/QPSK-BE-QKD. The best value of the modulation variance V_A is 0.49 and 1.04 for BPSK-BE-QKD and QPSK-BE-QKD, respectively.

Then, we further study the relationship between the modulation constellation and the secret key for BPSK-BE-QKD. As shown in Fig. 8A, we translate the constellation points along the $y = x$ axis. The calculation of the mutual information between Alice and Bob in this situation is detailed in Supplementary Note I. The calculation of the leaked information to Eve for this situation is completely the same with the discussion above, because changing the constellation diagram only changes α_k in Eq. 12, and we can still use Eqs. 3, 12, to 22

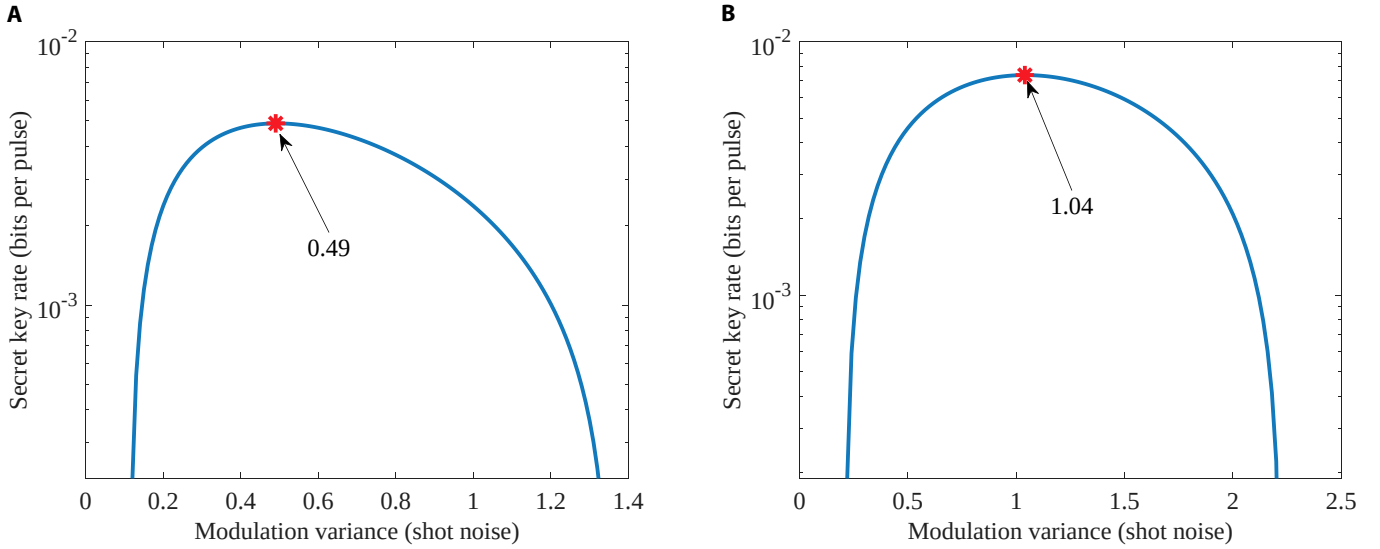

Fig. 7. Secret key rates of (A) BPSK-BE-QKD or (B) QPSK-BE-QKD via the modulation variance with homodyne detection in the linear Gaussian channel under collective attacks. The channel loss is $T = 10$ dB, and the excess noise is $\varepsilon = 0.02$.

