Rate-Adaptive Polar-Coding-Based Reconciliation for Continuous-Variable Quantum Key Distribution at Low Signal-to-Noise Ratio

Zhengwen Cao,[1,2] Xinlei Chen,[1] Geng Chai,[1,*] Kexin Liang,[1] and Yang Yuan[1]

[1] *Institute for Quantum Information and Technology, School of Information Science and Technology, Northwest University, Xi'an 710127, China*

[2] *State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an, 710071, China*

(Received 27 October 2022; revised 9 February 2023; accepted 13 March 2023; published 7 April 2023)

Information reconciliation significantly impacts the performance of the practical continuous-variable quantum key distribution (CV QKD) system. Fixed-rate error-correction codes limit the potential applications of the CV QKD because they lead to reduced reconciliation efficiency when the signal-to-noise ratio of the quantum channel changes, further deteriorating the system's performance. Therefore, we propose a rate-adaptive polar-coding-based reconciliation scheme for practical CV QKD systems with the time-variant quantum channel. Experimental results verify that the proposed scheme can successfully extract secret keys within the range of signal-to-noise ratios from −0.5 to −4.5 dB, and the minimum frame-error rate can be less than 10^{-3}. Moreover, the proposed scheme can promote the application of the CV QKD system in a realistic environment.

DOI: 10.1103/PhysRevApplied.19.044023

I. INTRODUCTION

In the quantum key distribution (QKD) protocol, the two remote legitimate parties (the sender, Alice, and the receiver, Bob) can obtain theoretically unconditionally secret keys after the generation, transmission, and measurement of quantum signals [1,2]. According to different information-encoding carriers, QKD can be divided into two classifications: discrete-variable (DV) QKD and continuous-variable (CV) QKD. In the former case, the transmitted information is encoded in finite-dimensional Hilbert space, such as the polarization of a single photon. A single-photon detector detects the quantum state at the receiving end. Such protocols are relatively mature, but the fabrication and detection of quantum states are somewhat difficult [3]. In the latter case, information is encoded in the Hilbert space of infinite dimensions, such as the information encoded in the quadrature component of the optical field, and the optical field detection is completed by heterodyne or homodyne detectors [4,5]. The CV QKD protocol has more potential advantages in a realistic environment, as it offers the probability for implementations based on classical communication devices [6–8].

In the actual CV QKD system, the initial variables obtained by the communicating parties contain some errors due to the imperfection of the experimental equipment and noise interference from the eavesdropper (Eve) [9]. Therefore, postprocessing operations, such as parameter estimation [10,11], information reconciliation [12,13], and privacy amplification [14,15], on the initial variables are essential before generating the secret keys. The initial variables are continuous variables, so it is difficult to correct the error directly. Thus, a nonbinary reconciliation algorithm is needed to take advantage of the mature channel-compiled-code technology. The continuous variables are quantized or rotated through information reconciliation to obtain data that can be directly error corrected. Then, the appropriate error-correction code is selected to obtain the same secret keys for both sides of communication [12,16]. Finally, Alice and Bob each apply a privacy amplification to their shared correction keys to construct the final keys. At present, the main information-reconciliation algorithms in CV QKD are slice reconciliation [12], symbol reconciliation [16], and multidimensional reconciliation [17]. Among them, slice reconciliation has high differentiation of variables at high signal-to-noise ratios, but it breaks the symmetry and has high complexity. Symbol reconciliation is simple and low complexity, but it is only suitable for high signal-to-noise ratio conditions, and the judgment bit error rate is too high at low signal-to-noise ratios. The multidimensional reconciliation algorithm proposed by Leverrier and coworkers does not quantify continuous-variable data into discrete values before error correction like the traditional CV QKD reconciliation protocol. Instead, it uses continuous variables directly for error correction [18]. The core idea is to convert the additive white Gaussian noise

*Corresponding author. chai.geng@nwu.edu.cn

 © 2023 American Physical Society

(AWGN) channel data into virtual binary-input AWGN (BIAWGN) channel data using the rotational mapping of spherical codes in the multidimensional space. It effectively solves the problem that Gaussian continuous variables are difficult to screen under low signal-to-noise ratios [19], with an excellent error-correction code can significantly extend the secret-key rate and the maximal secure-transmission distance [20]. Polar codes is a channel-compilation code method proposed by Turkish scientist Erdal Arikan and is the channel-coding method that can be rigorously proven to achieve channel capacity [21]. Polar codes has a good error-correction performance, and compiled codes can achieve low complexity. Taking advantage of these advantages, Jouguet and Kunz-Jacques [22] and Nakassis and Mink [23] added polar codes to the QKD information-reconciliation protocol. Their research showed better error-correction performance than low-density parity-check codes.

In CV QKD postprocessing, the performance of information reconciliation significantly impacts the secret-key rate and maximal secure-transmission distance [24]. Specifically, highly efficient error-correction codes can improve the system's performance, but such fixed-code-rate error-correction codes are usually only applicable at a specific signal-to-noise ratio. When the practical signal-to-noise ratio differs from the code's optimal suitable signal-to-noise ratio, the reconciliation efficiency also decreases. Therefore, when the application scenarios of the system become more and more flexible, or the transmission environment is complex, the information-reconciliation algorithm with a compatible signal-to-noise ratio guarantees the system's stable key generation. In view of the above deficiencies, Zhang *et al.* adopted the incremental freezing scheme [25] of information bits in polar codes to fix the step size of frozen information bits in the information reconciliation, thus realizing the fixed-step code-rate adjustment [26]. Based on this scheme, here, we propose a rate-adaptive polar-coding-based reconciliation scheme. In this scheme, the channel state is estimated after information reconciliation to estimate the signal-to-noise ratio (SNR) and calculate the code rate. Then, the position of punctured and shortened bits is determined, according to the decoding reliability of polar codes to achieve the goal of rate-adaptive adjustment. The experimental results show that the scheme can successfully extract the key at low signal-to-noise ratios (between -4.5 and -0.5 dB), maintain a reconciliation efficiency of over 98 %, and have a good frame-error performance. Compared with the previous scheme [26], this scheme has a better frame-error performance under the same SNR environment. It has practical application advantages in long-distance transmission or high-performance system design.

This paper is structured as follows. Section II presents the design of a rate-adaptive polar-coding-based reconciliation scheme for CV QKD. Section III presents the specific principles of the design of the rate-adaptive function in the reconciliation scheme. Experimental results are given in Sec. IV. Finally, Sec. V concludes the paper.

