Quantum key distribution using basis encoding of Gaussian-modulated coherent states

Peng Huang,[1,*] Jingzheng Huang,[1] Zheshen Zhang,[2] and Guihua Zeng[1,†]
[1]*Center for Quantum Sensing and Information Processing, State Key Laboratory of Advanced Optical Communication Systems and Networks, Shanghai Jiao Tong University, Shanghai 200240, China*
[2]*Department of Materials Science and Engineering, College of Optical Sciences, University of Arizona, Tucson Arizona 85721, USA*

(Received 23 November 2017; revised manuscript received 27 February 2018; published 9 April 2018)

The continuous-variable quantum key distribution (CVQKD) has been demonstrated to be available in practical secure quantum cryptography. However, its performance is restricted strongly by the channel excess noise and the reconciliation efficiency. In this paper, we present a quantum key distribution (QKD) protocol by encoding the secret keys on the random choices of two measurement bases: the conjugate quadratures X and P. The employed encoding method can dramatically weaken the effects of channel excess noise and reconciliation efficiency on the performance of the QKD protocol. Subsequently, the proposed scheme exhibits the capability to tolerate much higher excess noise and enables us to reach a much longer secure transmission distance even at lower reconciliation efficiency. The proposal can work alternatively to strengthen significantly the performance of the known Gaussian-modulated CVQKD protocol and serve as a multiplier for practical secure quantum cryptography with continuous variables.

DOI: 10.1103/PhysRevA.97.042311

I. INTRODUCTION

Quantum key distribution (QKD) provides an efficient way for two trusted parties to share a secure secret key string through an untrusted channel which is assumed to be controlled by the potential eavesdropper Eve. Nowadays, two families of QKD protocols are proposed: the discrete-variable QKD (DVQKD) [1,2] and continuous-variable QKD (CVQKD) [3–7] protocols. The secret key bits are encoded on the discrete spectrum of single photons and obtained by photon-counting measurements for the former one, while in the latter one, the secret key information is commonly encoded on the values of the light field quadratures of multiphoton quantum states, which are obtained by coherent detections. So far, the DVQKD and Gaussian-modulated coherent-state (GMCS) [4] CVQKD protocols have been proved secure against individual [8–11], collective [12–15], and coherent attacks [16–18] even when taking into account the finite-size effects [19–21].

The CVQKD protocol inherits the merits of high detection efficiency, high channel capacity, and superior compatibility with intense classical optical channels [22] from coherent optical communications. However, its secure transmission distance is too short compared to its counterpart. One of two main reasons is that the CVQKD protocol is quite sensitive to excess noise, which includes the unavoidable channel excess noise and the extra noise originated from the practical CVQKD system [23,24]. The other one is that CVQKD schemes require unique and a far more complicated error correction procedure, which further restricts the secure transmission distance. The proposal of discrete-modulated (DM) CVQKD [25,26], where the secret keys are encoded on the signs of the values of the quadratures, is just for the purpose of improving the reconciliation efficiency at low SNR by using a binary error correction code (ECC) to increase the secure transmission distance. Although other approaches, such as developing an efficient error-correcting code for Gaussian signals [27] and controlling the system excess noise directly [28] or by using a locally generated local oscillator [29–32], can be used to improve the secure transmission distance of GMCS CVQKD to some extent, the property of high sensitivities to excess noise and reconciliation efficiency of these value-encoding (VE) CVQKD schemes still fundamentally restricts their performance. The unavoidable high level of channel excess noise is common in practical application of the CVQKD protocol [33], and its fluctuation will further lower the reconciliation efficiency. Moreover, a recent report [34] shows that the frame error rate [28,35,36] of the ECC may further restrict the real reconciliation efficiency.

In this paper, we develop a QKD protocol which encodes secret keys on the discrete-distributed measurement bases of the Gaussian-modulated coherent states while not directly encoding the secret information on the continuous-distributed quadrature values as usual. Physically, this way may dramatically weaken the effects of channel excess noise and reconciliation efficiency on the secret key rate. We exemplify the security of the proposed scheme under a typical non-Gaussian individual attack, i.e., the partial intercept-resend attack combined with the beam-splitting attack [37]. In such a scenario, the proposed scheme may reduce observably the bound of leaked information to the eavesdropper, and subsequently, much higher performance may be obtained than that of the previous GMCS CVQKD scheme even with lower reconciliation efficiency.

II. THE BASIS-ENCODING QKD PROTOCOL

The proposed protocol, which is depicted in Fig. 1, executes the following steps: (1) Alice draws two random values, i.e., X_A, P_A, with Gaussian distributions $N \sim \mathcal{N}(0,V_A)$ to prepare

[*] huang.peng@sjtu.edu.cn
[†] ghzeng@sjtu.edu.cn

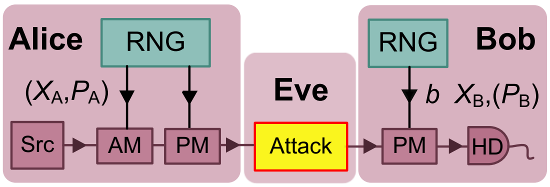

FIG. 1. Diagram of the basis-encoding CVQKD protocol. Src, coherent source; RNG, random number generator; AM, amplitude modulator; PM, phase modulator; HD, homodyne detector.

a coherent state $|X_A + iP_A\rangle$ and sends it to Bob. (2) Bob measures either quadrature X or P according to an independently generated random binary value b and obtains measurement results X_B, P_B related to X_A, P_A, respectively. (3) Alice and Bob perform a parameter estimation processing. In detail, Alice and Bob randomly choose a fraction of measurement results, and then Alice discards the uncorrelated quadrature to share a set of correlated Gaussian variables, which is used to evaluate the modulation variance, excess noise, and transmission efficiency. (4) For the residual measurement results, Bob informs Alice about the outcome values of his homodyne detection, and Alice judges the measurement basis Bob has used. For example, when $b = 0$, Bob measured the X quadrature and Alice also guesses that Bob has measured the X quadrature; then she decodes this value correctly as secret key 0, otherwise she gets an incorrect secret key 1. After these operations, Alice and Bob share a set of correlated binary raw key. (5) Alice and Bob perform reconciliation with binary codes and privacy amplification to distill a final secret key. We note that the quantum state transmission and the parameter estimation run the same as the conventional CVQKD protocol, while the obtained raw key and the following processing are different.

The decoding rules employed in the Step IV) are summarized as follows:

Correct decoding:
When $X_E > P_E$, $\beta_E^x X_B > C_E$ or $\beta_E^p P_B < C_E$
When $X_E < P_E$, $\beta_E^x X_B < C_E$ or $\beta_E^p P_B > C_E$
Incorrect decoding:
When $X_E > P_E$, $\beta_E^x X_B < C_E$ or $\beta_E^p P_B > C_E$
When $X_E < P_E$, $\beta_E^x X_B > C_E$ or $\beta_E^p P_B < C_E$

where $C_A = \frac{1}{2}(X_A + P_A)$, and β_A^x and β_A^p are the coefficients employed to give minimum variances of $\Delta X = \beta_A^x X_B - X_A$ and $\Delta P = \beta_A^p P_B - P_A$, respectively. The basic principle is comparing the distances from the adjustment of Bob's measurement result to the two original conjugate quadratures.