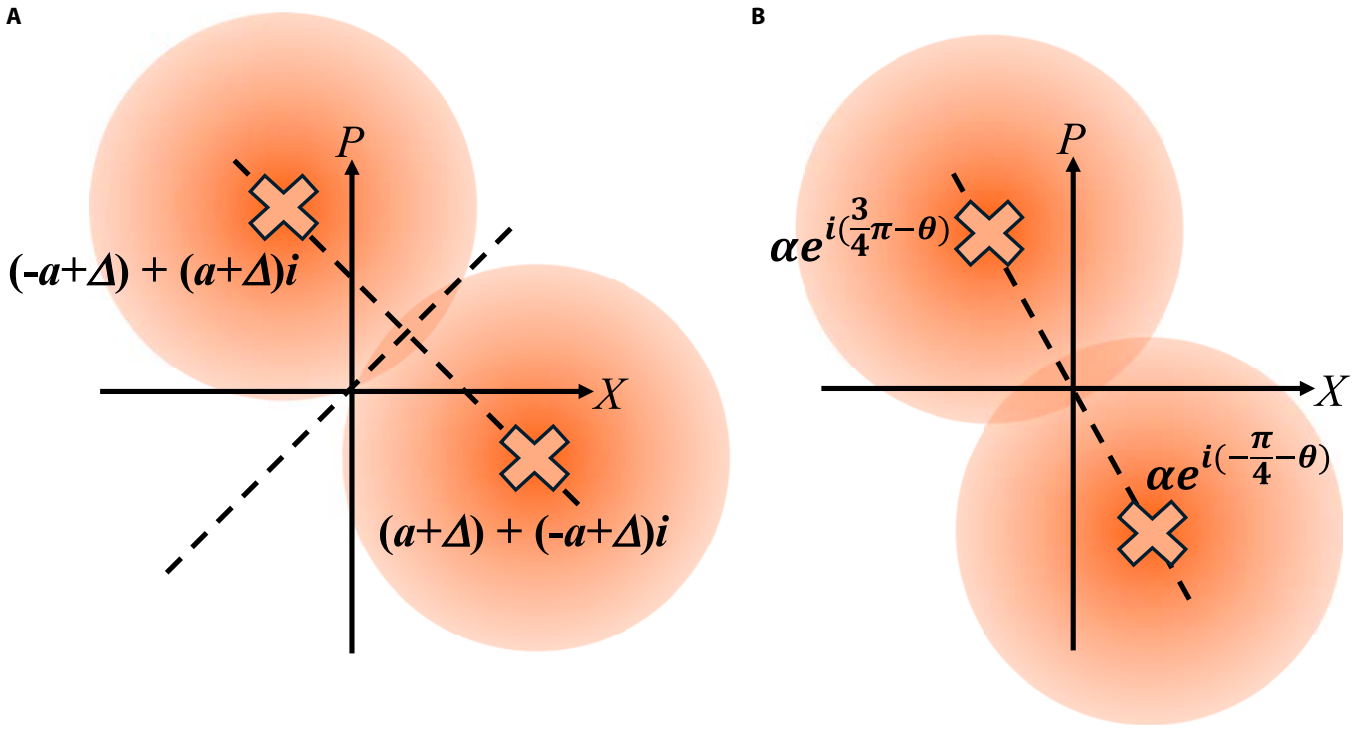

Fig. 8. Illustration of (A) the translation of constellation points and (B) the rotation of constellation points for BPSK-BE-QKD.

to calculate the leaked information. Figure 9A shows secret key rates of BPSK-BE-QKD via the translation distance Δ. It can be seen that translating the constellation points along the $y = x$ axis will not influence the secret key rate for BPSK-BE-QKD. Because no matter how the constellation points are translated along the $y = x$ axis, the probability density curves of the corresponding detection values when Bob performs the X and P measurements are always exactly the same. So, translation along the $y = x$ axis will not affect the performance of judging whether Bob performs an X or P measurement for both Alice and Eve and thus will not affect the secret key rate. Then, we rotate the constellation points around the original point as depicted in Fig. 8B. The calculation of the mutual information between Alice and Bob for this constellation is detailed in Supplementary Note I. As shown in Fig. 9B, the more rotations relative to the $y = -x$ axis, the lower the secret key rate is. When constellation points are located at $y = -x$, i.e., the rotation angle is 0, the secret key rate achieves its maximum. We can find that the symmetry relative to the $y = x$ axis is beneficial for BPSK-BE-QKD. Because as the rotation angle increases, the difference between the probability density curves of the corresponding detection values when Bob performs the X and P measurements

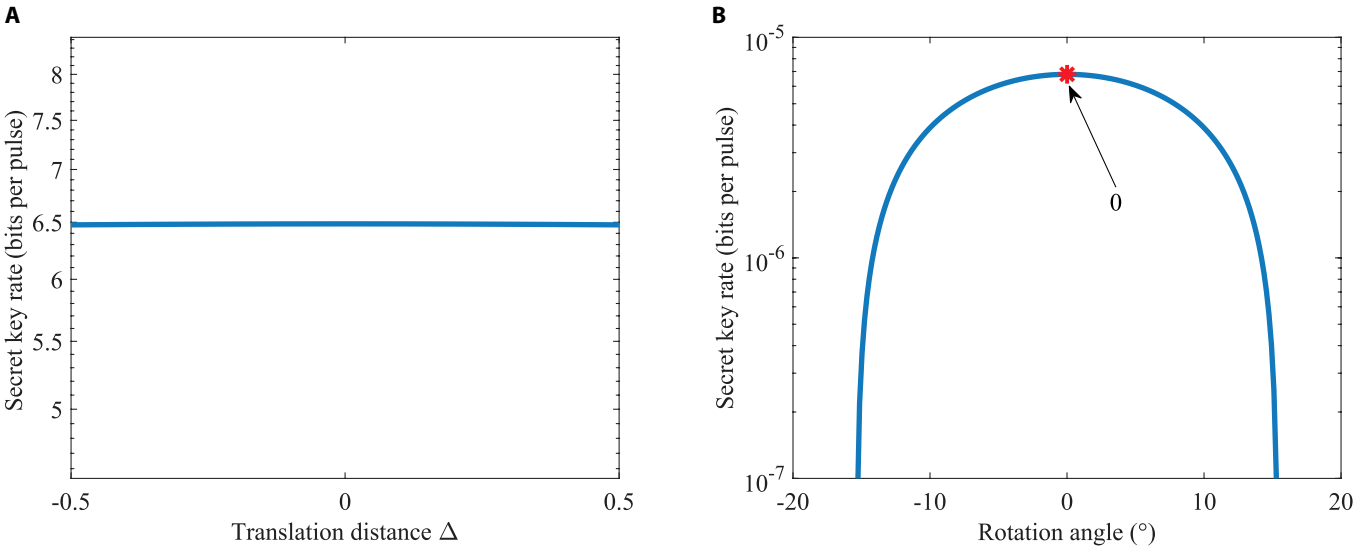

Fig. 9. Secret key rates of BPSK-BE-QKD with homodyne detection via (A) the translation distance Δ or (B) the rotation angle in the linear Gaussian channel under collective attacks. The channel loss is $T = 30$ dB, the excess noise is $\varepsilon = 0.02$, and the modulation variance $V_A = 0.5$.

will become larger. This will help Eve gain an information advantage in the base selection information, resulting in a relatively lower secret key rate.

We finally study the relationship between the modulation constellation and the secret key for QPSK-BE-QKD. We translate the constellation points in 2 different ways. As depicted in Fig. 10A, in the first way, we translate all the constellation points along the $y = x$ axis while fixing the constellation as a regular prism. In the second way, we translate 2 of the constellation points along the $y = x$ axis while fixing the other 2 constellation points at $(-a, 0)$ and $(0, -ai)$, as shown in Fig. 10B. As depicted in Fig. 11A, we observe that translating all the constellation points along the $y = x$ axis does not affect the secret key rate, similar to the protocol property observed in BPSK-BE-QKD. It is because of the similar reason discussed for Fig. 9A, i.e., the probability density curves of the corresponding detection values when Bob performs the X and P measurements are always exactly the same while translating all the constellation points along the $y = x$ axis. As shown in Fig. 11B, we know that if we fix 2 constellation points and translate the other 2 constellations along the $y = x$ axis, the secret key rate has its maximum value and the translation distance has its best value (i.e., the modulation constellation has its best shape). We can find that in this situation, the best shape of the modulation constellation is the rectangle. This is because only translating 2 of the constellation diagram's 4 points along the $y = x$ axis will cause the amount of information leaked to Eve to first decrease and then increase. Meanwhile, the overall mutual information between Alice and Bob can be seen as approximately equal, because the overall average bit error rate between Alice and Bob remains completely unchanged. Thus, the secret key rate will first increase and then decrease.

