Information reconciliation for phase shift keying discrete modulation continuous-variable quantum key distribution

Zhenguo Lu,[1,2] Weilin Liu,[1,2] Yu Zhang,[1,2] Zengliang Bai,[3] and Yongmin Li[1,2,4,*]

[1]*State Key Laboratory of Quantum Optics Technologies and Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan 030006, China*

[2]*Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan 030006, China*

[3]*School of Information, Shanxi University of Finance and Economics, Taiyuan 030006, China*

[4]*Hefei National Laboratory, Hefei 230088, China*

(Received 2 July 2025; accepted 19 November 2025; published 9 December 2025)

Discrete modulation continuous-variable quantum key distribution protocols are compatible with modern coherent optical communication technologies and devices. As a key part of the protocol, the performance of information reconciliation directly affects the secret key rate and transmission distance. Herein, we propose a reconciliation scheme for hard-decision strategy–based discrete modulation continuous-variable quantum key distribution protocol with eight-phase shift keying by combining slice reconciliation and raptor-like low-density parity-check (RL-LDPC) codes. We design the optimal binary sequence encoding of the discretized values of the receiver and sender, which reduce both the number of levels of error correction and the reconciliation complexity. In order to reduce the frame error rate, both the degree distribution and the size of the base matrix of RL-LDPC code is optimized. Simulation results show that the proposed scheme can reach reconciliation efficiencies of 92.05% and 93% with frame error rates of 6.2% and 11.7% at the signal-to-noise ratio of 0.15, respectively. At these points, the key rates can reach 0.0193 and 0.0195 bits/pulse, respectively.

DOI: 10.1103/kgpx-krj7

I. INTRODUCTION

Quantum key distribution (QKD) employs the fundamental principles of quantum mechanics and can provide the information-theoretically secure sharing of secret keys between two parties [1–3]. According to the information encoding carriers and detection methods, two types of approaches have been proposed: discrete-variable QKD (DV-QKD) and continuous-variable QKD (CV-QKD). The first one uses single-photon detection and has the advantages of a long transmission distance and relatively simple information reconciliation [4–10]. In contrast, the latter encodes information on the quadratures of quantized optical field and can provide high secret key rates in metropolitan areas with coherent detection. Discrete modulation CV-QKD uses a finite discrete constellation in the phase space to encode the key information, which is compatible with modern coherent optical communication technologies and devices [11–16].

In typical CV-QKD protocols, Alice prepares the quantum states and sends them to Bob via an insecure quantum channel. After Bob receives the states, he measures them using homodyne (heterodyne) detection. After the key sifting, Alice and Bob share a series of raw keys. However, the raw keys between them will inevitably differ because of attenuation and noise arising from the quantum channel and imperfect quantum state preparation and measurements. In this case, information reconciliation is necessary to correct the inconsistency of the raw keys [17] and enable the sharing of identical raw key information. Information reconciliation can be classified into direct and reverse reconciliation based on the criteria that Alice or Bob is viewed as the benchmark. In direct reconciliation, the system cannot generate a secure key when the transmittance of the quantum channel is less than 0.5 [18]. Reverse reconciliation can break this limit and achieve much longer transmission distances [19].

For discrete modulation CV-QKD protocols [20–26], two decision strategies exist: hard-decision strategy and soft-decision strategy [27]. For the first one, Bob immediately discretizes his measurement outcome and the resulting discrete values will form the raw key. In this case, one can rely on the entropy accumulation theorem to obtain a lower bound on the conditional smooth min-entropy of the raw key corresponding to Bob's discrete outcome, and prove the security of the protocols against the most general attacks. For the soft-decision strategy–based quadrature phase shift keying (QPSK) modulation, information reconciliation can be reduced to a channel coding task over a binary-input additive white Gaussian-noise (BI-AWGN) channel. For modulations with a large constellation that approximate to a Gaussian modulation, one can exploit the multidimensional (MD) reconciliation [15,28–30]. It eliminates coordinates with small absolute values by performing a rotation operation on the raw key vectors, and exhibits good information reconciliation performance at low signal-to-noise ratios (SNRs). Recently, the information reconciliation for hard-decision strategy–based QPSK modulation has been implemented using LDPC codes [26] and polar codes [31] over a binary symmetric channel.

