Non-Gaussian Reconciliation for Continuous-Variable Quantum Key Distribution

Xiangyu Wang,[1,*] Menghao Xu,[1] Yin Zhao,[1] Ziyang Chen,[2,†] Song Yu,[1] and Hong Guo[2]

[1] *State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China*

[2] *State Key Laboratory of Advanced Optical Communication Systems and Networks, School of Electronics and Center for Quantum Information Technology, Peking University, Beijing 100871, China*

(Received 20 October 2022; revised 9 February 2023; accepted 14 April 2023; published 25 May 2023)

Non-Gaussian modulation can improve the performance of continuous-variable quantum key distribution (CV QKD). For Gaussian-modulated coherent-state CV QKD, photon subtraction can realize non-Gaussian modulation, which can be equivalently implemented by non-Gaussian postselection. However, non-Gaussian reconciliation has not been deeply researched, which is one of the key technologies in CV QKD. In this paper, we propose a non-Gaussian reconciliation method to obtain identical keys from non-Gaussian data. Multidimensional reconciliation and multiedge-type low-density parity-check codes (MET LDPC) are used in a non-Gaussian reconciliation scheme, where the layered belief propagation decoding algorithm of MET LDPC codes is used to reduce the decoding complexity. Furthermore, we compare the error-correction performance of Gaussian data and non-Gaussian data. The results show that the error-correction performance of non-Gaussian data is better than Gaussian data, where the frame error rate can be reduced by 50 % for code rate 0.1 at SNR of 0.1554 and the average iteration number can be reduced by 25 %.

DOI: 10.1103/PhysRevApplied.19.054084

I. INTRODUCTION

Secure communication needs secret keys. However, the classical key-generation algorithm based on computational complexity is seriously threatened by a quantum computer and alternative mathematical algorithm. In order to solve this problem, scholars have proposed quantum key distribution (QKD) protocols based on the basic principles of quantum physics, which is one of the most mature quantum information technology [1–3]. QKD allows two separate parties (Alice and Bob) to establish unconditional secure keys through an unsecure quantum channel, which may be controlled by potential eavesdroppers (Eve). According to the encoding dimension of quantum states, QKD is divided into two branches, discrete-variable (DV) QKD [4,5] and continuous-variable (CV) QKD [6–9]. These two kinds of protocols both have unconditional security [10–13], in which Gaussian-modulated coherent states CV QKD protocols have the advantages of being compatible with classical coherent optical communication technology [14,15]. However, due to the imperfection of the practical system devices and the reconciliation efficiency of postprocessing, the transmission distance of CV QKD system is limited [16–18]. Therefore, improving the secret key rate at a given distance [19,20] and extending the transmission distance of the system are two significant development trends in the field of CV QKD [9,21,22].

Recently, CV QKD has made great progress in theory [23–25] and experiment [26,27]. The transmission distance has been significantly improved due to the optimization of experiment setups and the improvement of reconciliation efficiency [21,28]. Some alternative protocols have been proposed to improve the performance of CV QKD systems, such as the noiseless linear amplification [29] and photon subtraction [30,31]. These two quantum operations can extend the transmission distance. However, due to the imperfection of actual devices and other factors, it is difficult to implement in a physical system. Thus, it is hard to achieve the ideal effect. To solve these problems, some postselection protocols are proposed. Through Gaussian postselection, virtual noiseless linear amplification can be realized [32], it has been demonstrated experimentally [33]. The physical realization of photon subtraction operation requires an ideal single-photon detector. Therefore, the implementation cost will be increased, the effect will be reduced due to the imperfection of the actual devices. Non-Gaussian postselection is proposed to implement virtual photon subtraction, which avoids the use of single-photon detector and complex physical operation [34]. The raw data after Gaussian postselection is still following Gaussian distribution, while for the virtual photon subtraction

[*] xywang@bupt.edu.cn

[†] chenziyang@pku.edu.cn

inside Alice the raw data of Alice after non-Gaussian postselection is no longer following Gaussian distribution.

The postselection algorithm can realize virtual physical operation, which greatly reduces the implementation complexity. However, the corresponding classical postprocessing part has not been deeply studied. There are still errors between Alice's and Bob's raw data after postselection. Therefore, it is necessary to correct the errors by using channel coding and decoding technology to obtain consistent keys. The raw data are continuous variables in CV QKD. Therefore, it needs to be transformed into binary data that can be encoded through mapping transformation firstly. Generally, there are mainly two methods, slice reconciliation [35] and multidimensional reconciliation [36]. The former is usually used in the case of high SNR, while the latter is used in the case of low SNR. The common error-correction codes used in CV QKD are Raptor codes [37], Polar codes [38], and low-density parity-check codes (LDPC) [39] etc. Multiedge-type (MET) LDPC codes can achieve good error-correction performance under extremely low SNRs.

In this paper, we mainly focus on the non-Gaussian reconciliation in CV QKD. The raw data after photon subtraction no longer follow Gaussian distribution, the distribution varies with the number of photon subtraction. Firstly, we give the method that realizes the transformation from Gaussian distribution data to non-Gaussian data through the postselection filter function. This process is fundamental, since it affects the amount of raw data saved after non-Gaussian postselection, and it has a considerable impact on the secret key rate of the CV QKD system. Multidimensional reconciliation and MET LDPC codes are used for the non-Gaussian reconciliation in the reverse reconciliation system. We introduce a layered belief propagation decoding algorithm [40] into non-Gaussian data error correction, which greatly reduces the complexity of the postprocessing decoding process and does not increase the frame error rate (FER) of decoding. Furthermore, we test the error-correction performance of the non-Gaussian reconciliation. Although the noise and Bob's raw data still obey Gaussian distribution, Alice's data converge to medium amplitude after non-Gaussian postselection, so the antinoise performance of the system is improved. It can be seen from the results that the FER of non-Gaussian data error correction is obviously lower than that of Gaussian data under the same conditions, the average number of iterations is also significantly reduced by using layered decoding algorithm.