Experimental demonstration

To verify the feasibility of the BE-QKD protocol, we conduct an experiment demonstration of QPSK-BE-QKD under the 50.5-km optical fiber. The experiment step of QPSK-BE-QKD is demonstrated in Fig. 12. At the Alice site, a narrow-linewidth continous-wave (CW) laser with 100-Hz linewidth (NKT Koheras BASIK X15) is used to generate the optical carrier, followed by an optical isolator (ISO) to prevent the reflected light transmitting into the laser. Then, the optical light is splitted into 2 parts by the 50:50 beam splitter 1 (BS1). One part is transmitted to the Bob site to serve as a local osillator (LO), and the 90:10 BS3 is deployed to monitor the power of the LO. The other part served as the signal (SIG). Here, we used the pilot sequence scheme [48], where we alternately generate the pilot signal and the quantum signal. The amplitude of the pilot signal is 10 times larger than the quantum signal. It is used as the reference signal with the fixed amplitude and phase to help find the peak point of the pulse for Bob and correct the fast phase drift of quantum signals [48] due to the inconsistency in the arrival time of LO and SIG light at the receiver. SIG light is first sent into the phase modulator (PM; EOSPACE) to achieve the QPSK modulation (modulated as 4 states $|a\rangle$, $|ai\rangle$, $|-a\rangle$, and $|-ai\rangle$, where $a = \sqrt{V_A/2}$). Meanwhile, an arbitrary wave generator (AWG; Tektronix, AWG5200) is used to output a electronic analog signals $\theta(t)$ with the 50-MHz symbol rate to the PM, where $\theta(t)$ is controlled by random number data. When the random number is $\{0, 1, 2, 3\}$, $\theta(t) = \left\{0, \frac{V_\pi}{2}, V_\pi, -\frac{V_\pi}{2}\right\}$, where V_π is the half-wave voltage for PM. An ultra-high-extinction-ratio amplitude modulator (AM; EOSPACE) is deployed to cut the CW SIG light into pulse light with the 20% duty cycle. It is also controlled by the electronic analogy signal generated by the AWG, and its direct current (DC) bias voltage is provided by a DC stabilized power. Moreover, the phase of the modulation of the pilot signal is fixed to 0 (i.e., $\theta(t) = 0$), and we make its amplitude 10 times that of the quantum signal by the AM. Then, the SIG light is attenuated by variable optical attenuator (VOA) to control the modulation variance V_A. A 90:10 BS2 monitors the channel input optical power in real

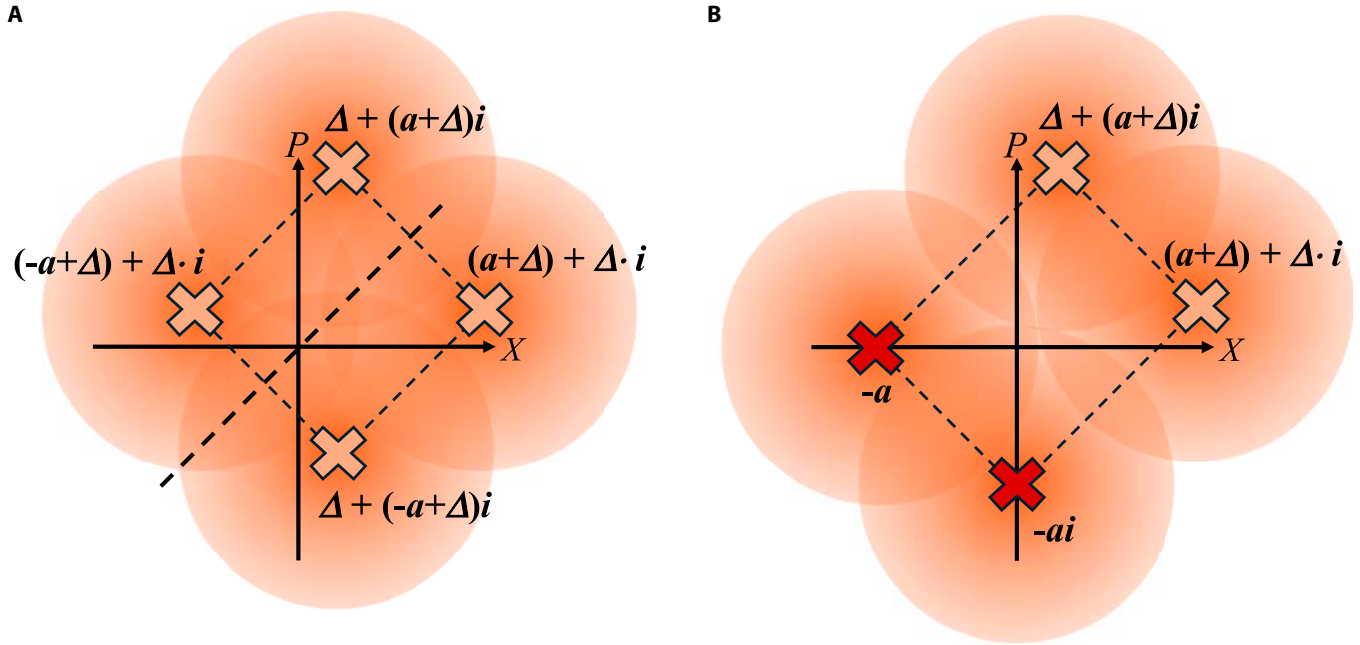

Fig. 10. Illustration of (A) translating all the constellation points while fixing the constellation diagram as a regular prism and (B) translating 2 of the constellation points while fixing the other 2 constellation points at $(-a, 0)$ and $(0, -ai)$ for QPSK-BE-QKD.