II. RATE-ADAPTIVE POLAR-CODING-BASED RECONCILIATION SCHEME FOR CV QKD

Considering collective attacks and finite-size effects, the secret-key rate of a CV QKD system with reverse reconciliation is given by [27]

$$K = f_{\text{rep}}(1-\alpha)(1-\text{FER})\frac{n}{\iota}[\beta I_{AB} - \chi_{BE} - \Delta n], \quad (1)$$

where f_{rep} is the system's repetition frequency, α is the system overhead, FER is the reconciliation frame-error rate, ι is the total number of variables exchanged by Alice and Bob, and n is the number of variables used for key extraction. β is the reconciliation efficiency. I_{AB} is the Shannon mutual information of Alice and Bob. χ_{BE} is the maximum of the Holevo information that Eve can obtain from information from Bob. Δn is the finite-size offset factor. It can be seen from Eq. (1) that the reconciliation efficiency, β, is the key to controlling whether the system can generate secret keys [18,20]:

$$\begin{aligned}\beta &= \frac{R}{C},\\ &= \frac{R}{0.5\log_2(1+\text{SNR})},\\ &= \frac{R}{0.5\log_2(1+\frac{P_S}{P_N})},\end{aligned} \quad (2)$$

where R is the code rate of the error-correction code, SNR is the signal-to-noise ratio, C is the security capacity of the quantum channel, P_S is the average power of the transmitted signal in the channel, and P_N is the Gaussian noise power in the channel [27]. Therefore, an imperfect reconciliation scheme reduces the secret-communication distance and secret-key rate.

In the actual CV QKD system, the channel characteristics fluctuate due to interference by Eve and the influence of noise, resulting in a decline in the reconciliation performance. Suppose a designed polar code with a given code rate or a specific SNR is still adopted. In that case, its error-correction capability leads to an increased FER or reduced reconciliation efficiency. It can be seen from Fig. 1 that, when the reconciliation efficiency is improved at a fixed distance, the secret-key rate also increases. However, when the reconciliation efficiency is fixed, the secret-key rate decreases as the channel loss increases with increasing transmission distance. To maintain the system's performance, it is necessary to adopt different code rates in different transmission environments. Therefore, the correct real-time evaluation of the channel's SNR

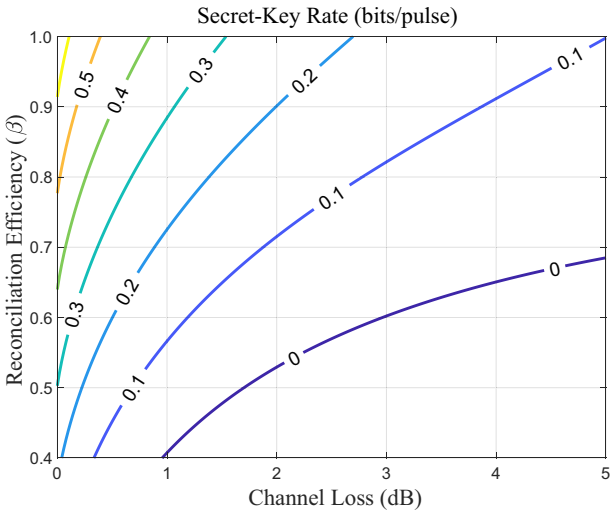

FIG. 1. Finite-size secret-key rate versus channel loss under different reconciliation efficiencies. From left to right, secret-key rate decreases with increasing channel loss under fixed reconciliation efficiency. Secret-key rate increases from bottom to top when the reconciliation efficiency is improved under fixed channel loss. Therefore, reconciliation efficiency is the key to restrict the secret-key rate. It can be seen from Eq. (2) that the error-correction code rate needs to be flexibly adjusted, according to the actual system's SNR changes to obtain a stable and efficient reconciliation performance.

[28] and the adaptive adjustment of the polar-code rate, according to the evaluation results, can guarantee a stable reconciliation performance of the system. In addition, if it can cooperate by raising the system's repetition frequency to increase the system's throughput or improve the overall performance of the postprocessing operation, the system's communication distance can be extended, or the system's secret-key rate can be improved. Here, we propose a rate-adaptive polar-coding-based information-reconciliation scheme. The detailed steps of the scheme (with reverse reconciliation as an example) are as shown in Fig. 2.

In the Gaussian-modulated coherent state (GMCS) CV QKD protocol [5], Alice prepares the first set of coherent states, $\{|x_1+ip_1\rangle, |x_2+ip_2\rangle, \ldots, |x_M+ip_M\rangle\}$, and sends them to Bob through the quantum channel. Bob uses the homodyne detector to measure the received coherent states. Owing to the system being affected by the detector's sensitivity and other factors in the actual experiment, Alice and Bob eventually share fewer variables than the total number of quantum states sent by Alice, i.e., $\{(x_i,y_i)|i=1,2,\ldots,\iota,\ \iota<M\}$, i.e., the initial variables. In the GMCS CV QKD protocol, the quantum channel is an AWGN channel. This means that $y=tx+z$, where t is related to the channel loss, $x\sim\mathcal{N}(0,\xi^2)$, and $z\sim\mathcal{N}(0,{\sigma_z}^2)$ is the channel noise with zero mean and a noise variance of ${\sigma_z}^2$. $t=\sqrt{\eta T}$, where η is the efficiency of the homodyne detector and T is the transmittance of the quantum channel. Details of the rate-adaptive information-reconciliation scheme are described as follows:

(1) First, Alice and Bob disclose the first set of variables for channel-state estimation—${\sigma_z}^2$ and SNR—and the estimation method is as follows [29]:

$$ {\sigma_z}^2=\frac{1}{\iota}\sum_{i=1}^{\iota}(y_i-tx_i)^2, \tag{3} $$

$$ \mathrm{SNR}=\frac{\xi^2}{{\sigma_z}^2}. \tag{4} $$

(2) After obtaining the channel state estimated by the first set of variables, Alice sends the second set of coherent states, and the two communicating parties directly conduct information reconciliation on the second set of initial variables. Alice and Bob divide the initial variables into d-dimensional vectors and normalize their Gaussian variables x and y to x' and y', respectively. Bob employs the QRNG to generate a uniformly distributed binary bit sequence, b, of total length L_b, the length of which is bounded by the mutual information between Alice and Bob, i.e., $\log_2 L_b/R\leqslant I_{AB}$.

(3) The sequence b is encoded as the information bit input of the polar encoder, and the matching code rate, R_b, is computed by the target reconciliation efficiency and estimated SNR of the first set of variables:

$$ R_b=\frac{\beta}{2}\log_2(1+\mathrm{SNR}). \tag{5} $$

The punctured and shortened bits are determined according to the matching code rate, and the code rate of the polar code is adjusted based on the decoding-reliability value of each subchannel after polarization, and the sequence c is output. Then, sequence c is converted into binary spherical sequence c'.

(4) Bob computes the rotation-mapping function, such that $M\left(y',c'\right)$ satisfies $M\left(y',c'\right)y'=c'$, and sends the function along with related side information to Alice by the public classical authenticated channel. $M\left(y',c'\right)$ and c' are independent, so data transmitted in the proposed scheme do not result in information leakage. After that, Alice maps the vector x' to v, such that $v=M\left(y',c'\right)x'$, and v is c with noise in the sequence.

(5) Alice decodes the polar code of sequence v. If decoding is successful, both parties obtain secret keys b. Moreover, Alice can recover all of Bob's initial variables from $M\left(y',c'\right)$, b, and side information. Suppose decoding fails, Bob randomly exposes some initial variables for channel-state estimation to improve the utilization of initial variables and the accuracy of the channel-state estimation.