The rest of the paper is organized as follows. In Sec. II, we introduce some basics of the non-Gaussian postselection, information reconciliation of CV QKD, presenting a postselection method to convert Gaussian distribution data to non-Gaussian distribution data, proposing the non-Gaussian reconciliation algorithm based on multidimensional reconciliation and MET LDPC codes. In Sec. III, we present the data distribution under different virtual photon subtraction numbers, the performance tests of information reconciliation on the non-Gaussian data after postselection under different virtual photon subtraction numbers, and the error-correction performance comparation with Gaussian data. In Sec. IV, we draw the conclusion of this paper.

II. NON-GAUSSIAN RECONCILIATION IN CV QKD

Non-Gaussian operation can increase the entanglement of the Gaussian entangled states. As a non-Gaussian operation, it has been proposed that photon subtraction in CV QKD can increase the transmission distance. It has been proved that the entanglement-based scheme and the corresponding prepare-and-measure scheme is secure [31]. Simultaneously, the feasibility and security of virtual photon subtraction scheme through non-Gaussian postselection have also been proved [34]. In this section, we first introduce the basic of the non-Gaussian postselection, then propose the postselection method to convert Gaussian distribution data to non-Gaussian distribution data, finally we present the non-Gaussian reconciliation scheme based on multidimensional reconciliation and MET LDPC codes.

A. Non-Gaussian postselection in CV QKD

The security of an entanglement-based model CV QKD photon subtraction protocol has been proved, the security of the corresponding prepare-and-measure (PM) model with equivalent postselection as virtual photon subtraction has also been proved [34]. Different from the Gaussian quantum state protocol, the non-Gaussian quantum state protocol cannot have a symplectic covariance matrix, so we cannot use von Neumann entropy to derive the Holevo boundary for secret key rate directly. However, we can estimate the secret key rate through the physical model equivalent to virtual photon subtraction. This equivalent physical model has been completed in our previous work [34]. The main idea is based on the optimality of Gaussian attacks [10,41,42]. The eavesdropper will not get more information from the non-Gaussian quantum state than the Gaussian quantum state, so the secret key rate of the non-Gaussian protocol is less than that of the corresponding Gaussian protocol. To ensure unconditional security, we can use the secret key rate of the corresponding Gaussian protocol as the lower bound of the secret key rate of the non-Gaussian protocol. In addition, the probability of photon subtraction success should also be considered when estimating the secret key rate of non-Gaussian protocol.

Most of the implementation of CV QKD is based on the PM scheme, which does not need to prepare entangled states, so it is easy to implement in experiment. The PM scheme of CV QKD with non-Gaussian postselection in Alice is shown in Fig. 1.

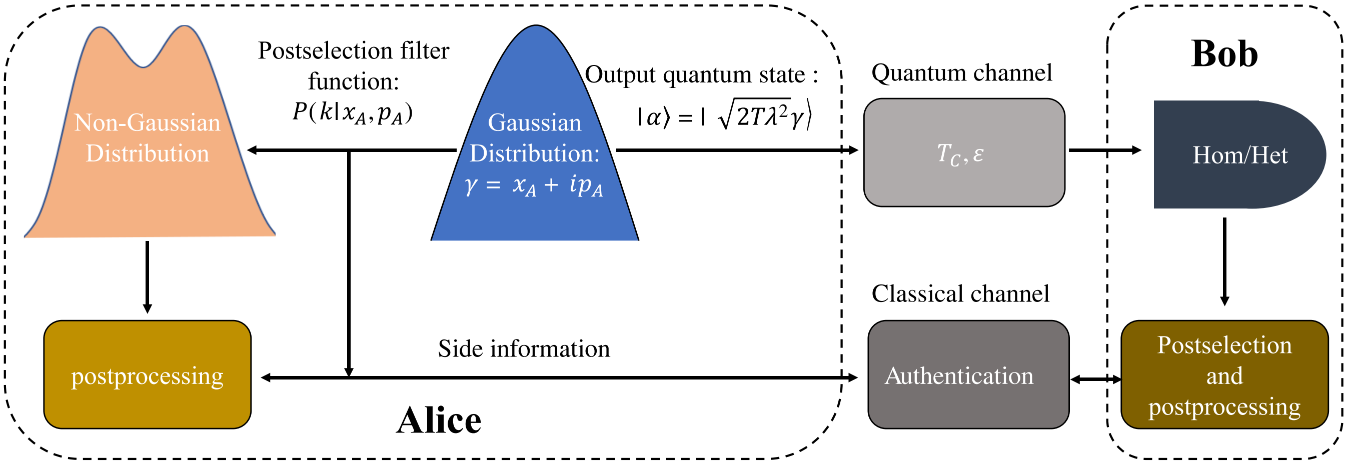

FIG. 1. The PM scheme of CV QKD with non-Gaussian postselection in Alice. $P(k|x_A, p_A)$ is the postselection filter function. γ are Alice's raw data. $|\alpha\rangle$ is output quantum state. T_C is the transmittance of quantum channel. ϵ is excess noise. Hom, homodyne detection; Het, heterodyne detection. The side information transmitted from the classical authentication channel includes the selection results of Alice in the postselection process and the information used in the postprocessing process.