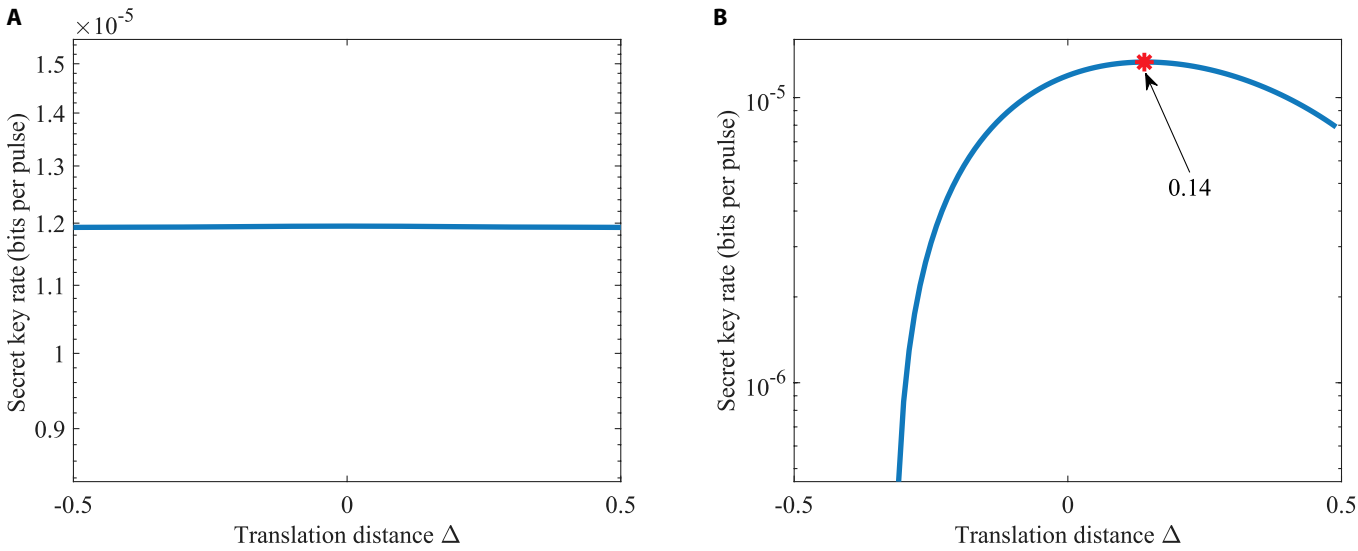

Fig. 11. Secret key rates of QPSK-BE-QKD with homodyne detection via the translation distance in the linear Gaussian channel under collective attacks when (A) translating all the constellation points while fixing the constellation diagram as a regular prism or (B) translating 2 of the constellation points while fixing the other 2 constellation points at $(-a, 0)$ and $(0, -ai)$. The channel loss is $T = 30$ dB, the excess noise is $\varepsilon = 0.02$, and the modulation variance $V_A = 0.5$.

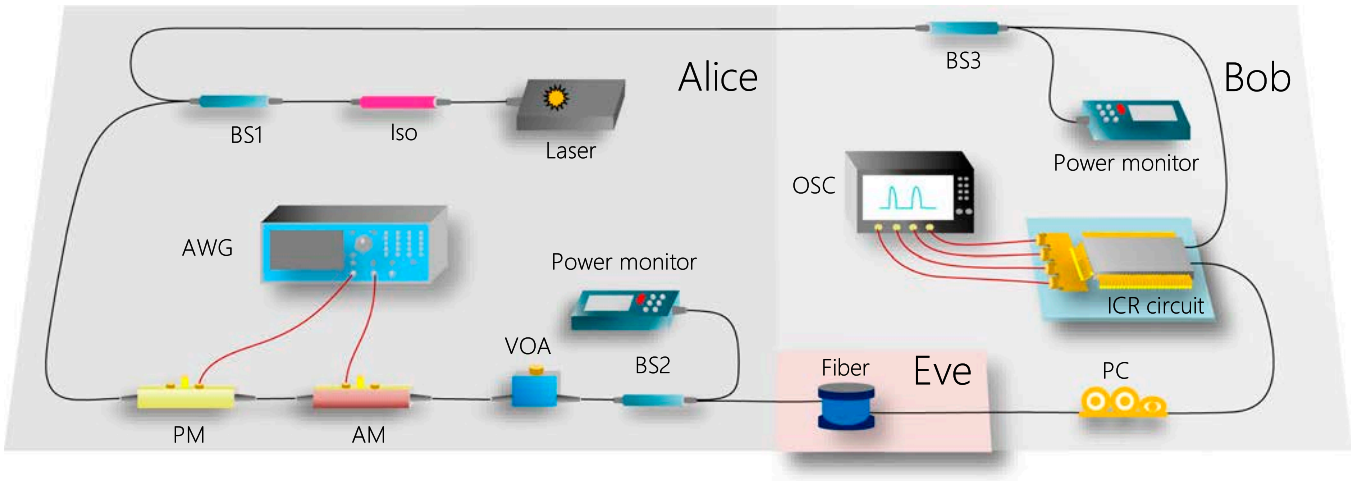

Fig. 12. Experimenntal demonstration of QPSK-BE-QKD.

time, followed by a 50.5-km fiber channel with 11 dB. It is noted that the channel is assumed to be fully controlled by Eve.