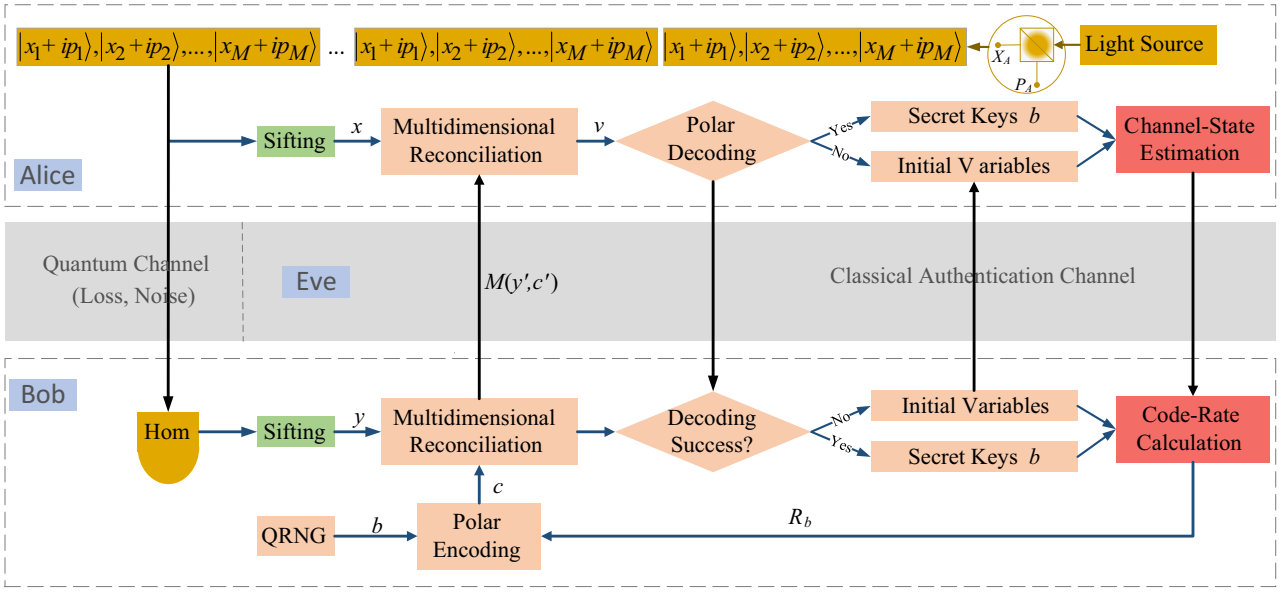

FIG. 2. Rate-adaptive CV QKD reverse polar-coding-based reconciliation scheme based on multidimensional reconciliation. Hom, homodyne detector; QRNG, quantum random-number generator; x and y, initial variables; b, random binary sequences generated by the QRNG; c, polar-encoder-output sequence; $M\left(y',c'\right)$, rotation-mapping function; R_b, matching code rate; v, decoder-input sequence. Alice transmits coherent states to Bob through the quantum channel repeatedly and randomly, and both parties postprocess on the classical authentication channel. After quantum state measurement and sifting, communication parties share a set of initial variables, x and y. Bob conducts information reconciliation on x and y. Matching code rate, R_b, required for reconciliation comes from the channel-state estimation results of the previous set of initial variables. After reconciliation, Alice uses initial variables to perform channel-state estimation and sends the result to Bob. Bob starts to prepare for information reconciliation of the next set of initial variables.

(6) Through the above steps, if decoding is successful in the reconciliation, Alice can use all the initial variables x and y to estimate the channel state. If decoding fails, Alice and Bob randomly choose a certain proportion of variables to estimate the channel. The channel-state-estimation result for this set of initial variables can assist with error correction and code-rate adjustment of the following set of initial variables.

By analogy, starting from the second set of initial variables, each set of initial variables directly conducts information reconciliation. Moreover, the channel characteristics and matching code-rate, R_b, required for information reconciliation are derived from the channel-state estimation results of the previous set of initial variables. After information reconciliation, Alice performs channel-state estimation. The result is used for the next set of initial variables to complete information reconciliation.

III. DESIGN OF RATE-ADAPTIVE RECONCILIATION SCHEME

Next, the proposed scheme is introduced in detail. Specifically, Sec. III A clearly introduces the real-time channel-state estimation scheme, and the rate-adaptive reconciliation scheme is discussed in Sec. III B.

A. Real-time channel-state estimation

A real-time channel-state estimation scheme is proposed for the problem of channel feature fluctuation in the CV QKD system. This scheme utilizes initial variables for channel-state estimation after each set of information reconciliation, which, in cooperation with the subsequent rate-adaptive reconciliation scheme, can improve the system's performance. Algorithm 1 illustrates the real-time channel-state estimation principle. In detail, Alice and Bob choose d to divide the second set of continuous-variables into d-dimensional vectors x and y, where d is the dimension of multidimensional reconciliation. Then the Gaussian variables x and y of Alice and Bob are normalized to x' and y', respectively. Bob uses a QRNG to generate a uniformly distributed binary bit sequence b and adds the corresponding cyclic redundancy check (CRC) parity check information (equivalent to increasing the code distance and improving the error-correction capability). Sequence c after adding the CRC to sequence b is encoded as the information bit input of the polar-code encoder.

Then, Bob maps d-dimensional vector $c' \in \left\{-1/\sqrt{d}, 1/\sqrt{d}\right\}^d$, according to the binary-phase-shift keying encoding, such that all code words lie on a sphere centered on zero. Afterwards, Bob computes the rotation-mapping function from y' to c' on the d-dimensional unit sphere,

Require: $M(y', c')$: rotation mapping function; x, y: d-dimensional initial variables; b: binary bit sequence; crc: CRC check code
Ensure: R_b: matching code-rate; s: secret keys
Initialize b randomly
repeat
  $x' \leftarrow$ normalize x, $y' \leftarrow$ normalize y
  $[b, crc]$ are input as the information bits of the polar code encoder, output c
  $c' \leftarrow$ Spherical mapping c
  Side information computing $M(y', c')$
  data mapping $v \leftarrow \|x\| * M(y', c') * x' / \|y\|$
  if ACK $= 0$ **then**
    decoding success, $s \leftarrow b$
    recover Bob's all initial variables $y \leftarrow (M(y', c')\,|c')\,\|y\|$
  else
    decoding failure
    randomly public Bob's initial variables y
  end if
  compute channel parameters
  compute the matching code-rate R_b
until EOT=1

Algorithm 1. Real-time channel-state estimation algorithm

which satisfies $M(y', c')\, y' = c'$. Subsequently, Bob shares $M(y', c')$ with Alice through the public channel and other side information, i.e., the norm of y and parameters of polar codes. With the received side information, Alice can map her Gaussian variable x' to v.