In the PM scheme, Alice generates coherent states $|\alpha\rangle$, where $\alpha = \sqrt{2T\lambda^2}\gamma$, $\gamma = x_A + ip_A$. x_A and p_A are both randomly selected from a Gaussian distribution data set with mean 0 and variance V_A. T is related to the transmittance of photon subtraction, $\lambda^2 = (V-1)/(V+1)$, and V is variance of the two-mode squeezed vacuum state. Then after the coherent states are prepared, they are sent to Bob through quantum channels. Bob performs homodyne or heterodyne detection according to the type of protocol after receiving the quantum states, the measurement results are recorded as x_B and p_B. If Bob performs homodyne detection, he informs Alice the quadratures (x or p) he measures. Alice keeps the same quadratures with Bob. While in the case of heterodyne detection, both quadratures of x and p are kept.

After the quantum measurement and base sifting step, Alice chooses to accept part of the raw data according to the non-Gaussian postselection filter function with probability $P(k|x_A, p_A)$, the probability function of subtracting k photons is described by

$$P(k|x_A, p_A) = \frac{1}{k!}[\frac{(1-T)\lambda^2}{2}(x_A^2 + p_A^2)]^k \times \exp[-\frac{(1-T)\lambda^2}{2}(x_A^2 + p_A^2)]. \quad (1)$$

Then she reveals the selection results to Bob. Bob keeps the corresponding raw data. After the non-Gaussian postselection, Alice's raw data no longer follow Gaussian distribution. But the distribution of Bob's raw data remains unchanged. The probability density function of the raw data before and after non-Gaussian postselection is shown in Fig. 2. The black solid line represents the original Gaussian distribution function of Alice's raw data. The red, green, blue solid lines represent the non-Gaussian distribution function of Alice's data after virtual photon subtraction with $k = 1, 2, 3$, respectively. As shown in Fig. 2, for the raw data of Alice, the probability of some data in the Gaussian distribution is lower than that in the non-Gaussian distribution. Therefore, it is impossible to directly sample non-Gaussian distribution data from Gaussian distribution data in this situation.

To solve this problem, the acceptance-rejection sampling method is used to convert the Gaussian distribution data to non-Gaussian distribution data, which is a sampling method from probability density function. This method is to extract subsequence of random variables from a

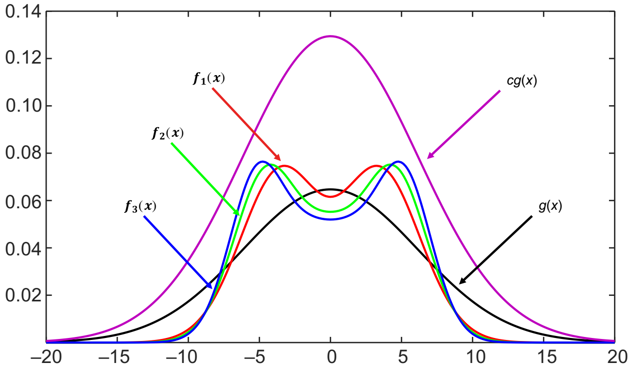

FIG. 2. Probability density function of the Gaussian distribution and non-Gaussian distribution after postselection. The X axis is the value of raw data, the Y axis is the corresponding density. $g(x)$ is the probability density function of Gaussian distribution. c is a constant for effective sampling. $f_1(x), f_2(x), f_3(x)$ are the probability density function of non-Gaussian distribution after virtual photon subtraction with $k = 1, 2, 3$ separately. The modulation variance is set to 20.

sequence with a specific distribution according to a rule and make them meet the given probability distribution. Suppose the random variable is x, its value range is $[a, b]$, its probability density function $f(x)$ of non-Gaussian distribution is bounded, which satisfies $\max\{f(x)|a \leqslant x \leqslant b\} = A$. For effective sampling, the probability density function of Gaussian distribution is required to be greater than that of non-Gaussian distribution for any x. However, as shown in Fig. 2, the probability density function of raw data $g(x)$ does not satisfy the condition that it is always greater than $f(x)$ $[f_1(x), f_2(x), f_3(x)]$ for any x. In order to satisfy the condition, we construct an alternative probability density function, which satisfies

$$cg(x) \geqslant f_k(x), x \in [a, b], \tag{2}$$

where c is a constant. The purple solid line represents the probability density function of $cg(x)$, it can be seen that the probability is greater than that of $f(x)$ for any x. The value of c should be as small as possible to improve sampling efficiency, which can be defined as

$$E = \frac{1}{m}. \tag{3}$$

It represents the average number of original distribution random variables m required to obtain a random variable with a specific distribution. In our case, it is equivalent to the success probability of the overall non-Gaussian postselection.

For a raw data x of Alice, she randomly generates a random number d that obeys a uniform distribution in the interval of $[0, cg(x)]$, where $d = cg(x)\xi, \xi \in U[0, 1]$. Then, she compares d and $f_k(x)$, if $d \leqslant f_k(x)$, she accepts x as a non-Gaussian distribution data after virtual subtraction of k photons. Otherwise, she rejects it and restarts the above process until all the raw data are completed.

After completing the non-Gaussian postselection process, they use the saved data to perform the postprocessing process through a classical authentication channel, including information reconciliation, parameter estimation, and privacy amplification. The secret key rate against collective attacks for reverse reconciliation of the k photons subtraction is described by

$$K_{\mathrm{PS}}^{k} = P(k)[\beta I(A:B) - S(E:B)], \tag{4}$$

where $P(k)$ is the success probability of overall virtual k photons subtraction (the success probability of the non-Gaussian postselection), β is reconciliation efficiency, $I(A:B)$ is classical mutual information between Alice and Bob, $S(E:B)$ is von Neumann entropy between Eve and Bob.