*Contact author: yongmin@sxu.edu.cn

Notice that the performance of M-PSK discrete modulation CV-QKD protocol improves with the size of the signal constellations M [32]. However, the information reconciliation problem is more complex to design and implement for signal constellations larger than four and has not been resolved.

Slice reconciliation has been employed in the information reconciliation of Gaussian modulation CV-QKD protocols at relatively high SNRs [33,34]. Notice that the slice reconciliation discretizes Bob's data that is similar to the hard-decision strategy. Therefore, it is compatible with the information reconciliation of the hard-decision-based discrete modulation CV-QKD protocols. However, the quantization step of the traditional slice reconciliation for Gaussian variables is no longer applicable, because the hard decision of the discrete modulation CV-QKD protocol requires that Bob immediately discretizes his measurement outcomes. The criteria of the discretization depends on the signal constellation, parameters of the quantum channel, detection efficiency and noise, etc.

Multiedge-type low-density parity-check (MET-LDPC) codes have good error correction performance that is closer to the Shannon limit at low code rates [35]. However, the optimal design of the degree distributions of MET-LDPC codes at arbitrary code rates is a challenge and only a few optimal degree distributions have been designed at present. Several rate-adaptive reconciliation techniques have been proposed such as puncturing and shortening [36], rateless reconciliation protocols [37], and the raptor-like low-density parity-check (RL-LDPC) codes [38]. RL-LDPC codes can dynamically adjust the code rate within a certain range based on the degree distribution of the fixed code rate while maintaining efficient error correction performance [39,40].

In this paper, we propose a slice reconciliation scheme for hard-decision discrete modulation CV-QKD protocol with eight-phase shift keying (8-PSK). First, we establish the mutual information computation procedure for the m-level quantization. Next, we design the optimal binary sequence encoding of the discretized values. This design is critical as it minimizes the required error correction levels, reduces reconciliation complexity, and prevents decoding failures caused by zero initial LLR values. By optimizing the degree distribution and base matrix of the RL-LDPC codes based on the degree distributions of the MET-LDPC code at a code rate of 0.1, we construct a RL-LDPC code with code rates 0.122 and 0.1235 that are close to the optimal code rate of 0.1279. This method effectively decreases the frame error rate (FER) of RL-LDPC codes. To further decreases the FER, we employ the erasure searching postprocessor. The proposed reconciliation scheme can reach reconciliation efficiencies of 92.05% and 93% with FERs of 6.2% and 11.7% at a SNR of 0.15. At these points, the key rates can reach 0.0193 and 0.0195 bits/pulse, respectively.

The rest of this paper is organized as follows: In Sec. II, we present the hard-decision discrete modulation CV-QKD protocol with an 8-PSK modulation. In Sec. III, we present the details of the reconciliation scheme: the slice reconciliation architecture, the calculation of the mutual information and the quantification methods, and the MLC-MSD structure. In Sec. IV, we describe the design of RL-LDPC codes. In Sec. V, we present the performance of the proposed reconciliation scheme. Finally, we give a summary in Sec. VI.

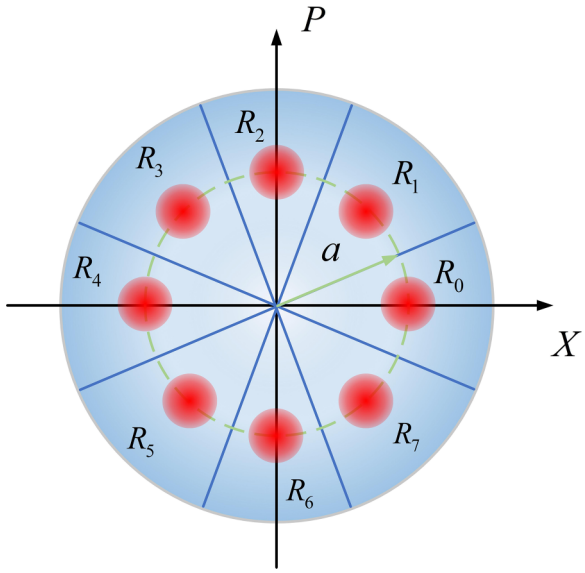

FIG. 1. Schematic of the 8-PSK discrete modulation CV-QKD with hard decision. $R_j (j = 0, 1, 2, 3, 4, 5, 6, 7)$ represents the quantization regions.