Through the above processes, Alice and Bob construct a virtual BIAWGN channel that inputs c (Bob) and outputs v (Alice) in a reverse reconciliation scheme [20]. Finally, Alice calculates the received information's log-likelihood ratio (LLR). For convenience, only a d-dimensional vector is considered, and its derivation is as follows:

$$\begin{aligned} \mathrm{LLR}(v_i) &= ln\frac{P_r(v_i|c_i(s=0))}{P_r(v_i|c_i(s=1))}, \\ &= ln\frac{\frac{1}{\sqrt{2\pi\sigma_z^2}}e^{-\frac{[\|x\|v_i-\|y\|c(s)]^2}{2\sigma_z^2}|s=0}}{\frac{1}{\sqrt{2\pi\sigma_z^2}}e^{-\frac{[\|x\|v_i-\|y\|c(s)]^2}{2\sigma_z^2}|s=1}}, \\ &= \frac{2\,\|x\|\,\|y\|}{\sqrt{d}\sigma_z^2}v_i, \end{aligned} \tag{6}$$

where $P_r(\cdot)$ is the channel's posterior probabilities. c_i and v_i are the ith components of c and v, respectively, where $i = [1, 2, \ldots, d]$. $c(s) = (-1)^s/\sqrt{d}$ and $s \in \{0, 1\}$. $\|\cdot\|$ is called a norm on the d-dimensional variable; σ_z^2 is the channel-estimation result of the previous set of variables. The polar-code decoding adopts a CRC-aided (CA) successive-cancellation list (SCL) [30], which adds the CRC based on the SCL [31] decoding. The SCL decoder allows, at most, L locally best candidates during the decoding process to reduce the chance of missing the correct code word. In each decoding step, the SCL doubles the number of candidate paths and selects the L best ones from the list by pruning. Then, the decoder adopts the prior information of "correct information bits can pass the CRC check" to select the L search paths and output the best decoding path. Thus, this CA SCL decoding can further improve the performance of polar codes.

Supposing decoding is successful, Alice sends acknowledge character ACK $= 0$, and both parties obtain a set of consistent secret keys b. Meanwhile, Alice recovers Bob's initial variables from $M(y', c')$ and $\|y\|$, which is given by

$$y = (M(y', c')\,|c')\,\|y\|, \tag{7}$$

where $\|y\|$ is sent from Bob to Alice when Bob sends the mapping function $M(y', c')$. $\|y\|$ is independent of c', so the secret keys' information is not disclosed. Furthermore, recovering Bob's initial variables does not require classical communication. Thus, it does not affect the security of the CV QKD system. On the other hand, Alice sends acknowledge character ACK $= 1$ if decoding fails. Bob randomly sends initial variables to Alice, so that Alice can estimate the channel characteristics more accurately. After that, the subsequent set of variables can perform reconciliation and error correction according to the channel-state estimation result of the previous set of variables.

B. Rate-adaptive reconciliation scheme

After deriving the real-time state of the channel, the polar-code rate needs to be adjusted to accommodate the fluctuating channel to improve the reconciliation performance. Here, we present a rate-adaptation reconciliation scheme based on the reliability of polar-code decoding. The detailed steps of the scheme are as follows:

(1) Bobcomputes the decoding-error probability, P_e, and reliability value of each channel, and then sorts the reliability value. Information bits are transmitted on the channel with high reliability, and frozen bits are transmitted on the channel with low reliability to assist in decoding.

Bob uses a method on the coding side to make each subchannel show different reliability. Since the multidimensional reconciliation transforms the channel into a virtual channel approximating a BIAWGN, the received signal's probability density function is still Gaussian. Therefore, the Gaussian approximation (GA) can measure the subchannel reliability, greatly reducing the computational complexity. The GA is a simplified approach to density evolution [32]. According to the Gaussian approximation assumption, the LLR of each subchannel obeys a Gaussian

distribution with a variance of 2 times the mean, i.e., $L_N^{(i)} \sim \mathcal{N}(m_N^{(i)}, 2m_N^{(i)})$, where $m_1^{(1)} = 2/\sigma^2$. According to this construction theory, the calculation of density evolution is transformed into a recursive calculation of $m_N^{(i)}$:

$$\begin{aligned} m_{2N}^{(2i-1)} &= \varphi^{-1}\left(1-\left[1-\varphi\left(m_N^{(i)}\right)\right]^2\right), \\ m_{2N}^{(2i)} &= 2m_N^{(i)}, \\ m_1^{(1)} &= 2/\sigma^2. \end{aligned} \tag{8}$$

The function $\varphi(x)$ is approximated as [32]

$$\varphi(x) = \begin{cases} 1-\dfrac{1}{\sqrt{4\pi x}}\displaystyle\int_{\infty}^{-\infty}\tanh\frac{u}{2} \\ \times e^{-\frac{(u-x)^2}{4x}}du, x>0, \\ 1, x=0, \end{cases} \tag{9}$$

so that the decoding-error probability of the subchannel is given by [33]

$$P_e\left(W_N^{(i)}\right) = Q\left(\frac{m_N^{(i)}}{\sqrt{2m_N^{(i)}}}\right) = Q\left(\sqrt{\frac{m_N^{(i)}}{2}}\right), \tag{10}$$

where $W_N^{(i)}$ is the channel transition probability; $Q(x) = 1/\sqrt{2\pi x}\int_x^{+\infty} e^{-\frac{t^2}{2}}dt$ is the complementary error function. The parent code is constructed by selecting the more reliable bit-channel locations as the set of information bits, and the less-reliable locations as the set of frozen bits by the GA.

(2) Bob can obtain the matching code rate, R_{b2}, for the second set of variables based on Eq. (5) after getting the channel parameters for the first set of variables. The information sequence of the second set of variables is encoded, and the sequence is encoded using systematic polar codes to distinguish the information bits clearly [34]. The encoding is done as follows.

For polar codes (N, K, A, A^c), the preencoded word is denoted as u. K more-reliable subchannels constitute a set A; $N-K$ less-reliable subchannels constitute a set A^c, which should be selected to transmit the information bits, u_A, and frozen bits, u_{A^c}, respectively. The length of K is $N \times R_{b2}$, which means that u_A is the sequence with length K, after adding the CRC check codes to sequence b. The systematic polar codes divide the encoded code word into two parts, i.e., $c = [c_A\ c_{A^c}]$. The frozen bits are generally fixed to 0, i.e., $u_{A^c} = 0$. Then, the encoding process can be expressed as [35]

$$\begin{aligned} c_A &= u_A G_{AA} + u_{A^c} G_{A^cA} = u_A G_{AA}, \\ c_{A^c} &= u_A G_{AA^c} + u_{A^c} G_{A^cA^c} = u_A G_{AA^c}, \end{aligned} \tag{11}$$

where G_{AA^c} denotes the submatrix of the generator matrix $G_N = F^{\otimes N}$, consisting of elements $G_{i,j}$ with $i \in A$ and $j \in A^c$, and similarly for the other submatrix.

(3) Alice and Bob perform information reconciliation and channel-state estimation on the second set of variables. After reconciliation, Bob computes matching code rate R_{b3} of the third set of variables, according to the channel-state estimation results of the second set of variables.