At the Bob site, a polarization controller (PC) is deployed to adjust the polarization of the SIG light to minimize the component on the V polarization of the SIG light as much as possible. Then, the LO and SIG lights are injected into the integrated conherent receiver (ICR; FUJITSU) circuit to measure the X and P quadratures, and randomly choose one of them as final measurement results. The detected signals are sampled by a real-time oscilloscope (OSC; Lecroy, WaveRunner 9404M-MS) with 1 GSamples/s sampling rate (20 sample points for one symbol). In the end, Bob announces the measurement results publicly and Alice tries to guess the measurement bases according to the decoding rule. The quantum efficiency is $\eta = 0.48$. The electrical noise $v_{el} = 0.0997$ (shot noise units), which is calibrated by sampling data without connecting the LO. Moreover, the frame length we used is10^5.

Then, we first need to find the peak point for each pulse. We calculate the power of the first 4×10^5 sampling data and find

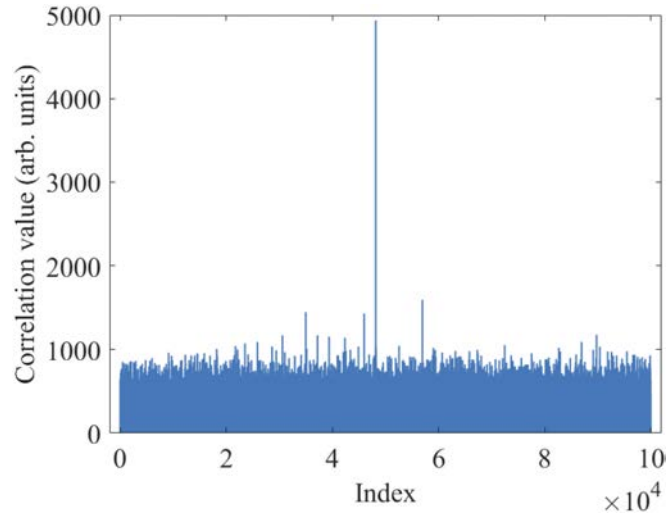

Fig. 13. Correlation value of the frame synchronization sequence and the received frame at different indices.

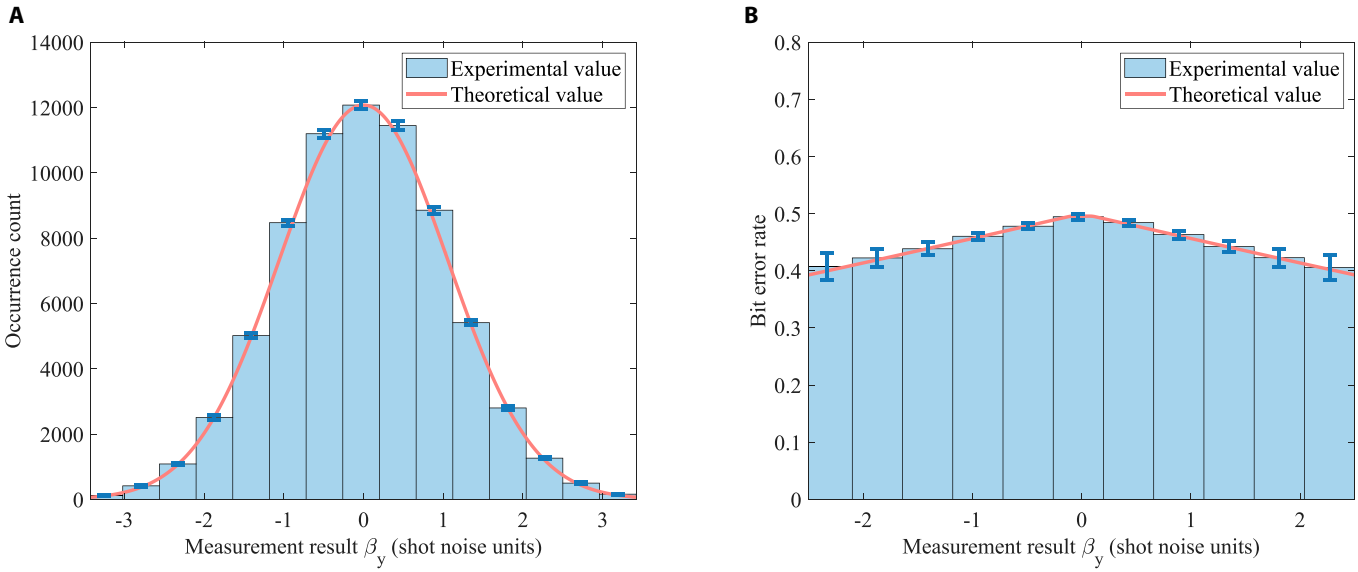

Fig. 14. The experimental and theoretical value of (A) the occurrence count and (B) the bit error rate via different measurement results β_y. The error bars denote the standard deviation (SD) of the experimental data.

its maximum value P_i. The corresponding index $i \ mod \ 20$ is the optimal sampling position. Then, we can extract the final sampling data at every 20 points from the optimal sampling position. Then, we use the pilot signal data to correct the fast phase drift of the quantum signal data. We directly use the phase angle of the 2 pilot signals to rotate the quantum signal and recover the quantum signal with the following formula:

$$A_j^{rot} = \sqrt{\frac{x_j^p + ip_j^p}{\left|x_j^p + ip_j^p\right|}} \cdot \sqrt{\frac{x_{j+1}^p + ip_{j+1}^p}{\left|x_{j+1}^p + ip_{j+1}^p\right|}} \tag{38}$$