II. DISCRETE MODULATION CV-QKD PROTOCOL WITH M-PSK MODULATION AND HARD DECISION

In Fig. 1, a schematic diagram of 8-PSK discrete modulation CV-QKD protocol with hard decision is shown [32]. In the quantum part of the protocol, Alice generates a uniform random number $x \in \{0, 1, 2, 3, 4, 5, 6, 7\}$ and prepares the coherent state $|\alpha_x\rangle = |\alpha e^{jx\pi/4}\rangle$ according to the value of x and sends it to Bob via an insecure quantum channel. Here, α denotes the amplitude of the coherent state. Bob uses heterodyne detection to measure the received state and get a measurement outcome $y = x_B + ip_B = |y|e^{i\theta}$, where $\theta \in [-\frac{\pi}{8}, \frac{7\pi}{8})$. Repeat the above two steps N times to collect sufficient data for both parties.

After the quantum phase of the protocol, Alice and Bob implement the data postprocessing part of the protocol including parameter estimation, key map, error correction, and privacy amplification to extract the shared secure key. For key mapping of the reverse reconciliation protocol, Bob discretizes his measurement outcome y and obtains the discretized value z according to the following criterion:

$$z = \begin{cases} j, & \text{if} \quad \theta \in \left[\frac{(2j-1)\pi}{8}, \frac{(2j+1)\pi}{8}\right) \\ \perp, & \text{otherwise} \end{cases}, \tag{1}$$

where $j \in \{0, 1, 2, 3, 4, 5, 6, 7\}$. Bob locates the positions where he gets the value $\perp$ and then they discard the corresponding data. At this stage, Alice's raw key string $\vec{X}$ consists of the remaining random number x, and Bob's raw key string $\vec{Z}$ consists of the remaining discretized value z.

III. LOW-COMPLEXITY SLICE RECONCILIATION FOR THE M-PSK DISCRETE MODULATION CV-QKD WITH HARD DECISION

A. Slice reconciliation

Figure 2 depicts the slice reconciliation scheme for the M-PSK discrete modulation CV-QKD with hard decision.

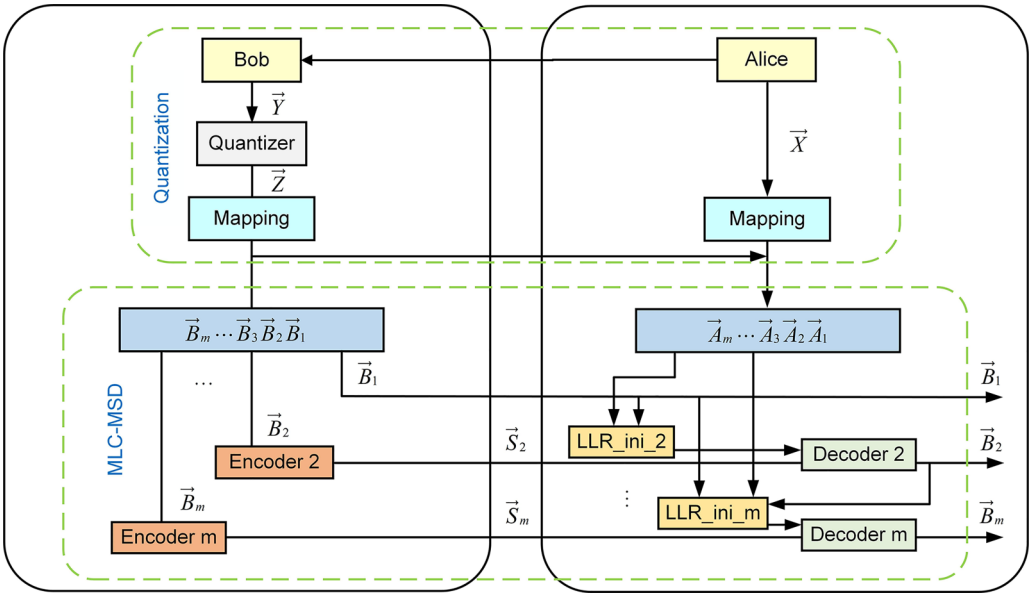

FIG. 2. Slice reconciliation scheme for the M-PSK discrete modulation CV-QKD with hard decision.