(4) Bob computes the number of punctured bits and shortened bits, according to R_{b3}. The code-word bits with lower decoding reliability are selected as the deletion positions, and information bits with lower decoding reliability are selected as the shortened-bit positions. The process is shown in Fig. 3.Setting the code rate as $R_{b2} = K_2/N_2$, the code words of the second group of initial variables have a code rate of R'_{b3} after puncturing r bits:

$$R'_{b3} = \frac{K_2}{N_2 - r}. \tag{12}$$

Punctured bits are not used for actual transmission, and these bit channels are considered channels with a capacity of 0. Therefore, the receiver can assign the LLRs of the punctured-bit positions to 0. Since punctured bits cannot provide any helpful information during decoding initialization, it increases the difficulty of error correction, and thus, increases the code rate equivalently. The code rate will be changed to R'_{b3} by adding shortened bits of length s:

$$R'_{b3} = \frac{K_2 - s}{N_2 - s}. \tag{13}$$

Bob makes public the shortened-bit positions and value. Since the encoder and decoder know the shortened bits in advance, these bit channels are considered channels with a capacity of 1, equivalent to transmission through a noiseless channel. Hence, the LLRs of shortened-bit positions tend to infinity (or, in practice, sufficiently large values) when decoding. With the appropriate addition of puncturing and shortening bits to the mother code, the code rate for the third set of variables will be changed to R''_{b3}:

$$R''_{b3} = \frac{K_2 - s}{N_2 - r - s} \cong R_{b3}. \tag{14}$$

(5) Repeat steps 3 and 4. The code rate of the subsequent set of variables is adjusted after the matching code rate, R_b, is computed using the channel-state estimation result of the previous set of variables. Bob passes the adjusted code word to Alice through the virtual BIAWGN channel for error correction.

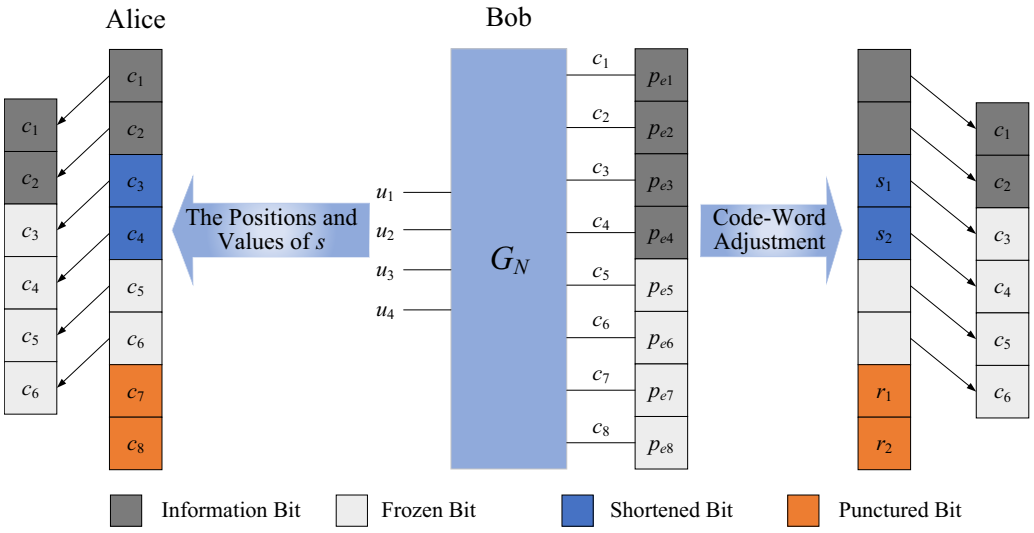

FIG. 3. Rate-adaptive reconciliation model based on decoding reliability. u_1–u_4 are the information bits to be encoded, c_1–c_8 are the encoded code-word bits, p_{e1}–p_{e8} are the reliability values corresponding to each code-word bit, s_1–s_2 are shortened bits, and r_1–r_2 are punctured bits. G_N, generator matrix.

IV. EXPERIMENTAL RESULTS

The change of the channel state affects the reconciliation performance, so it is necessary to adjust the polar-code rate according to the change of the channel state to maintain the stability of the system's information reconciliation. Therefore, the validity and accuracy of real-time channel-state estimation is the premise of rate adaptation. In a practical experiment, the system's noise-variance change over time is tested. Figure 4 shows the actual noise variance compared to the estimated noise variance. Figure 4(a) shows that the estimated values of the adjacent two sets of

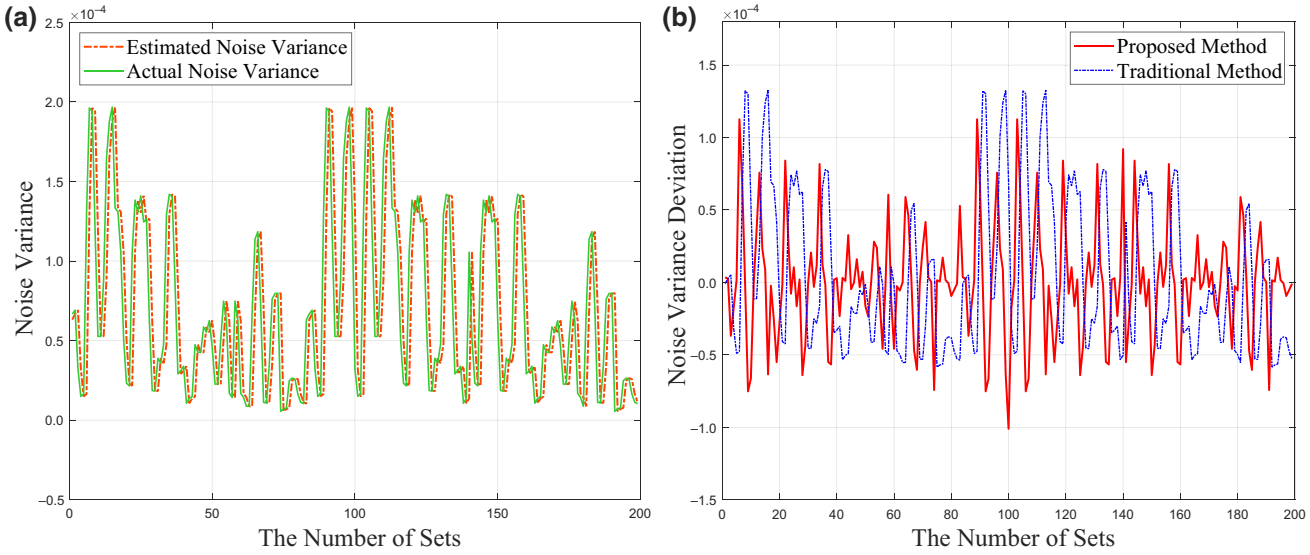

FIG. 4. Actual noise variance versus estimated noise variance. Abscissa represents the number of variable sets tested in the experiment. Ordinate of (a) represents noise variance. Solid line in (a) is the actual noise variance of each group of variables calculated by Eq. (3). Dotted line in (a) is the channel-state estimation proposed in this paper (Alice sends the coherent states to Bob repeatedly and randomly. After Bob receives them, both parties disclose the partial initial variables for the first time to estimate the channel state. Starting from the remaining initial variables, the channel state is estimated using the variables after reconciliation). Ordinate of (b) represents the deviation between actual noise variance and estimated noise variance. Dotted line in (b) shows the deviation of noise variance calculated by the traditional method (after Bob receives all variables, Alice and Bob randomly select a certain proportion of variables for channel-state estimation) from actual noise variance. Solid line in (b) shows the deviation of noise variance calculated by the proposed method from actual noise variance.

data are very close to the actual values, indicating that the channel-state estimation method designed in this scheme is effective. Figure 4(b) compares the deviation of the noise variance estimated by the traditional method [10] and the method in this paper relative to the actual noise variance. The deviation calculation method is $\sigma^2_{z\,\mathrm{real}} - \sigma^2_{z\,\mathrm{est}}$, where $\sigma^2_{z\,\mathrm{real}}$ represents the actual noise variance and $\sigma^2_{z\,\mathrm{est}}$ represents the estimated noise variance. Furthermore, Fig. 4(b) also indicates that the deviation between the traditional channel-state estimation method (after Bob receives all variables, Alice and Bob randomly select a certain proportion of variables for parameter estimation) and the channel-state estimation method proposed by this scheme are less than 1.5×10^{-4}, indicating that this scheme is effective and feasible.