B. Non-Gaussian reconciliation in CV QKD

Suppose that the variables of Alice and Bob are X and Y after non-Gaussian postselection. X follows non-Gaussian distribution and Y still follows Gaussian distribution. The quantum channel can be seen as an additive white Gaussian noise (AWGN) channel. Then we have $Y = tX + Z$, where t is related to the channel transmittance and detection efficiency, Z is channel noise, which follows Gaussian distribution. For information reconciliation, SNR is the main parameter of concern. Thus for simplicity, we can fit $t = 1$. In addition, direct reconciliation is limited by 3-dB loss. Therefore, reverse reconciliation is used in our scheme, which can break this limit. Alice performs the error correction to obtain the identical keys with Bob.

Alice and Bob first convert the AWGN channel to a virtual binary input AWGN channel. Then they can use channel coding and decoding technology to correct errors between them. Multidimensional reconciliation is used to finish the first step. Bob normalizes the data Y after postselection according to the dimension of multidimensional reconciliation. Then he randomly chooses a uniform distribution vector U, which is generated by a quantum random number generator. Next, a mapping function $M(Y', U)$ from normalized variable Y' to U is constructed by orthogonal transformation matrix. Y' and U satisfy the following relationship:

$$M(Y', U)Y' = U. \tag{5}$$

He sends the mapping function to Alice through a classical authentication channel, which means that eavesdropper Eve can get all the information but she cannot change the information without the knowledge of both sides of the legal communication. Alice receives the mapping function $M(Y', U)$ and normalizes her non-Gaussian distribution data X after postselection. Then she rotates her normalized data X' to V through the mapping function, which can be calculated by

$$M(Y', U)X' = V, \tag{6}$$

where V is the noise form of U. They repeat the above process until all the data are converted. Finally, they select the appropriate channel codes according to the channel parameters to perform the error-correction process.

MET LDPC codes are the generalization form of LDPC codes, which is very suitable for error correction under extremely low SNRs. They can achieve performance close to Shannon's limit. Thus, we choose the MET LDPC code as the channel-coding technology to correct the errors between Alice and Bob. Firstly, the code rate of MET LDPC code is calculated according to the estimated quantum channel characteristics. Secondly, the degree distribution of the code rate is obtained by density evolutionary algorithm. Then select a suitable construction method to generate the parity-check matrix. Finally, Alice and Bob use the matrix for encoding and decoding to correct the errors between them to get completely consistent data.

The encoding process in a CV QKD system is very different from that in classical communication. It does not need a generation matrix. The parity-check matrix of error-correction code is directly multiplied by the binary data after reconciliation to obtain the syndromes. Then Bob sends the syndromes to Alice through a classical authentication channel, which will be errorless in the transmission process but Eve can get all the information. This is different from classical communication. After getting the syndromes, Alice initializes the information according to the data after reconciliation and uses the same parity check matrix to correct errors. In the message iteration process of error correction, the syndromes sent by Bob needs to be used and compared with Alice's temporary syndromes to judge whether the decoding is successful. This is another big difference from classical communication.

The error-correction codes used in CV QKD are MET LDPC codes, which have many decoding algorithms, such as the probability domain belief propagation algorithm (BP), log-likelihood ratio belief propagation algorithm (LLR BP) and so on, in which the BP algorithm is a commonly used decoding algorithm in the CV QKD system. Compared with other decoding algorithms, it has higher accuracy and can ensure the success rate of decoding in the CV QKD system. In the conventional BP decoding algorithm, after information initialization, it is necessary to traverse the check nodes and variable nodes to update the edge information in the parity-check matrix, then updating the information of each node accordingly, finally comparing the syndromes. If the decision is successful, end the decoding, otherwise continue the iteration until the maximum number of iterations is reached. Although this algorithm has high accuracy, the updated nodes are in a waiting state before the next update, the utilization rate is low. Thus, a layered BP (LBP) decoding algorithm [40] is introduced to the postprocessing of the CV QKD system, which can make faster use of the updated node information and improve the decoding efficiency. In the LBP decoding algorithm, each layer will update the variable node, taking the updated variable node as the input of the next layer to participate in the operation of the next layer in the same iteration. In this way, the updated information will be immediately used in this iteration, which can reduce the iteration number. Generally, it only needs half of the iteration number to achieve the same effect as the BP decoding algorithm. Thus, it can speed up the decoding process and it is suitable for application in high-speed postprocessing for the CV QKD system.

III. PERFORMANCE OF THE PROTOCOL

In this section, we first present the performance of the non-Gaussian postselection in terms of sampling efficiency from Gaussian distribution data to non-Gaussian distribution data. Then we present the performance of non-Gaussian reconciliation for the CV QKD system in terms of reconciliation efficiency, frame error rate of error correction, and average iteration number.

A. Non-Gaussian postselection performance

As described in Sec. II, for the virtual k-photon subtraction, we cannot directly sample non-Gaussian data from the raw data of Gaussian distribution due to the probability of Gaussian distribution may be higher than that of the non-Gaussian distribution. We present the acceptance-rejection sampling method to solve this problem, in which the sampling efficiency is a very useful parameter to evaluate sampling performance. In addition to Eq. (3), the sampling efficiency can also be expressed by geometric interpretation. It refers to the probability that the data conforming to $c_k g(x)$ falls under $f_k(x)$.