$$x_j^q + ip_j^q \leftarrow \frac{x_j^q + ip_j^q}{A_j^{rot}} \tag{39}$$

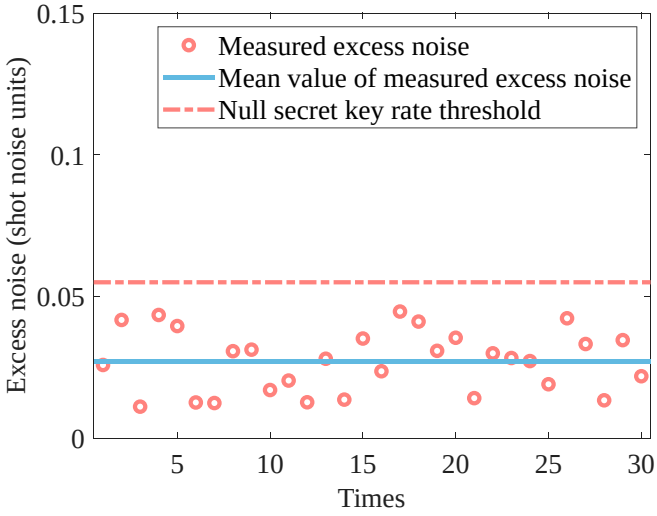

Fig. 15. Measured excess noise. The red circles represent the measured excess noise. The blue solid line represents the mean value of the measured excess noise. The red dash-dot line represents the excess noise threshold of the null secret key rate.

where x_j^p and p_j^p are the X and P component of the jth pilot signal, and x_j^q and p_j^q are the X and P components of the jth quantum signal.

In order to obtain the correlation between modulation data and receive data, we need to achieve the precise frame synchronization. We use a robust synchronizaion method proposed in [49] to find the frame header. The synchronization result is shown in Fig. 13. We observe that the correlation between the frame synchronization sequence and the received frame reaches its peak at index 48159, which is significantly higher than other indices. So, we successfully achieve the frame synchronization to get the correlation between modulation data and receive data. Then, we compensate the slow phase drift due to the slow

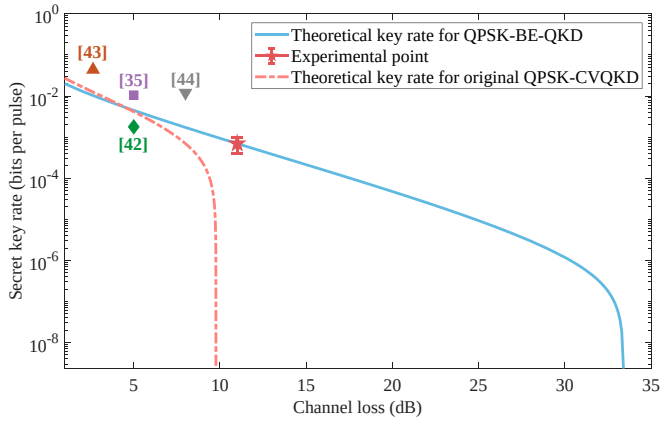

Fig. 16. Secret key rate via the channel loss. The red star point corresponds to the experimental result under the 50.5-km optical fiber. The blue solid curve shows the simulated secret key rates of QPSK-BE-QKD calculated from estimated parameters in the experiment. The red dash-dot curve shows the simulated secret key rates of the original QPSK-CVQKD calculated from the same parameters estimated in the experiment except the modulation variance V_A (we set its V_A to the optimal value obtained through traversal). Purple squares, green prisms, brown upper triangles, and gray lower triangles represent results in [35,42–44], respectively. The error bars denote the SD of the experimental data.

fluctuation of the transmission path length [50]. We also analyze the occurrence probabilities and the bit error rate between Alice and Bob for different measurement results β_y, as depicted in Fig. 14. The results show that the experimental value is consistent with the theoretical curve, where the theortical curve can be calculated according to the mutual information analysis above. Finally, we conduct the parameter evaluation, and the measured excess noises of 30 frames are shown in Fig. 15. We get that the mean modulation variance V_A is 1.003 and the mean excess noise ϵ is 0.02716. Meanwhile, we use a high-efficient information reconcilization algorithm [51] to make the reconcilization efficiency β reach 96.58%. Based on the calculation method for the secret key rate discussed above, we finally obtain the 13.12-kbps secret key rate under the 50.5-km optical fiber with 11-dB loss, as shown in Fig. 16. Based on the estimated parameters in the experiment, our QPSK-BE-QKD can theoretically sustain secure key generation under the 33-dB channel loss. It is noted that based on the same parameters estimated in our experiment except the modulation variance V_A (we set its V_A to the optimal value obtained through traversal), the original QPSK-CVQKD can only tolerate a maximum channel loss of approximately 10 dB.

Discussion

We have provided a security analysis of DMCS-BE-QKD protocol under individual and collective attacks in the linear Gaussian channel. The simulation result shows that the B/QPSK-BE-QKD protocol shows the better tolerance for the channel loss and excess noise than the original B/QPSK-CVQKD. The result shows that the B/QPSK-BE-QKD has potential to surpass the original B/QPSK-CVQKD without the channel assumption. We also conduct a proof-of-principle experiment for QPSK-BE-QKD under a 50.5-km optical fiber with 11-dB loss to prove the feasibility of the BE scheme. Since the quantum communication part of the BE-QKD scheme is the same as the traditional CVQKD, one can naturally choose the basis encoding or the traditional way in the practical application to optimize the secret key rate after the parameter estimation. Thus, the BE-QKD scheme can be perfectly compatible with the existing CVQKD terminals and applied in quantum access networks and quantum metropolitan networks, further promoting the quantum Internet as a reality. In addition, the BE scheme, as well as the security analysis framework proposed in this paper, have the potential to be applied to other QKD protocols and quantum secure direct communication [52–54] to further improve their performance. In conclusion, we believe the BE-QKD scheme provides an efficient way for practical secure quantum cryptography communication in large-scale and harsh environments.