It is known from Eq. (1) and Fig. 1 that the information-reconciliation performance is mainly reflected in the reconciliation efficiency and FER. Therefore, we explore the performance of the proposed rate-adaptive reconciliation scheme in terms of the reconciliation efficiency and FER. A report in the literature [17] proves that the higher the dimension of multidimensional reconciliation, the better the reconciliation performance. However, due to the construction of the orthogonal matrix, the highest dimension is limited to eight dimensions [17], so eight-dimensional reconciliation, i.e., $d = 8$, is chosen. The systematic polar code with an 8-bit CRC code as the outer code is used for the experiment. We set the search width, L, of the CA SCL to 16. Figure 5 compares the FER performance of the proposed scheme and the previous scheme [26], when the target reconciliation efficiency is above 98 % in the channel with different SNRs. According to Fig. 5, the FER performance of this paper's scheme is better

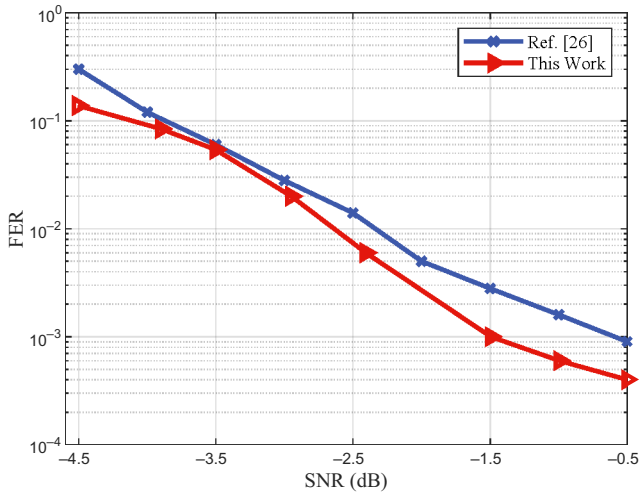

FIG. 5. FERs under the channel with different SNRs when the target reconciliation efficiency is above 98 %. Solid line with crosses results from the previous scheme [26]. Solid line with triangles results from the scheme proposed in this paper.

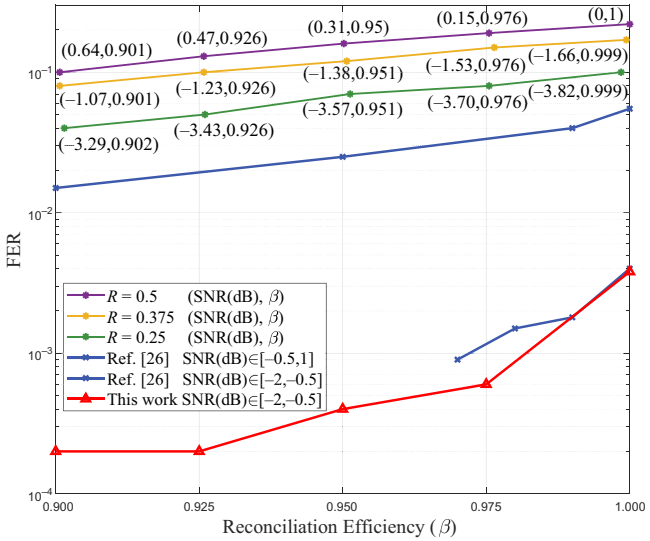

FIG. 6. FERs under different reconciliation efficiencies. Solid line with asterisk results from the traditional scheme [36], corresponding to the code rates $R = 0.5$, $R = 0.375$, and $R = 0.25$, respectively, from top to bottom. Coordinates (SNR(dB), β) on the asterisk represent the SNR and reconciliation efficiency. Three lines from bottom to top are rate-adaptive reconciliation schemes. Solid line with crosses results from the previous scheme [26], and solid line with triangles results from the scheme proposed in this paper.

than that of the previous scheme, regardless of the SNR. When the SNR is −0.5 dB, the FER reaches 4×10^{-4}. In addition, Fig. 6 shows the FER comparison between the traditional fixed-code-rate reconciliation [36], the rate-adaptive reconciliation scheme designed in the previous scheme [26], and the rate-adaptive reconciliation scheme proposed in this paper when the reconciliation efficiency is within 90 %, where $N = 512$ and the number of frames is 10^4. According to Fig. 6, although a lower code rate can give a better FER performance, when the reconciliation efficiency increases, the FER of the traditional fixed-code-rate reconciliation increases. Moreover, the rate-adaptive reconciliation scheme proposed in this paper has a better reconciliation performance than that of the previous scheme. When the reconciliation efficiency is within 90 %, the FER of this scheme is as low as 10^{-2} and 10^{-4}.

Figure 7 presents the secret-key-rate distinction between the traditional fixed-code-rate reconciliation scheme, the rate-adaptation scheme [26], and the proposed rate-adaptation scheme with respect to the transmission distance of the CV QKD system. The fixed-code-rate reconciliation scheme adopts the reconciliation efficiency when FER = 0.01, and the rate-adaptive scheme adopts the reconciliation efficiency when FER = 0.001. Here, we also compare the secret-key rate with the theoretical key-rate curve of the reconciliation efficiency, $\beta = 1$, and Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound [37],

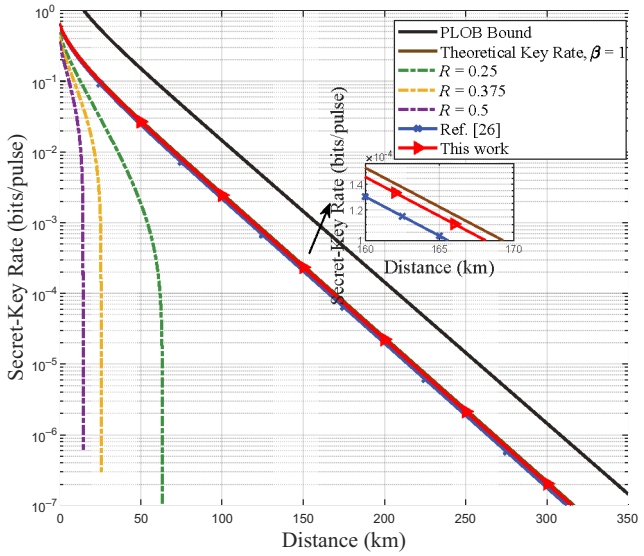

FIG. 7. Finite-size secret-key rate versus distance. Dotted line results from the traditional fixed-code-rate reconciliation scheme [36], corresponding to code rates $R = 0.5$, $R = 0.375$, and $R = 0.25$, respectively, from left to right. Solid black line represents the PLOB bound [37], solid brown line represents the theoretical key-rate curve with reconciliation efficiency $\beta = 1$, solid line with crosses results from the previous scheme [26], and solid line with triangles results from the scheme proposed in this paper. Security parameters are as follows: excess noise is 0.01, η is 0.6, standard loss of a single-mode optical fiber cable is 0.2 dB/km, and electric noise is 0.01.

i.e., the fundamental limit of repeaterless quantum communication. In contrast, the rate-adaptive reconciliation scheme proposed in this paper offers more advantages for practical applications of the CV QKD system.