It comprises two steps: quantization and multilevel coding and multistage decoding (MLC-MSD). In the first step, Bob quantizes his measurement outcome y and obains the discretized value z using the method in Sec. II. The raw key string $\vec{Z}$ is successively mapped to a set of m-level binary strings $\vec{B}_m \cdots \vec{B}_3\vec{B}_2\vec{B}_1$. Alice directly maps her raw key string $\vec{X}$ into an m-level binary string $\vec{A}_m \cdots \vec{A}_3\vec{A}_2\vec{A}_1$ with the same mapping rules as Bob. Next, for reverse reconciliation, Bob employs multilevel coding (MLC) to encode the quantized binary strings at each level and generates the syndromes $\vec{S}_1\vec{S}_2\vec{S}_3 \cdots \vec{S}_m$, which are sent to Alice via the classical channel. Note that the levels corresponding to the less significant bits may be directly disclosed because they have low mutual information and small effect on the reconciliation efficiency. Alice then performs multistage decoding (MSD) using the received syndromes and her binary strings. The decoding result of each level is used as the initial information for the decoding process of the next level in the MSD. Eventually, the two parties obtain identical bit strings $\vec{B}_m \cdots \vec{B}_3\vec{B}_2\vec{B}_1$ for privacy amplification to extract the secret key. The slice reconciliation efficiency can be expressed as follows:

$$\beta = \frac{H(Z) - m + \sum_{i=1}^{m} R_i}{I(X,Z)}, \tag{2}$$

where $H(Z)$ is the information entropy of z, R_i is the code rate of the error-correcting code of level i, m is the number of levels for MLC-MSD, and $I(X,Z)$ is the classical mutual information between X and Z.

B. Quantization

The average mutual information between Alice and Bob is given by

$$I = \sum_{k=0}^{K-1}\sum_{j=0}^{J-1} Q(k)\tilde{P}(z_j|x_k)\log_2\left\{\frac{\tilde{P}(z_j|x_k)}{\sum_{i=0}^{K-1} Q(i)\tilde{P}(z_j|x_i)}\right\}, \tag{3}$$

where x_k denotes Alice's raw key and $k \in \{0, 1, \ldots, 7\}$ marks the value of the raw key, $Q(i)$ denotes the probability that Alice's raw key is i, and z_j denotes Bob's raw key, where $j \in \{0, 1, \ldots, 7\}$. For the M-PSK modulation, the phase space is evenly partitioned into $M = 2^m$ intervals. For $M = 8$ as shown in Fig. 1, the probability that Bob's quantized value is z conditioned on Alice's data x is given by

$$\widetilde{P}(z \mid x) = \int_0^{\infty} r\,dr \int_{(2z-1)\pi/4}^{(2z+1)\pi/4} P(re^{i\theta} \mid x)\,d\theta, \tag{4}$$

where

$$P(y|x) = \frac{1}{2\pi\,\delta}\exp\left[-\frac{\left|y - \sqrt{T\eta}\,\alpha e^{\frac{i\pi x}{4}}\right|^2}{2\,\delta}\right], \tag{5}$$

$$y = re^{i\theta}, \tag{6}$$

where δ denotes the noise variance in the quantum channel, r is the amplitude of y, T denotes the channel transmittance, and η denotes the detection efficiency at the receiver. In the mapping stage, both the discretized value z and Alice's data x are mapped into binary strings and the mapping rule affects the distribution of the mutual information on different levels (but does not affect the total mutual information). In addition, the probability of the current-level bit being 0 or 1 depends on the already determined values of the lower-level bits. Therefore, the mutual information at each level depends on both the SNR and mapping rules and is expressed as follows:

$$\begin{aligned} I^i &= I(Z;X^i \mid X^0 \ldots X^{i-1}) \\ &= I(Z;X^i \ldots X^{l-1} \mid X^0 \ldots X^{i-1}) \\ &\quad - I(Z;X^{i+1} \ldots X^{l-1} \mid X^0 \ldots X^i), \end{aligned} \tag{7}$$

where X^i is the ith bit sent by Alice and Z is the quantized value of Bob. Each term in Eq. (7) can be determined by the average mutual information between Alice and Bob using Eq. (3). The total mutual information that depends on the SNR