The selection of c in Eq. (2) has a significant impact on sampling efficiency. First, it needs to satisfy that $f_k(x)$ is completely below $cg(x)$ in order to sample correctly. Secondly, the sampling efficiency should be as high as possible. That is, the value of c_k should be as small as possible when condition 1 is met. Therefore, its value can be calculated by

$$c_k = \max_x [\frac{f_k(x)}{g(x)}], x \in R. \tag{7}$$

As shown in Fig. 3, we give the Gaussian distribution probability density function of actual data and the corresponding non-Gaussian probability density function with virtual subtraction of one photon. We can obtain that the optimal value of c_1 is about 1.32 calculated by Eq. (7) when T is set to 0.8. The corresponding sampling efficiency is about 75.4%, which is much higher than the previous results of sampling with uniformly distributed data. Similarly, we can get the results of virtual k-photon subtraction.

B. Non-Gaussian reconciliation performance

Information reconciliation has an impact on the performance of the CV QKD system. Reconciliation efficiency not only affects whether secret keys can be extracted, but also affects the transmission distance of the CV QKD system. On the other hand, the success rate of reconciliation and processing speed also have an impact on the secret key rate of the system. Thus, we test the error-correction performance of both Gaussian and non-Gaussian data, including reconciliation efficiency, FER, and average iteration number (AIN).

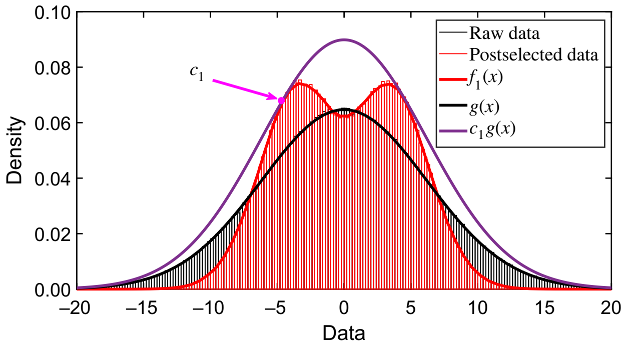

FIG. 3. The Gaussian distribution probability density function of actual data and non-Gaussian probability density function with virtual subtraction of one photon. The thin black line represents the probability density of raw data actually generated. The thin red line represents the probability density of postselected data after virtual subtraction of one photon. $g(x)$ and $f_1(x)$ are fitted probability density functions of raw data and postselected data (virtual subtraction of one photon) separately. The pink dot represents the point where c gets the optimal value when virtual subtracting one photon, recording as c_1. The purple line represents the probability density function after $g(x)$ is enlarged by c_1 times. The modulation variance is set to 20.

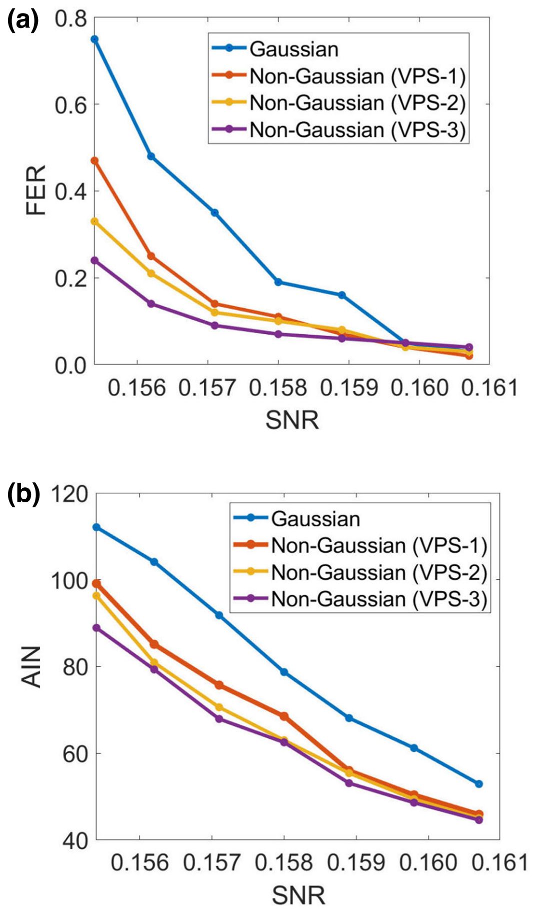

FIG. 4. Performance comparison of error correction between Gaussian and non-Gaussian data. The error-correction code used for Gaussian and non-Gaussian case is the MET LDPC code, whose rate is 0.1. (a) FER of Gaussian and non-Gaussian data after error correction under different SNR. (b) Average iteration number (AIN) of decoding corresponding to Gaussian and non-Gaussian data in (a). The blue line represents the FER or AIN of Gaussian data after error correction. The rest lines represent the FER or AIN of non-Gaussian data, where red line, yellow line, and purple line, respectively, represents virtual one-photon, two-photon, and three-photon subtraction (VPS-1, VPS-2, and VPS-3). The dots represent the error-correction performance of actual data, reconciliation efficiency from right to left is 93 %, 93.5 %, 94 %, 94.5 %, 95 %, 95.5 %, 96 % respectively. The maximum iteration number is set to 150.

The error-correction performance of four types of data distribution is tested under two MET LDPC codes. The data of these four types of distribution contain Gaussian distribution data and three non-Gaussian distribution data, which includes the data of virtual one-photon subtraction, virtual two-photon subtraction, virtual three-photon subtraction. The two MET LDPC codes are a rate of 0.1 and 0.05. For each rate of MET LDPC code and each type of data, seven sets of data with different SNR are tested. The test results are shown in Figs. 4 and 5.