V. CONCLUSION

Currently, the relatively mature CV QKD technology is gradually moving towards practical commercial and networking applications, and its transmission environment is becoming more and more complex. With the increase in the secret-key rate and transmission distance, the system has higher and higher requirements for postprocessing performance. In particular, the constraints of reconciliation efficiency and frame-error rate on information reconciliation are the critical problems of postprocessing that need to be solved urgently. Furthermore, the fluctuation of the channel characteristics in the existing system also causes the reconciliation performance to decrease. Therefore, a rate-adaptive-key reconciliation scheme with polar codes is proposed for information reconciliation of the CV QKD system, which can achieve a lower FER in the fluctuating channels than the previous scheme. In particular, the scheme estimates the channel state after information reconciliation to calculate the signal-to-noise ratio to determine the matching code rate. Finally, the positions of punctured bits and shortened bits are determined based on the decoding reliability of the polar code to achieve the goal of adaptively adjusting the code rate, thereby ensuring information-reconciliation performance under fluctuating channels. Compared with the previous scheme, this scheme can evaluate the system's channel state in real time, providing the realization basis for subsequent code-rate-adaptive reconciliation. Furthermore, a lower frame-error rate can be obtained between SNRs of -0.5 and -4.5 dB, and the frame-error rates are as low as 10^{-2} and 10^{-4} when the reconciliation efficiency is within 90 %. Data processing in this paper is completed on a CPU platform. The limited computing resources of the CPU limit the optimization of the decoding algorithm, so the speed cannot meet the real-time requirements of the system. A graphics processing unit (GPU) supports large-scale parallel operations and has abundant computing and storage resources. In future work, the GPU platform can be used to improve the system's performance. In addition, artificial intelligence can also be applied to postprocessing to complete many calculations and algorithmic reasoning functions.

ACKNOWLEDGMENTS

This work is supported by the National Natural Science Foundation of China (Grant No. 62071381), Shaanxi Provincial Key R&D Program General Project (2022GY-023), and ISN 23rd Open Project (ISN23-06) supported by the State Key Laboratory of Integrated Services Networks (Xidian University).

APPENDIX A: MAPPING-FUNCTION CALCULATION

The core idea of multidimensional reconciliation is to reformulate the attenuated physical Gaussian channel into a virtual BIAWGN channel. Here, we consider an eight-dimensional reconciliation as an example to introduce the multidimensional reverse reconciliation method. First, Alice and Bob divide the first set of continuous variables x and y, i.e., $x = (x_1, x_2, \ldots, x_8)^T$ and $y = (y_1, y_2, \ldots, y_8)^T$. The initial variables can be combined sequentially or randomly. Then, Alice and Bob normalize their Gaussian variables x and y to x' and y', respectively. Next, Alice and Bob normalize their Gaussian variables to a unit sphere, as follows:

$$x' = x/\|x\|, \|x\| = \sqrt{\langle x, x\rangle}, \tag{A1}$$

$$y' = y/\|y\|, \|y\| = \sqrt{\langle y, y\rangle}. \tag{A2}$$

The vectors x' and y' are uniformly distributed on the unit sphere $\mathbb{S}^7$ of euclidean space $\mathbb{R}^8$. Bob randomly generates a group of binary sequence c with uniform distribution and

maps them to the unit sphere:

$$(c_1, c_2, \ldots, c_d) \to \left(\frac{(-1)^{c_1}}{\sqrt{d}}, \frac{(-1)^{c_2}}{\sqrt{d}}, \ldots, \frac{(-1)^{c_d}}{\sqrt{d}}\right) = c'. \tag{A3}$$

Next, Bob computes the rotation-mapping function from y' to c' on the 8-dimensional unit sphere, which satisfies $M\left(y', c'\right) y' = c'$. The calculation method of the rotation-mapping function, $M\left(y', c'\right)$, is as follows:

$$M\left(y', c'\right) = \sum_{i=1,2,\ldots 8} \alpha_i \left(y', c'\right) A_i, \tag{A4}$$

where $\alpha_i = (A_i y' | c')$; $(A_1, A_2, \ldots, A_8)$ is a set of orthogonal matrices of $\mathbb{R}^{8\times 8}$ and is provided [17] such that $A_1 = I_8$, for $i, j > 1, A_i, A_j = -2\delta_{i,j} I_8$. $(A_1 y', A_2 y', \ldots, A_8 y')$ is an orthonormal basis of $\mathbb{R}^8$ for any $y' \in \mathbb{S}^7$. Then, for any $c', y' \in \mathbb{S}^7$, $\left(\alpha_1\left(y', c'\right), \alpha_2\left(y', c'\right), \ldots, \alpha_8\left(y', c'\right)\right)$ are the coordinates of c' in the basis $(A_1 y', A_2 y', \ldots, A_8 y')$. Subsequently, Bob shares $M\left(y', c'\right)$ with Alice through the classical authentication channel together with other side information, i.e., $\|y\|$, and parameters of polar codes. With the received side information, Alice can map her Gaussian variable x' to v:

$$v_i = M\left(y', c'\right) x', \tag{A5}$$

After the above steps, the virtual BIAWGN channel is established. Then, Alice uses the polar codes to recover c from v. Since the rotated discrete variables obey a uniform distribution, it maximizes the distance between data, eliminates the problem that a large number of Gaussian distributions are concentrated near zero and are easily disturbed by noise, and improves the discrimination between data.

APPENDIX B: CRC-AIDED DECODING OF POLAR CODES

In the SCL decoding process, there are $l \in \{1, 2, \ldots, N\}$ paths for decoding and searching at the same time. For any path l and any transmitted bit $u_i (i \in 1, 2, \ldots, N)$, the corresponding path metric value is defined as follows, when considering that the decoding process includes information bits and frozen bits [31]:

$$PM_l^{(i)} = \begin{cases} PM_l^{(i-1)}, \\ \quad u_i \text{ is information or frozen bit and } \hat{u}_i[l] = \delta\left(L_N^i[l]\right), \\ PM_l^{(i-1)} + \left|L_N^{(i)}[L]\right|, \\ \quad u_i \text{ is information or frozen bit and } \hat{u}_i[l] \neq \delta\left(L_N^i[l]\right), \\ +\infty, \\ \quad u_i \text{ is frozen bit and incorrect value}, \end{cases} \tag{B1}$$

where $\delta(x) = 1/2\,(1 - \text{sign}(x))$ and $PM_l^{(0)} = 0$. The decision rule of the SCL is

$$\hat{u}_i = \delta\left(L_N^{(i)}\left(y_1^N, \hat{u}_1^{i-1}\right)\right). \tag{B2}$$

The CA SCL decoding adds a sequence of CRC check codes to the message-bit sequence. The SCL decoding obtains L search paths by standard decoding. Then the best decoding path is output after selecting these L search paths with the a priori information that "the correct information bits can pass the CRC checksum." The length of the polar code is N, the length of the CRC check code is m, the length of the information bit of the polar code is K, and the length of the encoded information bit is k; there is $K = k + m$. The code rate of the polar code is still $R = K/N$. Let $L^{(i)}$ denote the set of candidate paths corresponding to level i of the code tree in the SCL decoder. The CRC-aided SCL decoding with the size of list, L, denoted by the CA SCL (L), can be described as follows [30].