In the future, we will try to analyze the secret key rate of DMCS-BE-QKD under collective attacks without the channel assumption. Theoretically, we need to traverse all possible states at AB_1 and all possible purifications of ρ_{AB_1}, and then use the one that will maximize the leaked information to Eve to calculate the leaked information. In Supplementary Note V, we prove that the leaked information remains unchanged for different purifications of ρ_{AB_1} under collective attacks. So, we just need to traverse all possible states at AB_1. We obtain hundreds of feasible ρ_{AB_1} under the constraints [17] for the general channel by the semi-definite programming and calculate the corresponding secret key rates. The simulation result shows that secret key rates under possible collective attacks we partly traversed are not less than the secret key rate under the collective entangling clone attack. This partly indicates that the collective entangling clone attack is likely to be the optimal attack. To traverse all possible states at AB_1, we will try more related numerical methods to solve this problem.

Acknowledgments

Funding: This work was supported by the Innovation Program for Quantum Science and Technology (grant no. 2021ZD0300703), Shanghai Municipal Science and Technology Major Project (2019SHZDZX01), the Key R&D Program of Guangdong province (grant no. 2020B0303040002), and the National Natural Science Foundation of China (no. 62101320).
Author contributions: G.Z. conceived the research project. P.H. developed the idea of DMCS-BE-QKD. M.G. performed the calculations and simulations of the secret key rate of DMCS-BE-QKD. M.G., L.H., X.L., T.W., and X.J. performed the proof-of-principle experiment. M.G., P.H., and G.Z. analyzed the data. All authors contributed to the writing of the paper.
Competing interests: The authors declare that they have no competing interests.

Data Availability

All of the data that support the findings of this study are reported in the main text and the Supplementary Materials. Source data are available from the corresponding authors on reasonable request.

Supplementary Materials

Supplementary Notes I to VIII
Figs. S1 to S6

References

1. Grosshans F, Grangier P. Continuous variable quantum cryptography using coherent states. *Phys Rev Lett*. 2002;88(5):Article 057902.
2. Grosshans F, Van Assche G, Wenger J, Brouri R, Cerf NJ, Grangier P. Quantum key distributions using gaussian-modulated coherent states. *Nature*. 2003;421(6920):238–241.
3. Weedbrook C, Lance AM, Bowen WP, Symul T, Ralph TC, Lam PK. Quantum cryptography without switching. *Phys Rev Lett*. 2004;93(17):Article 170504.
4. Lance AM, Symul T, Sharma V, Weedbrook C, Ralph TC, Lam PK. No-switching quantum key distribution using broadband modulated coherent light. *Phys Rev Lett*. 2005;95(18):Article 180503.
5. Weedbrook C, Pirandola S, Garcia-Patrón R, Cerf NJ, Ralph TC, Shapiro JH, Lloyd S. Gaussian quantum information. *Rev Mod Phys*. 2012;84(2):621–669.
6. Leverrier A, Grangier P. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Phys Rev Lett*. 2009;102(18): Article 180504.
7. Zhao YB, Heid M, Rigas J, Lütkenhaus N. Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks. *Phys Rev A*. 2009;79(1):Article 012307.