We test more than 100 data blocks for each case. The size of each data block is 10^6. As can be seen from the results of Figs. 4 and 5, the error-correction performance of the non-Gaussian case is higher than that of the Gaussian case both in FER and AIN. The LBP decoding algorithm is used for the error-correction process, which has little effect on FER of decoding. However it can reduce about half of the AIN, the decoding speed can be greatly increased to improve the secret key rate of the CV QKD system. FER is related to the set maximum number of iterations, the FER can be reduced by increasing the maximum number of iterations to a certain extent. But it will also increase the decoding delay simultaneously, thus there is a trade-off between FER and AIN. In order to compare the error-correction performance under different conditions, we set the maximum number of iterations to 150 for all the tests. In actual applications, the maximum number of iterations can be reasonably set according to the average number of iterations for different cases.

Figures 4 and 5 show the test results for two MET LPDC codes, the code rate of 0.1 and 0.05 separately. Although the error-correction performance of non-Gaussian data is better than that of Gaussian data at both codes, it also has some different characteristics. For the code rate of 0.1, the error-correction performance of non-Gaussian data is obviously better than that of Gaussian data both in FER and AIN, the error-correction performance is better with the increase of the number of virtual photon subtraction, especially at a relatively low SNR. This is mainly due to the fact that non-Gaussian postselection diffuses the data originally concentrated around 0 to the middle values, the larger the

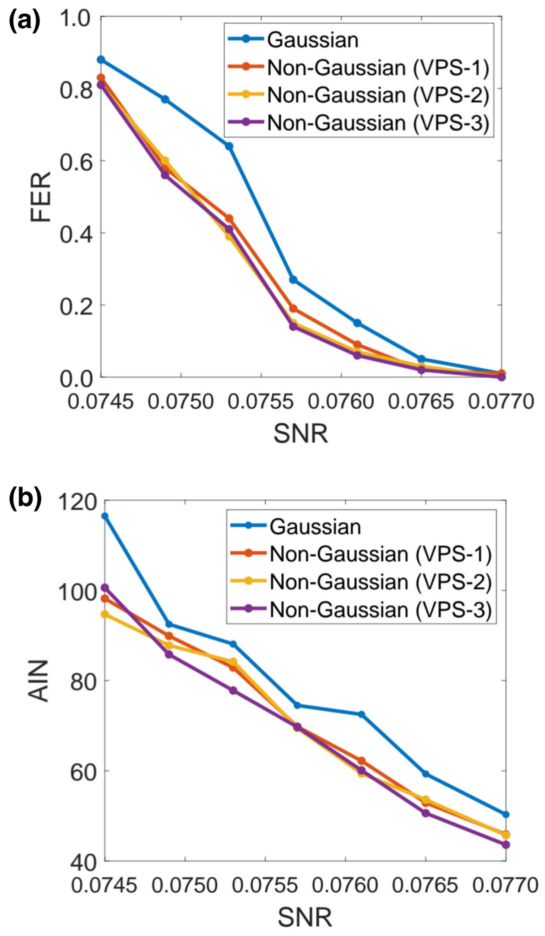

FIG. 5. Performance comparison of error correction between Gaussian and non-Gaussian data under the code rate of 0.05. (a) FER of Gaussian and non-Gaussian data after error correction under different SNR. (b) Average iteration number (AIN) of decoding corresponding to Gaussian and non-Gaussian data in (a). The dots represent the error-correction performance of actual data, reconciliation efficiency from right to left is 93.5 %, 94 %, 94.5 %, 95 %, 95.5 %, 96 %, 96.5 % respectively. The maximum iteration number is set to 150.

values diffusion with the increase of the number of virtual photon subtraction. Simultaneously, the large value will also concentrate to the middle value. Therefore, the error-correction performance will not continue to increase. At a relatively high SNR, error correction is relatively easy at this time, so FER of error correction is very low (close to 0) for both Gaussian data and non-Gaussian data, continuing to increase the SNR cannot reflect the advantages of non-Gaussian data. However, non-Gaussian data error correction can converge faster, so the AIV is less than that of Gaussian data, which will increase the error-correction speed and the secret key rate of the CV QKD system.

For the code rate of 0.05, the error-correction performance of non-Gaussian data is also higher than that of Gaussian data, but its advantage is lower than that of 0.1 code rate matrix. This is because the SNR of error-correction data corresponding to 0.05 code rate is low, the power of signal is much smaller than that of the noise. In this case, the signal is completely submerged in the noise, so it is difficult to correct the errors. Therefore, the advantages of non-Gaussian postselection are limited, with the increase of the number of photon subtraction, its advantage is not as obvious as that in 0.1 code rate. Although the error-correction gain caused by different photon subtraction is not very obvious, the non-Gaussian postselection data still makes the decoding converge faster than that of Gaussian data due to the reduction of the values near 0. Therefore, the FER and AIN performance of decoding processing is still improved.

We can use a rate-adaptive method [17] or non-fixed rate error-correction codes [28] to expand the applicable range of SNR. We have studied these two methods in the preamble work, combining these two methods, the non-Gaussian error-correction method proposed in this paper can play an advantage in a large range of SNR.