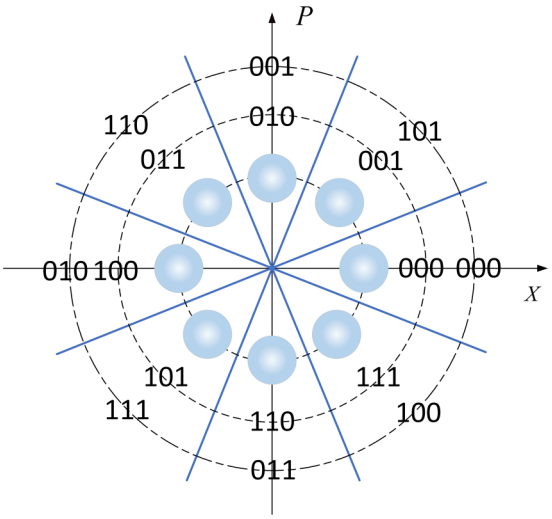

FIG. 3. Sequential and optimized mapping schemes for 8-PSK. The inner and outer rings represent the sequential and optimized mapping methods, respectively.

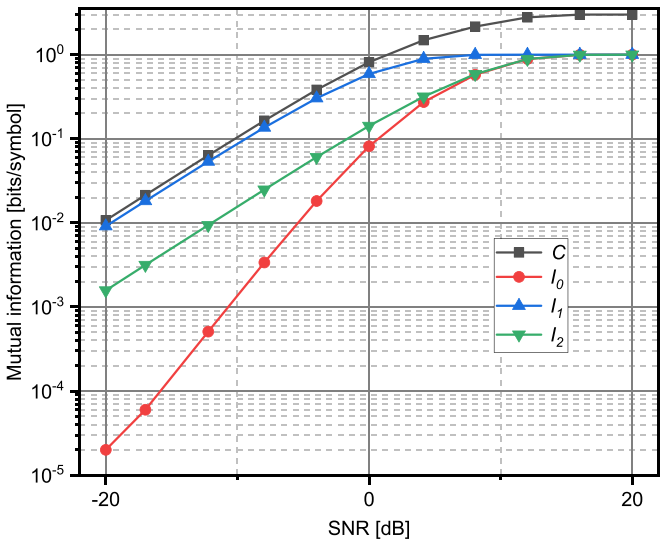

FIG. 4. Simulation results of the mutual information at each level. C denotes the capacity of the channel. (I_2, I_1, I_0) denote mutual information at levels 3, 2, and 1, respectively. I is the total mutual information

can be expressed as [41]

$$I = \sum_{i=1}^{m} I^i. \tag{8}$$

The optimal code rate for level i is given by

$$R_i^{\text{opt}} = 1 - [I^i(\infty) - I^i(s)], \tag{9}$$

where $I^i(s)$ is the mutual information at level i when SNR is s. By using the Eqs. (1)–(8), the reconciliation efficiency β can be determined.

To design the mapping rule, two factors are considered. The first one is minimization of the encoding levels, because the mapping method can determine the distribution of the mutual information on different levels. In this case, if the less significant bits have very low mutual information, Bob can simply directly disclose the entire level to simplify the error correction. The second one is that the mapping method should provide effective values of initial log-likelihood ratio (LLR) for each level. Considering the symmetry of the received state distribution in the phase space for M-PSK modulation, when Alice sends the state $|\alpha_x\rangle$ and the sequential mapping (inner ring in Fig. 3) is adopted, the received quantum states of Bob will fall into the region above or below the x axis with equal probability. Therefore, levels 2 and 3 of the mapped binary strings for Bob's quantized value z take the value of 0 or 1 with the same probability, i.e., the initial LLR for decoding is zero, which degrades the decoding performance.