In the finite-size scenarios, the secret key rate of the proposed protocol is given by

$$R = \frac{n}{N}[\beta I_{AB} - I_E - \Delta(n)], \tag{1}$$

where I_{AB} is the Shannon mutual information between Alice and Bob, I_E is the leaked information to Eve, $\Delta(n)$ is related to the security of the privacy amplification, β is the reconciliation efficiency, N is the block size of the shared data between Alice and Bob, and n is the number of the pulses used for key generation.

III. THE SECURITY AGAINST INDIVIDUAL ATTACK

Now we exemplify the security of the proposed scheme under the non-Gaussian individual attack, which combines partial intercept-and-resend (IR) and beam-splitting (BS) attacks with an assumption that the channel excess noise ε_c is introduced only in the IR part. In detail, Eve intercepts and resends a fraction μ of the pulses, while she performs a standard BS attack on the remaining fraction $1 - \mu$ of the pulses. In the IR part, Eve performs a simultaneous measurement of both X and P quadratures of the coherent states sent by Alice. Then she produces new ones displaced according to her measurement results and resends them to Bob. For Alice and Bob, the heterodyne measurement and reproduction of the quantum signal will introduce $2N_0$ excess noise, where N_0 is the shot noise variance. For Bob and Eve, Eve's IR operation will increase $2N_0$ modulation variance. In the BS part, Eve will replace the quantum channel with a perfect lossless and noiseless one connecting with a beam splitter with transmission efficiency T, where the extra input of the beam splitter is a Gaussian vacuum state. Then she will perform heterodyne detection on the split coherent state and obtain the results X_E and P_E. Finally, she will decode the secret information with X_E and P_E according to Bob's measurement results.

Suppose that the transmission efficiency is T, the channel excess noise is ε_c, and Bob uses homodyne detection with an efficiency η and electronics noise ν_{el}, then the quadratures of received Gaussian-modulated coherent states in Bob's station can be expressed as

$$\begin{aligned} X_B &= \sqrt{\eta T} X_A + \sqrt{\eta T}\delta X_{ex} + \delta X_v + \delta X_{el}, \\ P_B &= \sqrt{\eta T} P_A + \sqrt{\eta T}\delta P_{ex} + \delta P_v + \delta P_{el}, \end{aligned} \tag{2}$$

where δX_{ex} (δP_{ex}), δX_v (δP_v), and δX_{el} (δP_{el}) are the added extra quadratures arising from channel excess noise, shot noise, and electronic noise of homodyne detection, respectively, and they satisfy $\langle \delta X_{ex}^2\rangle = \langle \delta P_{ex}^2\rangle = \varepsilon_c$, $\langle \delta X_v^2\rangle = \langle \delta P_v^2\rangle = 1$, and $\langle \delta X_{el}^2\rangle = \langle \delta P_{el}^2\rangle = \nu_{el}$ in shot noise units, respectively.

We first consider the error rates of Alice's and Eve's decoding according to Bob's measurement results for the BS attack in the asymptotic regime. For a more general BS attack model, the extra input of the beam splitter is a thermal state. Then a channel excess noise ε_c results. According to Eq. (2), the quantum bit error rate (QBER) between Alice and Bob can be calculated as

$$\begin{aligned} P_e^{AB} &= \int_0^{+\infty} \frac{1}{\sqrt{2\pi}\sigma_{n_1}} \mathrm{erf}\left(\frac{n}{\sqrt{2}\sigma_m}\right) e^{-\frac{n^2}{2\sigma_{n_1}^2}} dn \\ &= \arctan\left(\frac{\sigma_{n_1}}{\sigma_m}\right)/\pi, \end{aligned} \tag{3}$$

where $\sigma_m^2 = 2V_A$, $\sigma_{n_1}^2 = 4\varepsilon_c + \frac{4}{\eta T}(1 + \nu_{el})$, and $\mathrm{erf}(x) = \int_0^x e^{-t^2} dt$ is the error function (see Appendix A for details).

After receiving Bob's measurement results, Eve will decoding the data from her heterodyne detection. The principle of her secret key decoding procedure is similar as Alice's, which

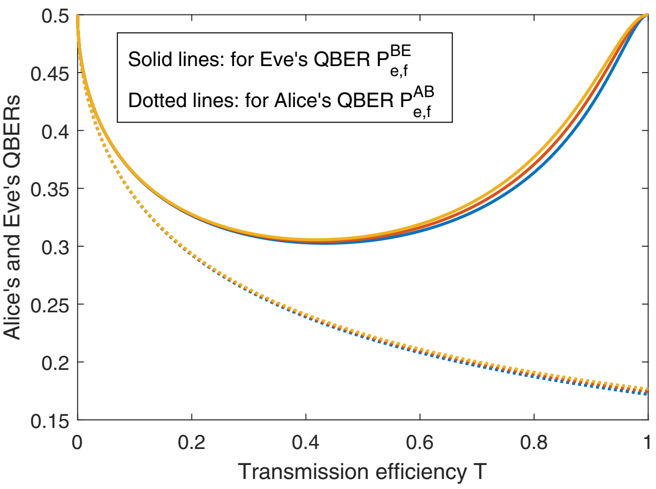

FIG. 2. The QBERs $P^{AB}_{e,f}$ and $P^{BE}_{e,f}$ as a function of transmission efficiency for different channel excess noise ε_c. From bottom to top, $\varepsilon_c = 0.1, 0.16, 0.22$.

can be summarized as

Correct decoding:
When $X_E > P_E$, $\beta^x_E X_B > C_E$ or $\beta^p_E P_B < C_E$
When $X_E < P_E$, $\beta^x_E X_B < C_E$ or $\beta^p_E P_B > C_E$
Incorrect decoding:
When $X_E > P_E$, $\beta^x_E X_B < C_E$ or $\beta^p_E P_B > C_E$
When $X_E < P_E$, $\beta^x_E X_B > C_E$ or $\beta^p_E P_B < C_E$

where $C_E = \frac{1}{2}(X_E + P_E)$, and β^x_E and β^p_E are the coefficients employed to give minimum variances of $\Delta X = \beta^x_E X_B - X_E$ and $\Delta P = \beta^p_E P_B - P_E$, respectively. The QBER between Bob and Eve is given by

$$\begin{aligned} P^{BE}_e &= 1 - \int_{-\infty}^{+\infty} \frac{e^{-\frac{m^2}{2\sigma_m^2}}}{2\sqrt{2\pi}\sigma_m} \mathrm{erfc}\left(\frac{m}{\sqrt{2}\sigma_{n_2}}\right) \\ &\quad \mathrm{erfc}\left(\frac{m}{\sqrt{2}\sigma_{n_3}}\right) dm \\ &= 1 - F_e, \end{aligned} \tag{4}$$

where $F_e = \int_{-\infty}^{+\infty} \frac{e^{-\frac{m^2}{2\sigma_m^2}}}{2\sqrt{2\pi}\sigma_m} \mathrm{erfc}(\frac{m}{\sqrt{2}\sigma_{n_2}}) \mathrm{erfc}(\frac{m}{\sqrt{2}\sigma_{n_3}})\, dm$ is an integrable function with a numerical solution, $\sigma^2_{n_2} = \frac{4}{1-T} + 2(\frac{T}{1-T})^2 \varepsilon_c$, and $\sigma^2_{n_3} = \frac{T^2+(2-T)^2}{(1-T)^2}\varepsilon_c + \frac{4}{\eta T}\nu_{el} + \frac{4-T}{1-T} + (2\sqrt{\frac{1-T}{T}} + \sqrt{\frac{T}{1-T}})^2 + \frac{4(1-\eta)}{\eta T}$ (see Appendix A for details).