Figure 6 shows the secret key rate and transmission distance comparison of the original protocol (Gaussian case) and one-photon subtraction protocol (non-Gaussian case). Figure 6 shows that non-Gaussian protocols can still achieve high secret key rate over long distance range, which greatly expand the maximal transmission distance. However, for the short distance range, the secret key rate is more worthwhile than the original protocols. The main reason is that the probability of photon subtraction success is low. In other words, for non-Gaussian postselection, after selecting the original Gaussian data, since the amount

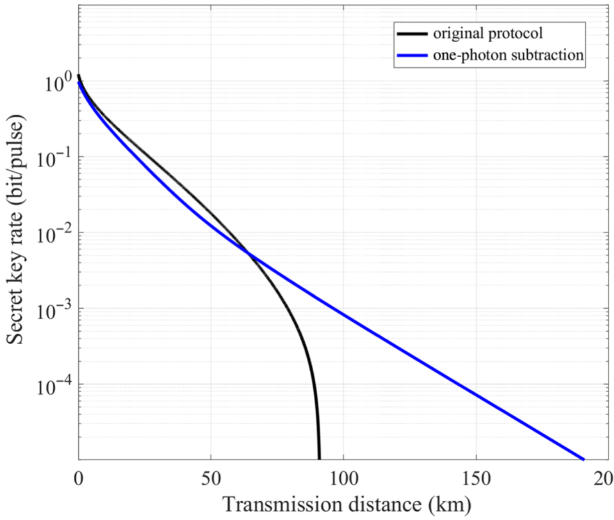

FIG. 6. The secret key rate and transmission distance comparison of the original protocols (Gaussian case) and one-photon subtraction (non-Gaussian case). The modulation variance is 20. Reconciliation efficiency is 95 %.

of selected data is reduced, the average secret key rate is reduced.

In practical application, we are more concerned about the amount of secret keys obtained per unit time when the secret key rate is greater than 0. For non-Gaussian postselection, the reduction of data will lead to the reduction of the secret key rate of single pulse, but it will greatly improve the data-processing speed. The reconciliation efficiency and decoding success rate of non-Gaussian data are higher than that of Gaussian data, thus the secret key rate per unit time is not necessarily lower than that in the Gaussian case even at short distance range. It can be further studied in the subsequent high-speed implementation.

IV. CONCLUSION

In this paper, we propose a non-Gaussian reconciliation method for CV QKD protocols by non-Gaussian postselection at Alice's side, which can reduce the FER and AIN of decoding. We propose an effective postselection method to obtain non-Gaussian data follows a specific distribution from Gaussian data, which greatly improves the success rate of virtual photon subtraction of the CV QKD system. Multidimensional reconciliation and MET LDPC codes are used to perform the information reconciliation in postprocessing of the CV QKD system. The layered belief propagation decoding algorithm is introduced to the error correction, which can greatly reduce the decoding complexity and improve the decoding speed. We test the error-correction performance of Gaussian data and non-Gaussian data after our proposed postselection under two representative codes with rate of 0.1 and 0.05. We test seven sets of data for each case, respectively. The corresponding reconciliation efficiency ranges from 93 % to 96.5 %. The results show that the FER and AIN of decoding performance of non-Gaussian data is significantly better than that of Gaussian data, which greatly improves the secret key rate of the CV QKD system.

ACKNOWLEDGMENTS

This work is supported by National Natural Science Foundation of China under Grants No. 62001041, No. 62201012, the Fundamental Research Funds of BUPT under Grant No. 2022RC08, and the Fund of State Key Laboratory of Information Photonics and Optical Communications under Grant No. IPOC2022ZT09.

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

[2] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. **92**, 025002 (2020).

[3] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Advances in quantum cryptography, Adv. Opt. Photon. **12**, 1012 (2020).

[4] C. H. Bennett and G. Brassard, in *Proc of IEEE International Conference on Computers* (IEEE, New York, 1984).

[5] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, W. Chen, *et al.*, Twin-field quantum key distribution over 830-km fibre, Nat. Photonics **16**, 154 (2022).

[6] F. Grosshans and P. Grangier, Continuous Variable Quantum Cryptography Using Coherent States, Phys. Rev. Lett. **88**, 057902 (2002).

[7] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Quantum key distribution using Gaussian-modulated coherent states, Nature **421**, 238 (2003).

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

[9] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Experimental demonstration of long-distance continuous-variable quantum key distribution, Nat. Photonics **7**, 378 (2013).

[10] R. García-Patrón and N. J. Cerf, Unconditional Optimality of Gaussian Attacks Against Continuous-Variable Quantum Key Distribution, Phys. Rev. Lett. **97**, 190503 (2006).

[11] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security Against Coherent Attacks, Phys. Rev. Lett. **109**, 100502 (2012).

[12] A. Leverrier, Composable Security Proof for Continuous-Variable Quantum Key Distribution with Coherent States, Phys. Rev. Lett. **114**, 070501 (2015).

[13] N. Jain, H.-M. Chin, H. Mani, C. Lupo, D. S. Nikolic, A. Kordts, S. Pirandola, T. B. Pedersen, M. Kolb, B. Ömer, *et al.*, Practical continuous-variable quantum key distribution with composable security, Nat. Commun. **13**, 4740 (2022).

[14] Z. Chen, X. Wang, S. Yu, Z. Li, and H. Guo, Continuous-mode quantum key distribution with digital signal processing, Npj Quantum Inf. **9**, 28 (2023).

[15] H. Wang, Y. Pi, W. Huang, Y. Li, Y. Shao, J. Yang, J. Liu, C. Zhang, Y. Zhang, and B. Xu, High-speed Gaussian-modulated continuous-variable quantum key distribution with a local local oscillator based on pilot-tone-assisted phase compensation, Opt. Express **28**, 32882 (2020).