Initialize one null path included in the initial list, and set its metric to 0, i.e., $L^{(0)} = \{\phi\}$ and $PM(\phi) = 0$. At the ith level of the code tree, double the number of candidate paths in the list by concatenating bits d_i taking values of 0 and 1, that is,

$$L^{(i)} = \left\{\left(d_1^{i-1}, d_i\right) | d_1^{i-1} \in L^{(i-1)}, d_i \in \{0, 1\}\right\}, \tag{B3}$$

for each $d_1^i \in L^{(i)}$, update the path metric(s). If the number of paths in the list is no more than L, skip this step; otherwise, reserve L best paths with the largest metrics and

delete the others. Repeat to double the number of candidate paths, and search to reserve the best path until level N is reached. Then, the paths in the list are examined one by one with decreasing metrics. The decoder outputs the first path detected by the CRC as the estimation sequence. If no such path is found after traversing $L^{(N)}$, the algorithm declares a decoding failure.

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

[2] A. Acin, S. Massar, and S. Pironio, Efficient quantum key distribution secure against no-signalling eavesdroppers, New J. Phys. **8**, 126 (2006).

[3] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Theor. Comput. Sci. **560**, 7 (2014).

[4] N. J. Cerf, M. Levy, and G. Van Assche, Quantum distribution of Gaussian keys using squeezed states, Phys. Rev. A **63**, 052311 (2001).

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

[6] T. A. Eriksson, T. Hirano, B. J. Puttnam, G. Rademacher, R. S. Luís, M. Fujiwara, R. Namiki, Y. Awaji, M. Takeoka, N. Wada, and Masahide Sasaki, Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 tbit/s data channels, Commun. Phys. **2**, 9 (2019).

[7] Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, Long-Distance Continuous-Variable Quantum Key Distribution over 202.81 km of Fiber, Phys. Rev. Lett. **125**, 010502 (2020).

[8] H.-M. Chin, N. Jain, U. L. Andersen, D. Zibar, and T. Gehring, Digital synchronization for continuous-variable quantum key distribution, Quantum Sci. Technol. **7**, 045006 (2022).

[9] J. Wu and Q. Zhuang, Continuous-Variable Error Correction for General Gaussian Noises, Phys. Rev. Appl. **15**, 034073 (2021).

[10] A. Leverrier, F. Grosshans, and P. Grangier, Finite-size analysis of a continuous-variable quantum key distribution, Phys. Rev. A **81**, 062343 (2010).

[11] M. Zou, Y. Mao, and T.-Y. Chen, Optimal parameter estimation without consuming raw keys for continuous-variable quantum key distribution, J. Phys. B: At., Mol. Opt. Phys. **55**, 155502 (2022).

[12] G. Van Assche, J. Cardinal, and N. J. Cerf, Reconciliation of a quantum-distributed Gaussian key, IEEE Trans. Inf. Theory **50**, 394 (2004).

[13] X. Wang, H. Wang, C. Zhou, Z. Chen, S. Yu, and H. Guo, Continuous-variable quantum key distribution with low-complexity information reconciliation, Opt. Express **30**, 30455 (2022).

[14] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels, Phys. Rev. Lett. **77**, 2818 (1996).

[15] Y. Luo, Y. Li, J. Yang, L. Ma, W. Huang, and B. Xu, in *Quantum and Nonlinear Optics VII*, Vol. 11558 (SPIE, 2020), p. 25.

[16] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Continuous Variable Quantum Cryptography: Beating the 3 dB Loss Limit, Phys. Rev. Lett. **89**, 167901 (2002).

[17] 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).

[18] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Long-distance continuous-variable quantum key distribution with a gaussian modulation, Phys. Rev. A **84**, 062317 (2011).

[19] 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).

[20] C. Zhou, X. Wang, Z. Zhang, S. Yu, Z. Chen, and H. Guo, Rate compatible reconciliation for continuous-variable quantum key distribution using raptor-like LDPC codes, Sci. China Phys. Mech. Astron. **64**, 260311 (2021).

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

[22] P. Jouguet and S. Kunz-Jacques, High performance error correction for quantum key distribution using polar codes, Inf. Comput. **14**, 329 (2014).

[23] A. Nakassis and A. Mink, in *Quantum Information and Computation XII*, Vol. 9123 (SPIE, 2014), p. 32.

[24] X. Wang, Y. Zhang, Z. Li, B. Xu, S. Yu, and H. Guo, Efficient rate-adaptive reconciliation for CV-QKD protocol, Quantum Inf. Comput. **17**, 1123 (2017).

[25] B. Li, D. Tse, K. Chen, and H. Shen, in *2016 IEEE International Symposium on Information Theory (ISIT)* (IEEE, 2016), p. 46.

[26] M. Zhang, H. Hai, Y. Feng, and X. Jiang, Rate-adaptive reconciliation with polar coding for continuous-variable quantum key distribution, Quantum Inf. Process. **20**, 318 (2021).

[27] 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).

[28] X. Wang, Y. Zhang, S. Yu, and H. Guo, High efficiency postprocessing for continuous-variable quantum key distribution: Using all raw keys for parameter estimation and key extraction, Quantum Inf. Process. **18**, 264 (2019).

[29] G. Chai, Z. Cao, W. Liu, S. Wang, P. Huang, and G. Zeng, Parameter estimation of atmospheric continuous-variable quantum key distribution, Phys. Rev. A **99**, 032326 (2019).

[30] K. Niu and K. Chen, CRC-aided decoding of polar codes, IEEE Commun. Lett. **16**, 1668 (2012).

[31] A. Balatsoukas-Stimming, M. B. Parizi, and A. Burg, LLR-based successive cancellation list decoding of

polar codes, IEEE Trans. Signal Process. **63**, 5165 (2015).

[32] S.-Y. Chung, T. J. Richardson, and R. L. Urbanke, Analysis of sum-product decoding of low-density parity-check codes using a gaussian approximation, IEEE Trans. Inf. Theory **47**, 657 (2001).

[33] P. Trifonov, Efficient design and decoding of polar codes, IEEE Trans. Commun. **60**, 3221 (2012).

[34] E. Arikan, Systematic polar coding, IEEE Commun. Lett. **15**, 860 (2011).

[35] L. Li, Z. Xu, and Y. Hu, Channel estimation with systematic polar codes, IEEE Trans. Vehicular Technol. **67**, 4880 (2018).

[36] S. Zhao, Z. Shen, H. Xiao, and L. Wang, Multidimensional reconciliation protocol for continuous-variable quantum key agreement with polar coding, Sci. CHINA Phys., Mech. Astron. **61**, 090323 (2018).

[37] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8**, 15043 (2017).