Considering the finite-size effect [24], the transmission efficiency T and the channel excess noise ε_c in Eqs. (3) and (4) should be renewed. Here we denote Alice's and Eve's renewed QBERs as $P^{AB}_{e,f}$ and $P^{BE}_{e,f}$ in the finite-size scenarios, respectively (see Appendix A for details). As shown in Fig. 2, these renewed QBERs will sightly increase with the channel excess noise, and the high abundance of Alice's QBER will lead to low necessary reconciliation efficiency for the BE QKD protocol.

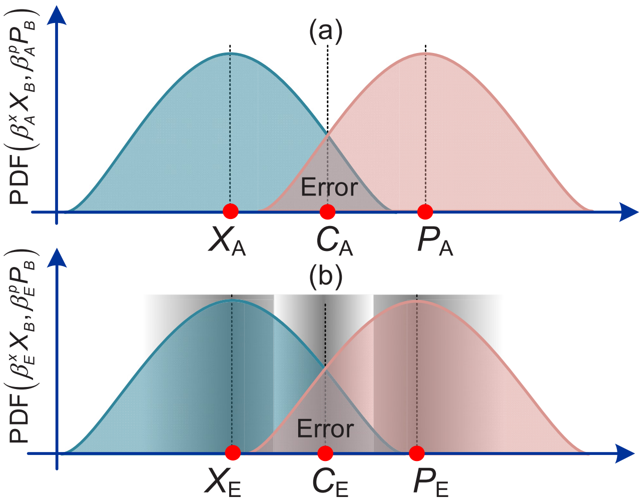
(a)
$\mathrm{PDF}\left(\beta^x_A X_B, \beta^p_A P_B\right)$
Error
X_A
C_A
P_A
(b)
$\mathrm{PDF}\left(\beta^x_E X_B, \beta^p_E P_B\right)$
Error
X_E
C_E
P_E

FIG. 3. Demonstration of the decoding rules for (a) Alice and (b) Eve employed in the proposed scheme.

According to Refs. [37,38], a lower bound of the mutual information I_{AB} is the Gaussian mutual information I^g_{AB} with the expression as

$$I^g_{AB} = 1 - H\left(P^{AB}_{e,f}\right). \tag{5}$$

The leaked information contains two parts with the form

$$I_{BE} = \mu I^{IR}_{BE} + (1-\mu) I^{BS,\varepsilon_c=0}_{BE}, \tag{6}$$

where I^{IR}_{BE} and $I^{BS,\varepsilon_c=0}_{BE}$ denote the leaked information for Eve's IR and BS attacks, respectively. Here V'_A denotes the modulation variance of the reproduced quantum signals after Eve's IR attack. The calculations of the secret key rate for GMCS CVQKD and the proposed scheme are given in Appendix B.

As the known CVQKD protocols, the foundational security of the basis-encoding (BE) QKD also relies on Heisenberg's uncertainty principle, which makes a restriction that the eavesdropper cannot obtain the precise values of the conjugate quadratures X and P of the transmitted quantum states simultaneously. In particular, we note here that the estimated QBER between Alice and Bob is from the deviations between Bob's measurement results X_B, P_B and Alice's encoding values X_A, P_A, whereas Eve's estimated QBER originates from the deviations between Bob's measurement results X_B, P_B and Eve's heterodyne measurement results X_E, P_E. However, Eve's heterodyne detection inevitably introduces extra shot noise, which deteriorates her decoding error rate. We show Alice's and Eve's decoding principles for the proposed BE QKD protocol in Fig. 3, which depicts the probability density functions of Alice's and Bob's adjustmental variables. It can be seen that Alice's decoding reference points X_A, P_A, C_A are known constant values, while Eve's reference points X_E, P_E, C_E themselves are Gaussian random variables, which will result in a much higher QBER for Eve even when the quantum channel is very lossy and noisy.

IV. THE SIMULATION PERFORMANCE

The numerical simulations of the secret key rates for the proposed scheme are displayed in Fig. 4. We note here the

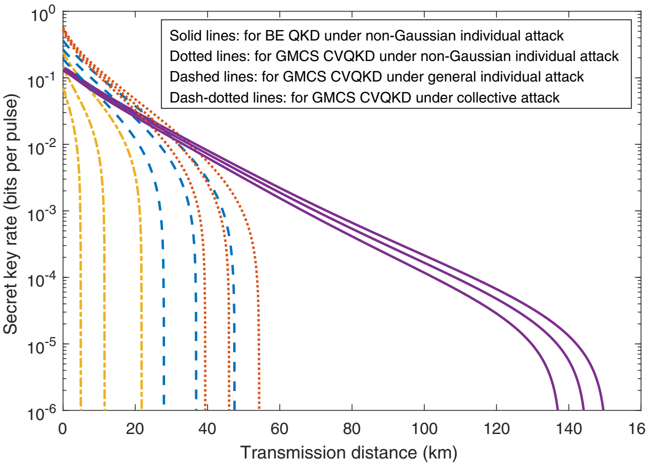

FIG. 4. Secret key rates via transmission distance for different channel excess noise ε_c in the finite-size scenario. From top to bottom, $\varepsilon_c = 0.1, 0.16, 0.22$.

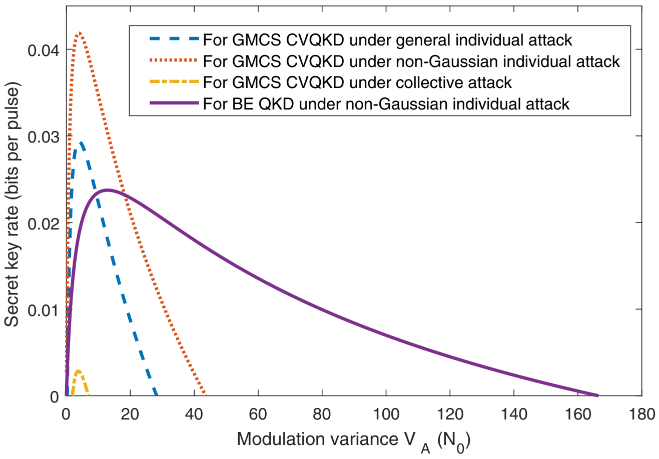

FIG. 6. Secret key rate as a function of modulation variance for the proposed BE QKD and GMCS CVQKD protocols under different attacks.

non-Gaussian individual attack involved in this paper is weaker than the general individual attack. For comparison, we plot the secret key rate of the GMCS CVQKD scheme under the same non-Gaussian individual, the general individual, and collective attacks in Fig. 4. The quantum channel is characterized by its transmission $T = 10^{-0.02d}$, where d is the distance between Alice and Bob. The block length is $N = 2 \times 10^{12}$, the modulation variance is $V_A = 10$, reconciliation efficiency is $\beta = 0.9$, $n/N = 0.5$, and the quantum efficiency and electronic noise of Bob's detection are $\eta = 0.6$ and $\nu_{el} = 0.02$, respectively. Clearly, the contrastive results show that the secure transmission distance for the BE QKD protocol has been dramatically promoted in the cases of relatively high-level channel excess noise, which benefits the practical large-scale secure quantum cryptography with continuous variables.