[16] T. Shen, Y. Huang, X. Wang, H. Tian, Z. Chen, and S. Yu, Strengthening practical continuous-variable quantum key distribution against measurement angular error, Opt. Express **29**, 30978 (2021).

[17] X. Wang, Y. Zhang, S. Yu, B. Xu, Z. Li, and H. Guo, Efficient rate-adaptive reconciliation for continuous-variable quantum key distribution, Quantum Inf. Comput. **17**, 1123 (2017).

[18] X. Wang, S. Guo, P. Wang, W. Liu, and Y. Li, Realistic rate-distance limit of continuous-variable quantum key distribution, Opt. Express **27**, 13372 (2019).

[19] D. Huang, D. Lin, C. Wang, W. Liu, S. Fang, J. Peng, P. Huang, and G. Zeng, Continuous-variable quantum key distribution with 1 mbps secure key rate, Opt. Express **23**, 17511 (2015).

[20] T. Wang, P. Huang, Y. Zhou, W. Liu, H. Ma, S. Wang, and G. Zeng, High key rate continuous-variable quantum key distribution with a real local oscillator, Opt. Express **26**, 2794 (2018).

[21] D. Huang, P. Huang, D. Lin, and G. Zeng, Long-distance continuous-variable quantum key distribution by controlling excess noise, Sci. Rep. **6**, 19201 (2016).

[22] N. Wang, S. Du, W. Liu, X. Wang, Y. Li, and K. Peng, Long-Distance Continuous-Variable Quantum Key Distribution with Entangled States, Phys. Rev. Appl. **10**, 064028 (2018).

[23] S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, Asymptotic Security of Continuous-Variable Quantum Key Distribution with a Discrete Modulation, Phys. Rev. X **9**, 021059 (2019).

[24] J. Lin, T. Upadhyaya, and N. Lütkenhaus, Asymptotic Security Analysis of Discrete-Modulated Continuous-Variable Quantum Key Distribution, Phys. Rev. X **9**, 041064 (2019).

[25] Y. Huang, T. Shen, X. Wang, Z. Chen, B. Xu, S. Yu, and H. Guo, Realizing a Downstream-Access Network using Continuous-Variable Quantum Key Distribution, Phys. Rev. Appl. **16**, 064051 (2021).

[26] Y. Tian, P. Wang, J. Liu, S. Du, W. Liu, Z. Lu, X. Wang, and Y. Li, Experimental demonstration of continuous-variable measurement-device-independent quantum key distribution over optical fiber, Optica **9**, 492 (2022).

[27] H. Wang, Y. Li, Y. Pi, Y. Pan, Y. Shao, L. Ma, Y. Zhang, J. Yang, T. Zhang, W. Huang, *et al.*, Sub-gbps key rate four-state continuous-variable quantum key distribution within metropolitan area, Commun. Phys. **5**, 162 (2022).

[28] C. Zhou, X. Wang, Y. Zhang, Z. Zhang, S. Yu, and H. Guo, Continuous-Variable Quantum Key Distribution with Rateless Reconciliation Protocol, Phys. Rev. Appl. **12**, 054013 (2019).

[29] R. Blandino, A. Leverrier, M. Barbieri, J. Etesse, P. Grangier, and R. Tualle-Brouri, Improving the maximum transmission distance of continuous-variable quantum key distribution using a noiseless amplifier, Phys. Rev. A **86**, 012327 (2012).

[30] T. Opatrný, G. Kurizki, and D.-G. Welsch, Improvement on teleportation of continuous variables by photon subtraction via conditional measurement, Phys. Rev. A **61**, 032302 (2000).

[31] P. Huang, G. He, J. Fang, and G. Zeng, Performance improvement of continuous-variable quantum key distribution via photon subtraction, Phys. Rev. A **87**, 012317 (2013).

[32] J. Fiurášek and N. J. Cerf, Gaussian postselection and virtual noiseless amplification in continuous-variable quantum key distribution, Phys. Rev. A **86**, 060302 (2012).

[33] H. M. Chrzanowski, N. Walk, S. M. Assad, J. Janousek, S. Hosseini, T. C. Ralph, T. Symul, and P. K. Lam, Measurement-based noiseless linear amplification for quantum communication, Nat. Photonics **8**, 333 (2014).

[34] Z. Li, Y. Zhang, X. Wang, B. Xu, X. Peng, and H. Guo, Non-Gaussian postselection and virtual photon subtraction in continuous-variable quantum key distribution, Phys. Rev. A **93**, 012310 (2016).

[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, Quantum key distribution over 25 km with an all-fiber continuous-variable system, Phys. Rev. A **76**, 042305 (2007).

[36] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, Multidimensional reconciliation for a continuous-variable quantum key distribution, Phys. Rev. A **77**, 042325 (2008).

[37] A. Shokrollahi, Raptor codes, IEEE Trans. Inf. Theory **52**, 2551 (2006).

[38] E. Arikan, Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels, IEEE Trans. Inf. Theory **55**, 3051 (2009).

[39] T. Richardson and R. Urbanke, *Modern Coding Theory* (Cambridge University Press, New York, 2008).

[40] D. Hocevar, in *IEEE Workshop on Signal Processing Systems, 2004. SIPS 2004.* (IEEE, Texas, 2004), p. 107.

[41] M. Navascués, F. Grosshans, and A. Acín, Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography, Phys. Rev. Lett. **97**, 190502 (2006).

[42] M. M. Wolf, G. Giedke, and J. I. Cirac, Extremality of Gaussian Quantum States, Phys. Rev. Lett. **96**, 080502 (2006).