Herein, we design an optimized mapping rule, as shown in Fig. 3 (the outer ring). The proposed mapping not only reduces the MLC-MSD complexity but also eliminates the decoding failure caused by zero initial LLR values.

Figure 4 shows the conditional mutual information at each level and the total mutual information between Alice and Bob for the additive white Gaussian noise channel. The mutual information (I_2, I_1, I_0) at each level increases with the SNR and eventually converges to 1. The mutual information for different levels satisfy $I_1 > I_2 > I_0$.

Table I lists the mutual information and code rate of each level at SNR of 0.15. The mutual information at levels 2 and 3 dominates the total mutual information, accounting for 82.97% and 15.09%, respectively, whereas the mutual information at level 1 is only 1.94% of total mutual information. Therefore, the bit string of level 1 has a negligible effect on the total information, Bob sends it directly to Alice and only encodes the bit strings of level 2 and 3. In this way, the decoding process can be significantly simplified.

C. MLC-MSD

In the proposed scheme, the MLC-MSD method is employed to perform error correction on the raw key strings of both parties. Bob encodes the bit sequences at each level separately to generate the respective syndromes, which are sent to Alice via a classical public channel. To correct the bit errors to match Bob's bit sequences, Alice employs the syndromes and her data as side information to implement MSD. In the initial stage of the decoding, Alice determines the probability that Bob's quantized value z conditioned on Alice's data x by using Eq. (4). By combining the mapping rule, the probability that each level of z is decoded as 0 or 1 is then determined, and the corresponding LLR is computed by

$$L^{(0,0)}(P_i) = L^{(0,0)} q_{ij} = \log_2 \frac{P_i(0)}{P_i(1)} = \log_2 \frac{\widetilde{P}\{z_i = 0 \mid x_i\}}{\widetilde{P}\{z_i = 1 \mid x_i\}}, \tag{10}$$

TABLE I. Mutual information at each level with SNR of 0.15.

Level	Mutual information	Code rate	Percentage (%)
1	0.0030	0.0031	1.933
2	0.1280	0.1279	82.973
3	0.0233	0.0233	15.094

where $L^{(0,0)}(P_i)$ is the initial LLR value of the ith variable node in layer 0 of LDPC, and $L^{(0,0)}q_{ij}$ is the initial value of the information sent by the ith variable node in layer 0 of LDPC to the jth check node.

At each decoding level, we employ the layered sum-product decoding algorithm to correct the error bits, which gradually approach the correct decoding results through iterative computation [42]. The decoding results of each level are used as side information to the next level to aid in the decoding. Finally, the transmitter and receiver share identical binary sequences.

IV. CONSTRUCTION OF RL-LDPC CODE

The LDPC code significantly affects the reconciliation efficiency and FER of the error correction [43]. In general, the degree distribution is determined for the target code rate by using the density evolution algorithm [44]. The degree distribution of the MET-LDPC code can be expressed as follows:

$$\begin{aligned} \nu(r,x) &= \sum v_i r^b x^d \\ \mu(x) &= \sum \mu_i x^d \end{aligned}, \tag{11}$$

where $\nu(r,x)$ is the degree distribution of the variable nodes, $\mu(x)$ is the degree distribution of the check nodes, v_i is the ratio of the variable node i to the total number of variable nodes, and μ_i is the ratio of the check nodes i to the total number of check nodes. Subsequently, the LDPC code is constructed based on the designed degree distribution using the progressive-edge-growth (PEG) technique [45,46].