8. Sych D, Leuchs G. Coherent state quantum key distribution with multi letter phase-shift keying. *New J Phys*. 2010;12(5):Article 053019.
9. Lütkenhaus N. Security against eavesdropping in quantum cryptography. *Phys Rev A*. 1996;54(1):97.
10. Slutsky BA, Rao R, Sun PC, Fainman Y. Security of quantum cryptography against individual attacks. *Phys Rev A*. 1998;57(4):2383.
11. Bechmann-Pasquinucci H. Eavesdropping without quantum memory. *Phys Rev A*. 2006;73(4):Article 044305.
12. Grosshans F, Cerf NJ, Wenger J, Tualle-Brouri R, Grangier P. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. *Quantum Inf Comput*. 2003;3(7):535–552.
13. Biham E, Mor T. Security of quantum cryptography against collective attacks. *Phys Rev Lett*. 1997;78(11):2256.
14. Garcia-Patrón R, Cerf NJ. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. *Phys Rev Lett*. 2006;97(19):Article 190503.
15. Navascués M, Grosshans F, Acin A. Optimality of Gaussian attacks in continuous-variable quantum cryptography. *Phys Rev Lett*. 2006;97(19):Article 190502.
16. Ghorai S, Grangier P, Diamanti E, Leverrier A. Asymptotic security of continuous-variable quantum key distribution with a discrete modulation. *Phys Rev X*. 2019;9(2):Article 021059.
17. Lin J, Upadhyaya T, Lütkenhaus N. Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution. *Phys Rev X*. 2019;9(4):Article 041064.
18. 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.
19. Kaur E, Guha S, Wilde MM. Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution. *Phys Rev A*. 2021;103(1):Article 012412.
20. 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(8):Article 080501.
21. Renner R, Gisin N, Kraus B. Information-theoretic security proof for quantum-key-distribution protocols. *Phys Rev A*. 2005;72(1):Article 012332.
22. Renner R, Cirac JI. de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. *Phys Rev Lett*. 2009;102(11):Article 110504.
23. Coles PJ, Metodiev EM, Lütkenhaus N. Numerical approach for unstructured quantum key distribution. *Nat Commun*. 2016;7(1):11712.
24. 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(20):Article 200501.
25. Leverrier A, Garcia-Patrón R, Renner R, Cerf NJ. Security of continuous-variable quantum key distribution against general attacks. *Phys Rev Lett*. 2013;110(3):Article 030502.
26. Leverrier A. Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction. *Phys Rev Lett*. 2017;118(20):Article 200501.
27. Matsuura T, Maeda K, Sasaki T, Koashi M. Finite-size security of continuous-variable quantum key distribution with digital signal processing. *Nat Commun*. 2021;12(1):252.
28. Lupo C, Ouyang Y. Quantum key distribution with nonideal heterodyne detection: Composable security of discrete-modulation continuous-variable protocols. *PRX Quantum*. 2022;3(1):Article 010341.
29. Kanitschar F, George I, Lin J, Upadhyaya T, Lütkenhaus N. Finite-size security for discrete-modulated continuous-variable quantum key distribution protocols. *PRX Quantum*. 2023;4(4):Article 040306.
30. Lodewyck J, Bloch M, Garcia-Patrón R, Fossier S, Karpov E, Diamanti E, Debuisschert T, Cerf NJ, Tualle-Brouri R, McLaughlin SW, et al. Quantum key distribution over 25km with an all-fiber continuous-variable system. *Phys Rev A*. 2007;76(4):Article 042305.
31. Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P, Diamanti E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat Photonics*. 2013;7(5):378–381.
32. Huang D, Lin D, Wang C, Liu W, Fang S, Peng J, Huang P, Zeng G. Continuous-variable quantum key distribution with 1 mbps secure key rate. *Opt Express*. 2015;23(13):17511–17519.
33. Wang T, Huang P, Zhou Y, Liu W, Ma H, Wang S, Zeng G. High key rate continuous-variable quantum key distribution with a real local oscillator. *Opt Express*. 2018;26(3):2794–2806.
34. Zhang Y, Chen Z, Pirandola S, Wang X, Zhou C, Chu B, Zhao Y, Xu B, Yu S, Guo H. Long-distance continuous-variable quantum key distribution over 202.81 km of fiber. *Phys Rev Lett*. 2020;125(1):Article 010502.
35. Wang H, Li Y, Pi Y, Pan Y, Shao Y, Ma L, Zhang Y, Yang J, Zhang T, Huang W, et al. Sub-Gbps key rate four-state continuous-variable quantum key distribution within metropolitan area. *Commun Phys*. 2022;5(1):162.
36. Jouguet P, Kunz-Jacques S, Debuisschert T, Fossier S, Diamanti E, Alléaume R, Tualle-Brouri R, Grangier P, Leverrier A, Pache P, et al. Field test of classical symmetric encryption with continuous variables quantum key distribution. *Opt Express*. 2012;20(13):14030–14041.
37. Huang D, Huang P, Li H, Wang T, Zhou Y, Zeng G. Field demonstration of a continuous-variable quantum key distribution network. *Opt Lett*. 2016;41(15):3511–3514.
38. Karinou F, Brunner HH, Fung CHF, Comandar LC, Bettelli S, Hillerkuss D, Kuschnerov M, Mikroulis S, Wang D, Xie C, et al. Toward the integration of CV quantum key distribution in deployed optical networks. *IEEE Photon Technol Lett*. 2018;30(7):650–653.
39. Zhang Y, Li Z, Chen Z, Weedbrook C, Zhao Y, Wang X, Huang Y, Xu C, Zhang X, Wang Z, et al. Continuous-variable QKD over 50 km commercial fiber. *Quantum Sci Technol*. 2019;4(3):Article 035006.
40. Kumar R, Qin H, Alléaume R. Coexistence of continuous variable QKD with intense DWDM classical channels. *New J Phys*. 2015;17(4):Article 043027.
41. Huang P, Huang J, Zhang Z, Zeng G. Quantum key distribution using basis encoding of Gaussian-modulated coherent states. *Phys Rev A*. 2018;97(4):Article 042311.
42. Eriksson TA, Luis RS, Puttnam BJ, Rademacher G, Fujiwara M, Awaji Y, Furukawa H, Wada N, Takeoka M, Sasaki M. Wavelength division multiplexing of 194 continuous variable quantum key distribution channels. *J Lightwave Technol*. 2020;38(8):2214–2218.
43. Milovančev D, Vokić N, Laudenbach F, Pacher C, Hübel H, Schrenk B. Spectrally-shaped continuous-variable QKD operating at 500 MHz over an optical pipe lit by 11 DWDM

channels. Paper presented at: Proceedings of the Optical Fiber Communication Conference; 2020; San Diego, CA, USA.
44. Laudenbach F, Schrenk B, Pacher C, Hentschel M, Fung CHF, Karinou F, Poppe A, Peev M, Hübel H. Pilot-assisted intradyne reception for high-speed continuous-variable quantum key distribution with true local oscillator. *Quantum*. 2019;3:193.
45. Devetak I, Winter A. Distillation of secret key and entanglement from quantum states. *Proc R Soc A*. 2005;461(2053):207–235.
46. Nielsen MA, Chuang IL. *Quantum computation and quantum information.* Cambridge (England): Cambridge Univ. Press; 2010.
47. Řeháček J, Englert BG, Kaszlikowski D. Iterative procedure for computing accessible information in quantum communication. *Phys Rev A*. 2005;71(5):Article 054303.
48. Wang T, Huang P, Li L, Zhou Y, Zeng G. High key rate continuous-variable quantum key distribution using telecom optical components. *New J Phys*. 2024;26(2):Article 023002.
49. Wang P, Huang P, Chen R, Zeng G. Robust frame synchronization for free-space continuous-variable quantum key distribution. *Opt Express*. 2021;29(16):25048–25063.
50. Huang P, Wang T, Chen R, Wang P, Zhou Y, Zeng G. Experimental continuous-variable quantum key distribution using a thermal source. *New J Phys*. 2021;23(11):Article 113028.
51. Wang X, Zhang Y, Yu S, Xu B, Li Z, Guo H. Efficient rate-adaptive reconciliation for continuous-variable quantum key distribution. *Quantum Inf Comput*. 2017;17:1123–1134.
52. Cao Z, Wang L, Liang K, Chai G, Peng J. Continuous-variable quantum secure direct communication based on Gaussian mapping. *Phys Rev Appl*. 2021;16(2):Article 024012.
53. Cao Z, Lu Y, Chai G, Yu H, Liang K, Wang L. Realization of quantum secure direct communication with continuous variable. *Research*. 2023;6:0193.
54. Paparelle I, Mousavi F, Scazza F, Bassi A, Paris M, Zavatta A. Practical quantum secure direct communication with squeezed states. arXiv. 2023. https://doi.org/10.48550/arXiv.2306.14322