The tolerable excess noise and necessary reconciliation efficiency to guarantee a positive secret key rate for the proposed protocol are depicted in Fig. 5, where the reconciliation efficiency and channel excess noise are specified as $\beta = 0.9$ and $\varepsilon_c = 0.1$, respectively. The contrastive results show that the proposed protocol exhibits capabilities of much higher tolerable excess noise and much lower necessary reconciliation efficiency than the conventional GMCS CVQKD scheme, which enables the EB QKD protocol to reach a much longer secure transmission distance even at a lower reconciliation efficiency. So the proposed protocol may be more applicable in the scenarios of bad quantum channels and low-efficiency ECC.

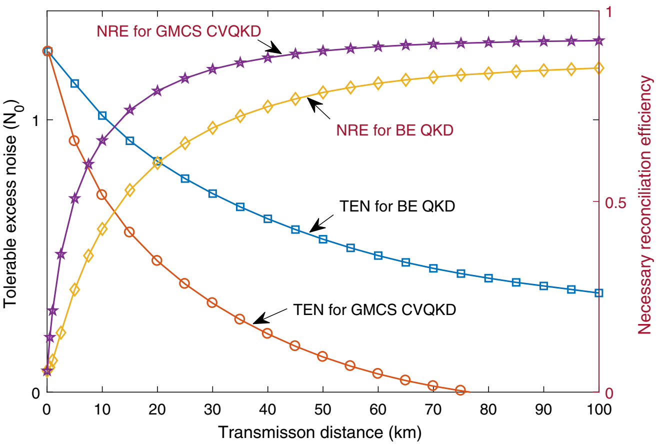

FIG. 5. Tolerable excess noise (TEN) and necessary reconciliation efficiency (NRE) as a function of transmission distance against the non-Gaussian individual attack for the proposed scheme and the GMCS CVQKD scheme.

Moreover, the secret key rate as a function of modulation variance V_A is depicted in Fig. 6, where the reconciliation efficiency, channel excess noise, and transmission distance are set as $\beta = 0.9$, $\varepsilon_c = 0.1$, and $d = 25$ km, respectively. We can find that the optimal modulation variance is larger than the known GMCS CVQKD scheme, and the relatively flat distribution allows us to achieve high performance with a more flexible choice of modulation variance, which quite eases the demand of the sensitivity of homodyne detection and is meaningful for practical high-speed implementation of quantum key distribution.

V. DISCUSSION AND CONCLUSIONS

The main differences between the proposed scheme and the DVQKD protocols are that Alice usually sends coherent states with a few photons per pulse (about five) and performs homodyne detection but not photon counting. Also, similar with the DM CVQKD schemes, the error rate is not upper bounded, which is in disagreement with the security proofs for DVQKD protocols which impose a maximum admissible QBER. It should be mentioned that the decoy states are necessary for the DM CVQKD protocols to guarantee the unconditional security [26], which makes the practical implementation of these protocols complicated. As shown in Fig. 7, the QBER of the proposed scheme can be a high value and close to 0.5 with the increase of reconciliation efficiency, which is induced by both the noise and losses of the quantum channel controlled by Eve, but the security is still ensured. Moreover, the main

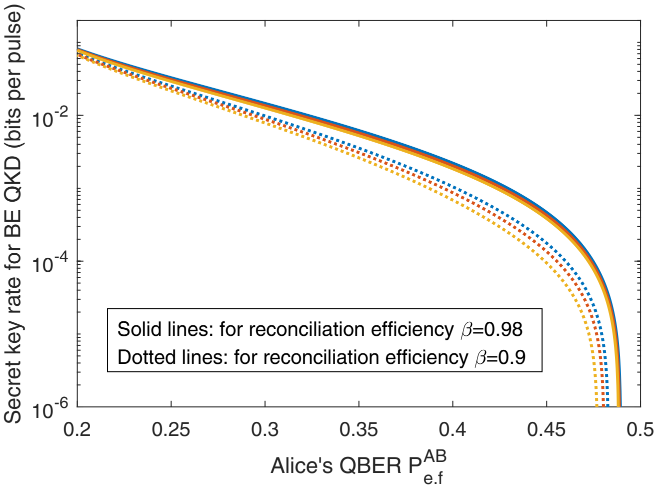

FIG. 7. The secret key rate of the proposed BE QKD under a non-Gaussian individual attack as a function of Alice's QBER $P_{e,f}^{AB}$ for different reconciliation efficiency and channel excess noise ε_c. From top to bottom, $\varepsilon_c = 0.1, 0.16, 0.22$.

difference between the proposed scheme and the DM CVQKD schemes [25] is that the latter ones belong to the type of VE CVQKD protocols, which are essentially sensitive to excess noise and reconciliation efficiency. Actually, Eve's information under collective attacks for the DM CVQKD schemes can be also bounded by the Holevo information, which has the same form as the one obtained for GMCS CVQKD schemes. However, the one for the proposed BE QKD protocol has not yet been tightly bounded.

We note that the secret key rate of the proposed protocol will be not superior to the GMCS CVQKD schemes in the scenarios of the short-distance quantum channel and high-efficiency ECC, shown in Fig. 8. This is because the channel capacity for key distribution between Alice and Bob and simultaneously the one between Bob and Eve are both initiatively decreased. With the quantum channel and ECC becoming better, the merits of the high capacity of Gaussian channels are notable, and, subsequently, a higher secret key rate can be achieved. We sacrifice the channel capacity to improve the tolerable excess noise and lower the necessary reconciliation efficiency. In addition, since the first three steps of the proposed protocol are the same as GMCS CVQKD scheme, one may integrate these two schemes in practice. Especially when the quantum channel is quite noisy and lossy, and the reconciliation efficiency is low under the current signal-to-noise ratio, one may choose to execute the proposed BE QKD scheme.

As summarized above, we present a QKD protocol based on the BE method, which we prove to be secure against a non-Gaussian individual attack. The contrastive analysis shows that the use of the BE method allows us to achieve direct distribution of discrete secret keys by using Gaussian-modulated coherent states over very noisy and lossy quantum channels even with low reconciliation efficiency, which was impossible for the previous CVQKD protocols. Moreover, the BE method can be naturally integrated with the previous GMCS CVQKD schemes to strengthen their performance for practical application scenarios. Further work will include analysis of the unconditional security, as well as the implementation of the present protocol.

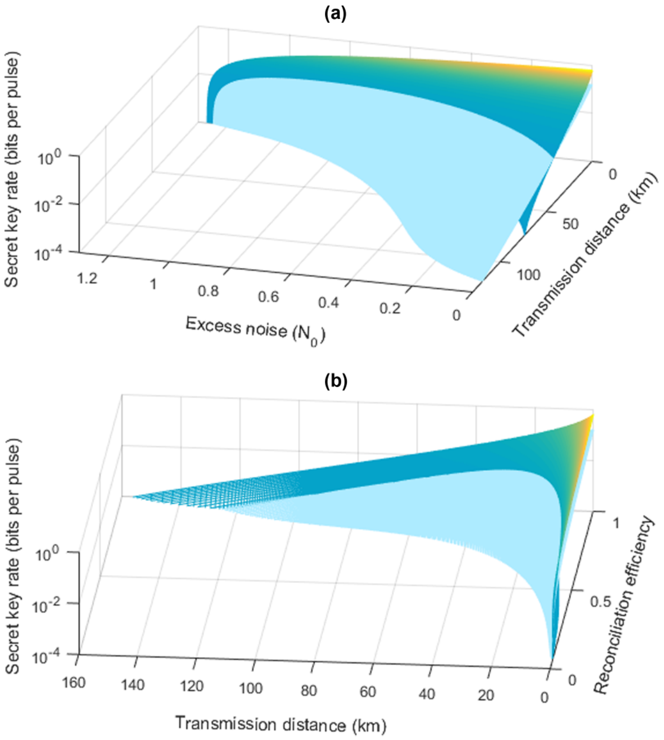

FIG. 8. Secret key rate as a function of (a) excess noise and transmission distance and (b) reconciliation efficiency and transmission distance. The light and dark blue surfaces denote the secret key rates for the proposed BE QKD scheme and the GMCS CVQKD scheme under the non-Gaussian individual attack, respectively.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China (Grants No. 61332019, 61671287, 61631014) and the National Key Research and Development Program (Grant No. 2016YFA0302600).

APPENDIX A: EVE'S INDIVIDUAL ATTACK

In the basis-encoding QKD protocol, Alice sends the Gaussian modulated signal through the lossy and noisy quantum channel to Bob. Here we consider the case that Eve performs a particular non-Gaussian individual attack which combines partial intercept-and-resend (IR) and beam-splitting (BS) attacks, and the channel excess noise ε_c is all introduced in the IR step. In particular, Eve intercepts and resends a fraction μ of the pulses, while she performs a standard BS attack on the remaining fraction $1 - \mu$ of the pulses. For the IR step, Eve performs a simultaneous measurement of both X and P quadratures of the coherent states sent by Alice (Fig. 9). Then she produces a new one displaced according to her measurement results and resends it to Bob. For the BS step, Eve will replace the quantum channel with a perfect lossless and noiseless quantum channel connecting with a beam splitter with transmission efficiency T, where the extra input of the beam splitter is a Gaussian vacuum state. Eve's BS attack can

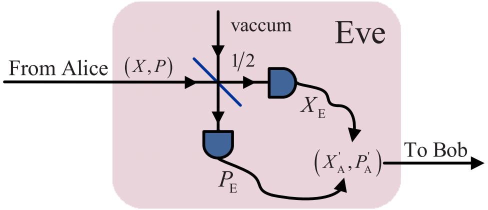

FIG. 9. The description of Eve's intercept-and-resend attack.

be depicted in Fig. 10, where $\hat{a}_1$ is the quantum signal and $\hat{a}_1^v$ is the input of vacuum state.

Suppose that the transmission efficiency is T, the channel excess noise is ε_c, and Bob uses homodyne detection with an efficiency η and electronics noise ν_{el}, then the quadratures of received Gaussian-modulated coherent states in Bob's station can be expressed as

$$\begin{aligned} X_B &= \sqrt{\eta T} X_A + \sqrt{\eta T}\delta X_{ex} + \delta X_v + \delta X_{el}, \\ P_B &= \sqrt{\eta T} P_A + \sqrt{\eta T}\delta P_{ex} + \delta P_v + \delta P_{el}, \end{aligned} \tag{A1}$$

where δX_{ex} (δP_{ex}), δX_v (δP_v), and δX_{el} (δP_{el}) are arising from channel excess noise, shot noise, and electronic noise of homodyne detection, respectively, and satisfy $\langle \delta X_{ex}^2\rangle = \langle \delta P_{ex}^2\rangle = \varepsilon$, $\langle \delta X_v^2\rangle = \langle \delta P_v^2\rangle = 1$, and $\langle \delta X_{el}^2\rangle = \langle \delta P_{el}^2\rangle = \nu_{el}$ in shot noise units, respectively. The variances of Bob's measurement results (the values of quadrature X or P obtained by Bob's homodyne detection) for the IR or BS case can be expressed in the shot-noise units as [37]

$$\begin{aligned} \langle y^2\rangle_{\text{IR}} &= \eta T(V_A + 2) + 1 + \nu_{el}, \\ \langle y^2\rangle_{\text{BS}} &= \eta T V_A + 1 + \nu_{el}. \end{aligned} \tag{A2}$$

The total excess noise introduced by this non-Gaussian individual attack should satisfy $2\mu = \varepsilon_c$.

We first consider the Eve's IR attack model. Eve intercepts the quantum signal from Alice and performs perfect heterodyne detection; then she will adjust the measurement results and obtain

$$\begin{aligned} X_E &= X_A + \delta X_0^v + \delta X_1^v, \\ P_E &= P_A + \delta P_0^v - \delta P_1^v, \end{aligned} \tag{A3}$$

where $\delta X_0^v(\delta P_0^v)$, $\delta X_1^v(\delta P_1^v)$ are the quadratures of the vacuum states induced in the encoding step and heterodyne detection, respectively. Then she will reproduce the quantum signal state and resend to Bob with the quadratures

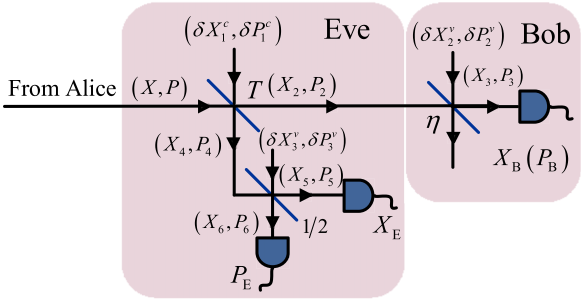

FIG. 10. The description of Eve's beam-splitting attack by using heterodyne detection.

$$\begin{aligned} X'_A &= X_A + \delta X_0^v + \delta X_1^v + \delta X_2^v, \\ P'_A &= P_A + \delta P_0^v - \delta P_1^v + \delta P_2^v, \end{aligned} \tag{A4}$$

where $\delta X_2^v(\delta P_2^v)$ is the quadrature of the vacuum state induced by the reproduction of the quantum signal state.

Now we consider the general BS attack model, where the extra input mode $\hat{a}_1^c$ of the beam splitter is a thermal state. The quadratures of the output modes $\hat{a}_2$ and $\hat{a}_4$ can be expressed as

$$\begin{aligned} X_2 &= \sqrt{T} X_A + \sqrt{T}\delta X_0^v + \sqrt{1-T}\delta X_1^v + \sqrt{T}\delta X_{ex}, \\ P_2 &= \sqrt{T} P_A + \sqrt{T}\delta P_0^v + \sqrt{1-T}\delta P_1^v + \sqrt{T}\delta P_{ex}, \\ X_4 &= -\sqrt{1-T} X_A - \sqrt{1-T}\delta X_0^v + \sqrt{T}\delta X_1^v \\ &\quad + \frac{T}{\sqrt{1-T}}\delta X_{ex}, \\ P_4 &= -\sqrt{1-T} P_A - \sqrt{1-T}\delta P_0^v + \sqrt{T}\delta P_1^v \\ &\quad + \frac{T}{\sqrt{1-T}}\delta P_{ex}, \end{aligned} \tag{A5}$$

where $\delta X_0^v(\delta P_0^v)$, $\delta X_1^v(\delta P_1^v)$ are the quadratures of the vacuum states induced in the encoding step and lossy channel, respectively, and $\delta X_{ex} = \sqrt{\frac{1-T}{T}}\delta X_{ex}^c$ $(\delta P_{ex} = \sqrt{\frac{1-T}{T}}\delta P_{ex}^c)$ is the quadrature induced by noisy quantum channel referred to the channel input and $\delta X_1^c = \delta X_1^v + \delta X_{ex}^c$ $(\delta P_1^c = \delta P_1^v + \delta P_{ex}^c)$. For a standard BS attack, $\delta X_{ex} = \delta P_{ex} = 0$:

$$\begin{aligned} X_B &= X_3 = \sqrt{\eta T} X_A + \sqrt{\eta T}\delta X_{ex} + \delta X_B + \delta X_{el}, \\ P_B &= P_3 = \sqrt{\eta T} P_A + \sqrt{\eta T}\delta P_{ex} + \delta P_B + \delta P_{el}, \\ X_E &= -X_5 = \sqrt{\frac{1-T}{2}} X_A + \delta X_E - \frac{T}{\sqrt{2(1-T)}}\delta X_{ex}, \\ P_E &= P_6 = \sqrt{\frac{1-T}{2}} P_A + \delta P_E - \frac{T}{\sqrt{2(1-T)}}\delta P_{ex}, \end{aligned} \tag{A6}$$

where $\delta X_B = \delta X_v = \sqrt{\eta T}\delta X_0^v + \sqrt{\eta(1-T)}\delta X_1^v + \sqrt{1-\eta}\delta X_2^v$, $\delta P_B = \delta P_v = \sqrt{\eta T}\delta P_0^v + \sqrt{\eta(1-T)}\delta P_1^v + \sqrt{1-\eta}\delta P_2^v$, $\delta X_E = \sqrt{\frac{1-T}{2}}\delta X_0^v - \sqrt{\frac{T}{2}}\delta X_1^v - \sqrt{\frac{1}{2}}\delta X_3^v$, and $\delta P_E = \sqrt{\frac{1-T}{2}}\delta P_0^v - \sqrt{\frac{T}{2}}\delta P_1^v + \sqrt{\frac{1}{2}}\delta P_3^v$. Here $X_2^v(P_2^v)$ and $X_{el}(P_{el})$ are the quadratures of the vacuum state induced in the imperfect homodyne detection and the quadrature induced by the noisy homodyne detection referred to the channel input, respectively.

In the following, we will first calculate the QBER of Alice's and Eve's decoding according to Bob's measurement results for a BS attack in the asymptotic regime. First, we consider the QBER between Alice and Bob. Because of the symmetry of quadratures X_A and P_A, we just consider the case of $X_A > P_A$ for simplicity. According to Eqs. (A1) and (A6), the inequality $\beta_A^x X_B < C_A$ and $\beta_A^p P_B > C_A$ can be expanded to

$$\begin{aligned} X_A - P_A &< -2\delta X_{ex} - \frac{2}{\sqrt{\eta T}}(\delta X_v + \delta X_{el}), \\ X_A - P_A &< 2\delta P_{ex} + \frac{2}{\sqrt{\eta T}}(\delta P_v + \delta P_{el}). \end{aligned} \tag{A7}$$

When we set $M = X_A - P_A, N_1^x = -2\delta X_{ex} - \frac{2}{\sqrt{\eta T}}(\delta X_v + \delta X_{el})$, and $N_1^p = 2\delta P_{ex} + \frac{2}{\sqrt{\eta T}}(\delta P_v + \delta P_{el})$, these variables follow the normal distributions as

$$M \sim \mathcal{N}(0,\sigma_m^2), \quad N_1^x, \quad N_1^p \sim \mathcal{N}(0,\sigma_{n_1}^2), \tag{A8}$$

where $\sigma_m^2 = 2V_A$ and $\sigma_{n_1}^2 = 4\varepsilon_c + \frac{4}{\eta T}(1 + \nu_{el})$. The QBER between Alice and Bob can be calculated as

$$\begin{aligned} P_e^{AB} &= \frac{1}{2}\big[P\big(M < N_1^x \big| M > 0\big) + P\big(M < N_1^p \big| M > 0\big)\big] \\ &= \frac{1}{2}\big[P\big(0 < M < N_1^x\big)/P(M > 0) \\ &\quad + P\big(0 < M < N_1^p\big)/P(M > 0)\big] \\ &= P\big(0 < M < N_1^x\big) + P\big(0 < M < N_1^p\big) \\ &= \iint\limits_{0<m<n_1^x} \frac{e^{-\frac{m^2}{2\sigma_m^2} - \frac{(n_1^x)^2}{2\sigma_{n_1}^2}}}{2\pi\sigma_m\sigma_{n_1}}\, dm\, dn_1^x \\ &\quad + \iint\limits_{0<m<n_1^p} \frac{e^{-\frac{m^2}{2\sigma_m^2} - \frac{(n_1^p)^2}{2\sigma_{n_1}^2}}}{2\pi\sigma_m\sigma_{n_1}}\, dm\, dn_1^p \\ &= \frac{1}{2\pi\sigma_{n_1}\sigma_m}\int_{n_1^x}^{0} e^{-\frac{m^2}{2\sigma_m^2}}\, dm \int_{-\infty}^{0} e^{-\frac{(n_1^x)^2}{2\sigma_{n_1}^2}}\, dn_1^x \\ &\quad + \frac{1}{2\pi\sigma_{n_1}\sigma_m}\int_{n_1^p}^{0} e^{-\frac{m^2}{2\sigma_m^2}}\, dm \int_{-\infty}^{0} e^{-\frac{(n_1^p)^2}{2\sigma_{n_1}^2}}\, dn_1^p \\ &= \int_0^{+\infty} \frac{1}{\sqrt{2\pi}\sigma_{n_1}} \mathrm{erf}\left[\frac{n}{\sqrt{2}\sigma_m}\right] e^{-\frac{n^2}{2\sigma_{n_1}^2}}\, dn \\ &= \arctan\left(\frac{\sigma_{n_1}}{\sigma_m}\right)/\pi, \end{aligned} \tag{A9}$$

where $\mathrm{erf}(x) = \int_0^x e^{-t^2}\, dt$ is the error function.

Now we calculate the QBER between Bob and Eve. After receiving Bob's measurement results, Eve will decoding her data from heterodyne detection. From Eq. (A6), we can see the quadratures X_E and P_E are symmetric. Also, we can just consider the case of $X_E > P_E$ for simplicity, which can be expanded to

$$M > N_2, \tag{A10}$$

where $N_2 = \sqrt{\frac{2}{1-T}}(\delta P_E - \delta X_E) + \frac{T}{1-T}(\delta X_{ex} - \delta P_{ex})$, which follows the distribution

$$N_2 \sim \mathcal{N}(0,\sigma_{n_2}^2), \tag{A11}$$

where $\sigma_{n_2}^2 = \frac{4}{1-T} + 2(\frac{T}{1-T})^2\varepsilon_c$.

According to Eq. (A6), the inequality $\beta_E^x X_B < C_E$ and $\beta_E^p P_B > C_E$ can be expanded to

$$M < N_3^x, \quad M < N_3^p, \tag{A12}$$

where $N_3^x = \sqrt{\frac{2}{1-T}}(\delta P_E + \delta X_E) - \frac{2}{\sqrt{\eta T}}(\delta X_B + \delta X_{el}) - \frac{2-T}{1-T}\delta X_{ex} - \frac{T}{1-T}\delta P_{ex}$, and $N_3^p = -\sqrt{\frac{2}{1-T}}(\delta P_E + \delta X_E) + \frac{2}{\sqrt{\eta T}}(\delta P_B + \delta P_{el}) + \frac{2-T}{1-T}\delta P_{ex} + \frac{T}{1-T}\delta X_{ex}$, which can be further simplified by replacing the variables δX_E, δP_E, δX_B, and δP_B. Then we can get their distributions as

$$N_3^x, N_3^p \sim \mathcal{N}(0,\sigma_{n_3}^2), \tag{A13}$$

where $\sigma_{n_3}^2 = \frac{T^2+(2-T)^2}{(1-T)^2}\varepsilon_c + \frac{4}{\eta T}\nu_{el} + \frac{4-T}{1-T} + (2\sqrt{\frac{1-T}{T}} + \sqrt{\frac{T}{1-T}})^2 + \frac{4(1-\eta)}{\eta T}$. The QBER between Bob and Eve can be calculated as

$$\begin{aligned} P_e^{BE} &= \frac{1}{2}\big[P\big(M < N_3^x \big| M > N_2\big) \\ &\quad + P\big(M < N_3^p \big| M > N_2\big)\big] \\ &= \frac{1}{2}\big[P\big(N_2 < M < N_3^x\big)/P(M > N_2) \\ &\quad + P\big(N_2 < M < N_3^p\big)/P(M > N_2)\big] \\ &= P\big(N_2 < M < N_3^x\big) + P\big(N_2 < M < N_3^p\big) \\ &= \iiint\limits_{n_2<m<n_3^x} \frac{e^{-\frac{m^2}{2\sigma_m^2} - \frac{n_2^2}{2\sigma_{n_2}^2} - \frac{(n_3^x)^2}{2\sigma_{n_3}^2}}}{2\pi\sqrt{2\pi}\sigma_m\sigma_{n_2}\sigma_{n_3}}\, dm\, dn_2\, dn_3^x \\ &\quad + \iiint\limits_{n_2<m<n_3^p} \frac{e^{-\frac{m^2}{2\sigma_m^2} - \frac{n_2^2}{2\sigma_{n_2}^2} - \frac{(n_3^p)^2}{2\sigma_{n_3}^2}}}{2\pi\sqrt{2\pi}\sigma_m\sigma_{n_2}\sigma_{n_3}}\, dm\, dn_2\, dn_3^p \\ &= 2\int_{-\infty}^{+\infty} \frac{e^{-\frac{m^2}{2\sigma_m^2}}}{\pi\sqrt{2\pi}\sigma_m}\left[\frac{\sqrt{\pi}}{2} + \frac{\sqrt{\pi}}{2}\mathrm{erf}\left(\frac{m}{\sqrt{2}\sigma_{n_2}}\right)\right] \\ &\quad \times \left[\frac{\sqrt{\pi}}{2} - \frac{\sqrt{\pi}}{2}\mathrm{erf}\left(\frac{m}{\sqrt{2}\sigma_{n_3}}\right)\right] dm \\ &= 1 - \int_{-\infty}^{+\infty} \frac{e^{-\frac{m^2}{2\sigma_m^2}}}{2\sqrt{2\pi}\sigma_m}\mathrm{erfc}\left(\frac{m}{\sqrt{2}\sigma_{n_2}}\right)\mathrm{erfc}\left(\frac{m}{\sqrt{2}\sigma_{n_3}}\right) dm \\ &= 1 - F_e, \end{aligned} \tag{A14}$$

where $F_e = \int_{-\infty}^{+\infty} \frac{e^{-\frac{m^2}{2\sigma_m^2}}}{2\sqrt{2\pi}\sigma_m}\mathrm{erfc}(\frac{m}{\sqrt{2}\sigma_{n_2}})\mathrm{erfc}(\frac{m}{\sqrt{2}\sigma_{n_3}})\, dm$, which is an integrable function with a numerical solution. The simplification of Eq. (A14) is obtained by using the following result:

$$\begin{aligned} &P(M > N_2) \\ &= \iint\limits_{m<n_2} \frac{e^{-\frac{m^2}{2\sigma_m^2} - \frac{n_2^2}{2\sigma_{n_2}^2}}}{2\pi\sigma_m\sigma_{n_2}}\, dm\, dn_2 \\ &= \int_{-\infty}^{+\infty} \frac{e^{-\frac{m^2}{2\sigma_m^2}}}{\sqrt{2\pi}\sigma_m}\left[\frac{\sqrt{\pi}}{2}\mathrm{erfc}\left(\frac{m}{\sqrt{2}\sigma_{n_2}}\right) + \frac{\sqrt{\pi}}{2}\right] dm \\ &= \frac{1}{2}, \end{aligned} \tag{A15}$$

where we use the equation

$$\begin{aligned}\int_{-\infty}^{m} e^{-\frac{n_2^2}{2\sigma_{n_2}^2}}\,dn_2 &= \sqrt{2}\sigma_{n_2}\int_{-\infty}^{\frac{m}{\sqrt{2}\sigma_{n_2}}} e^{-t^2}\,dt\\ &= \sqrt{2}\sigma_{n_2}\left(\int_{0}^{\frac{m}{\sqrt{2}\sigma_{n_2}}} e^{-t^2}\,dt + \int_{-\infty}^{0} e^{-t^2}\,dt\right)\\ &= \sqrt{\frac{\pi}{2}}\sigma_{n_2}\mathrm{erf}\left(\frac{m}{\sqrt{2}\sigma_{n_2}}\right) + \sqrt{\frac{\pi}{2}}\sigma_{n_2}. \qquad \text{(A16)}\end{aligned}$$

Now we consider the QBERs in the finite-size scenario. When considering finite-size effect, the transmission efficiency T and the channel excess noise ε_c in Eqs. (A9) and (A14) should be renewed as [24]

$$\begin{aligned}T' &= \left[\sqrt{T} - z_{\varepsilon_{PE}/2}\sqrt{\frac{1+T\varepsilon_c}{(N-n)V_A}}\right]^2\\ \varepsilon_c' &= \left[T\varepsilon_c + z_{\epsilon_{PE}/2}(1+T\varepsilon_c)\sqrt{\frac{2}{N-n}}\right]\Big/T', \qquad \text{(A17)}\end{aligned}$$

where $z_{\epsilon_{PE}/2}$ is such that $1-\mathrm{erf}(z_{\epsilon_{PE}/2}/\sqrt{2})/2 = \epsilon_{PE}/2$, ϵ_{PE} quantifies the failure probability of the parameter estimation. Moreover, n is the number of the pulses used for key generation, and N is the block size of the shared data between Alice and Bob. We denote the renewed Alice's and Eve's QBERs in the finite-size scenarios as $P_{e,f}^{AB}$ and $P_{e,f}^{BE}$, respectively.

APPENDIX B: CALCULATION OF SECRET KEY RATE FOR DIFFERENT CVQKD PROTOCOLS

The secret key rate in finite-size scenario can be obtained as

$$R = \frac{n}{N}[\beta I_{AB} - I_E - \Delta(n)], \qquad \text{(B1)}$$

where $\Delta(n) = 7\sqrt{\frac{\log_2(2/\epsilon_s)}{n}}$ is related to the security of the privacy amplification, and ϵ_s is the smooth parameter. The particular non-Gaussian individual attack includes intercept-resend and BS parts, and the actual secret key rate of the proposed QKD scheme under this attack can be calculated in two parts. However, the achievable secret key rate can be lower bounded by the information rate for an equivalent Gaussian attack characterized by the same evaluated parameters [37,38]. Here the mutual information between Alice and Bob I_{AB} is bounded by the Gaussian mutual information I_{AB}^{g} with the expression as

$$I_{AB}^{g} = 1 - H\big(P_{e,f}^{AB}\big), \qquad \text{(B2)}$$

which is lower than the actual mutual information I_{AB}^{ng} with the expression as

$$I_{AB}^{ng} = \mu I_{AB}^{BS,\varepsilon_c=0} + (1-\mu)I_{AB}^{BS,\varepsilon_c=2}, \qquad \text{(B3)}$$

where $\mu = \varepsilon_c'/2$, $I_{AB}^{BS,\varepsilon_c=0} = 1 - H[P_e^{AB}(\varepsilon_c=0)]$, and $I_{AB}^{BS,\varepsilon_c=2} = 1 - H[P_e^{AB}(\varepsilon_c=2)]$. We use $I_{AB} = I_{AB}^{g}$ to calculate the secret key rate in this paper. The leaked information can be calculated as $I_E = I_{BE}$ for reverse reconciliation, which can be expressed as

$$I_{BE} = \mu I_{BE}^{IR} + (1-\mu)I_{BE}^{BS,\varepsilon_c=0}, \qquad \text{(B4)}$$

where $I_{BE}^{IR} = 1 - H[P_{e,f}^{AB}(\varepsilon_c = 0, V_A' = V_A + 2)]$ and $I_{BE}^{BS,\varepsilon_c=0} = 1 - H[P_{e,f}^{BE}(\varepsilon_c=0)]$. Here V_A' denotes the modulation variance of the reproduced quantum signal states after Eve's IR attack.

For the GMCS CVQKD protocol, the secret key rate for the reverse reconciliation scheme under the general individual attack in a finite-size scenario also can be calculated with Eq. (B1), where I_{AB} and I_E can be calculated as [35,37]

$$\begin{aligned}I_{AB} &= \frac{1}{2}\log_2\frac{\eta T' V_A + 1 + \eta T'\varepsilon_c' + \nu_{el}}{1 + \eta\varepsilon_c' + \nu_{el}},\\ I_E &= \frac{1}{2}\log_2\frac{\eta T' V_A + 1 + \eta T'\varepsilon_c' + \nu_{el}}{\eta/\left[1 - T' + T'\varepsilon_c' + \frac{T'}{V_A+1}\right] + 1 - \eta + \nu_{el}}.\end{aligned} \qquad \text{(B5)}$$

For the particular non-Gaussian individual attack, the leaked information to Eve can be evaluated by form of Eq. (B4), where I_{BE}^{IR} and $I_{BE}^{BS,\varepsilon_c=0}$ should be renewed according to Eq. (B5) as $I_{BE}^{IR} = I_{AB}(\varepsilon_c = 0, V_A' = V_A + 2)$ and $I_{BE}^{BS,\varepsilon_c=0} = I_E(\varepsilon_c = 0)$.

Also, the secret key rate under collective attack in the finite-size scenario can be calculated as Eq. (B1), where I_{AB} has the same expression as the one in Eq. (B5) and I_E should be renewed as χ_{BE} with the expression [24,35]

$$\chi_{BE} = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\lambda_i - 1}{2}\right), \qquad \text{(B6)}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$. The symplectic eigenvalues λ_i are given by

$$\begin{aligned}\lambda_{1,2}^2 &= \frac{1}{2}(A \pm \sqrt{A^2 - 4B}),\\ \lambda_{3,4}^2 &= \frac{1}{2}(C \pm \sqrt{C^2 - 4D}), \qquad \text{(B7)}\\ \lambda_5 &= 1,\end{aligned}$$

where $A = V^2(1-2T') + 2T' + T'^2(V + \chi_{\mathrm{line}}')^2$, $B = T'^2(V\chi_{\mathrm{line}}' + 1)^2$, $C = \frac{V\sqrt{B} + T'(V + \chi_{\mathrm{line}}') + A\chi_{\mathrm{hom}}}{T'(V + \chi_{\mathrm{tot}}')}$, and $D = \sqrt{B}\frac{V + \sqrt{B}\chi_{\mathrm{hom}}}{T'(V + \chi_{\mathrm{tot}}')}$ with $V = V_A + 1$, $\chi_{\mathrm{line}}' = 1/T' - 1 + \varepsilon_c'$, $\chi_{\mathrm{hom}} = (1 + \nu_{el})/\eta - 1$, and $\chi_{\mathrm{tot}}' = \chi_{\mathrm{line}}' + \chi_{\mathrm{hom}}/T'$.

[1] C. H. Bennett and G. Brassard, *Proceedings of IEEE International Conference Computers, System and Signal Processing* (IEEE, New York, 1984), pp. 175–179.

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[3] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).

[4] F. Grosshan, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).

[5] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).

[6] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **95**, 180503 (2005).

[7] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).

[8] N. Lütkenhaus, Phys. Rev. A **54**, 97 (1996).

[9] B. A. Slutsky, R. Rao, P.-C. Sun, and Y. Fainman, Phys. Rev. A **57**, 2383 (1998).

[10] H. Bechmann-Pasquinucci, Phys. Rev. A **73**, 044305 (2006).

[11] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Quantum Inf. Comput. **3**, 535 (2003).

[12] E. Biham and T. Mor, Phys. Rev. Lett. **78**, 2256 (1997).

[13] E. Biham, M. Boyer, G. Brassard, J. van de Graaf, and T. Mor, Algorithmica **34**, 372 (2002).

[14] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).

[15] M. Navascués, F. Grosshans, and A. Acín, Phys. Rev. Lett. **97**, 190502 (2006).

[16] B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005).

[17] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).

[18] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).

[19] V. Scarani and R. Renner, Phys. Rev. Lett. **100**, 200501 (2008).

[20] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, Phys. Rev. Lett. **110**, 030502 (2013).

[21] A. Leverrier, Phys. Rev. Lett. **118**, 200501 (2017).

[22] R. Kumar, H. Qin, and R. Alléaume, New J. Phys. **17**, 043027 (2015).

[23] Y. Shen, X. Peng, J. Yang, and H. Guo, Phys. Rev. A **83**, 052304 (2011).

[24] A. Leverrier, F. Grosshans, and P. Grangier, Phys. Rev. A **81**, 062343 (2010).

[25] A. Leverrier and P. Grangier, Phys. Rev. Lett. **102**, 180504 (2009).

[26] A. Leverrier and P. Grangier, Phys. Rev. A **83**, 042312 (2011).

[27] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Photonics **7**, 378 (2013).

[28] D. Huang, P. Huang, D. Lin, and G. Zeng, Sci. Rep. **6**, 19201 (2016).

[29] D. Huang, D. Lin, P. Huang, and G. Zeng, Opt. Lett. **40**, 3695 (2015).

[30] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, Phys. Rev. X **5**, 041009 (2015).

[31] D. B. S. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, Phys. Rev. X **5**, 041010 (2015).

[32] A. Marie and R. Alléaume, Phys. Rev. A **95**, 012316 (2017).

[33] D. Huang, P. Huang, H. Li, T. Wang, Y. M. Zhou, and G. H. Zeng, Opt. Lett. **41**, 3511 (2016).

[34] S. J. Johnson, A. M. Lance, L. Ong, M. Shirvanimoghaddam, T. C. Ralph, and T. Symul, New J. Phys. **19**, 023003 (2017).

[35] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, Phys. Rev. A **76**, 042305 (2007).

[36] J. Martinez-Mateo, D. Elkouss, and V. Martin, Sci. Rep. **3**, 1576 (2013).

[37] J. Lodewyck, T. Debuisschert, R. García-Patrón, R. Tualle-Brouri, N. J. Cerf, and P. Grangier, Phys. Rev. Lett. **98**, 030503 (2007).

[38] F. Grosshans and N. J. Cerf, Phys. Rev. Lett. **92**, 047905 (2004).