The RL-LDPC code is a specialized class of MET-LDPC codes that utilizes the degree distribution parameters of MET-LDPC codes. It not only exhibits near-Shannon-limit coding performance but also the rateless property of Raptor codes. As shown in Fig. 5, the base matrix of the RL-LDPC code consists of four types of submatrices including edge type 1 (A), edge type 2 (B), identity matrix (C), and zero matrix (D). To construct matrix A, the degree distribution of the edge type 1 variable node is extracted from the known MET-LDPC code and used as the degree distribution of matrix A afternormalization. Then, matrix A of the RL-LDPC code is constructed with the PEG algorithm based on this new degree distribution. For matrix B, since it has more rows than columns, the PEG algorithm cannot be used to construct it. To construct matrix B, we normalize the degree distribution of the edge type 2 check node from the MET-LDPC code and use it to generate the transpose of matrix B with the PEG algorithm. Finally, by combining the four matrices A–D, the base matrix of RL-LDPC code is constructed.

The code rate of the RL-LDPC code can be adjusted to achieve the desired target code rate by cutting or expanding the base matrix structure of the RL-LDPC code. The modified code rate is given by

$$R_p = \frac{N-M}{N-p}, \tag{12}$$

$$R_e = \frac{N-M}{N+e}, \tag{13}$$

where R_p is the code rate of the cutted RL-LDPC code, and R_e is the code rate of the expanded RL-LDPC code.

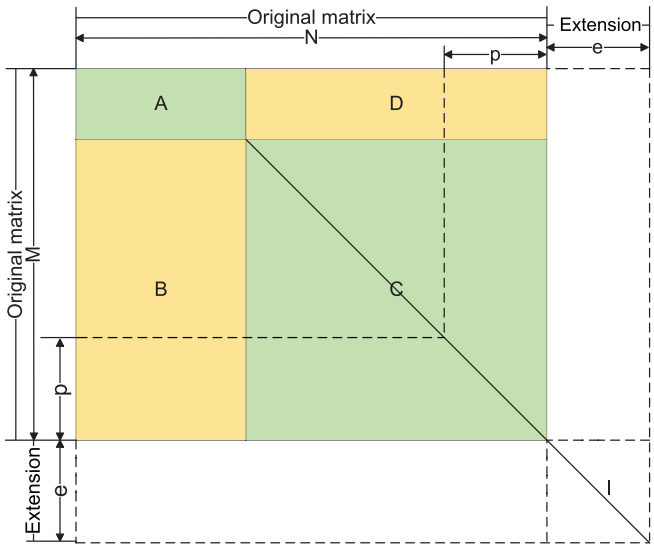

FIG. 5. Schematic of cutting and extending the base matrix of the RL-LDPC code. N and M denote the number of columns and rows of the matrix, respectively. p is the cutting length of the matrix, and e is the expanding length of the matrix. A–D represent the four submatrices of the RL-LDPC code.

Notably, the code rate of the base matrix of RL-LDPC code does not change when the number of columns and rows of the base matrix are adjusted in the same proportion. When the base matrix is cut or expanded, the optimal degree distribution of submatrix B that has a dominant effect on the performance of the RL-LDPC code will vary. To maintain good performance, the degree distribution of the submatrix B should be redesigned. The design of the new degree distribution can refer to the degree distributions of the reference codes with similar code rates.

V. PERFORMANCE SIMULATION AND OPTIMIZATION

In this section, we present the performance simulation and optimization of the proposed reconciliation scheme in the 8-PSK discrete modulation CV-QKD. To this end, the RL-LDPC code with a code rate 0.02 is directly constructed for level 3 based on the degree distributions of the code rate 0.02 [35]. For level 2, the optimal rate is 0.1279 and we construct different codes with code rates of 0.1, 0.122, 0.1235, and 0.125, respectively, based on the degree distribution information of code rate 0.1 and 0.15 [35]. To construct the codes, a base matrix is first designed and then extended using the quasi-cyclic extension algorithm [47,48]. The performance of RL-LDPC code for level 2 is optimized in three ways: the degree distribution of the edge type 2, the base matrix size, and erasure-searching postprocessing (ESPP) [49].

Following the analysis described in Sec. IV, we improve the FER of the RL-LDPC code for level 2 by adjusting the degree distribution of the edge type 2. Figure 6 shows the FER of RL-LDPC codes versus the different degree distributions of edge type 2 [the coefficient t in $\mu(x) = tx_2^2 + (1-t)x_2^3$].The code rates for levels 2 and 3 are (0.122, 0.1235, 0.125) and 0.02, respectively. The FER increases with t and the lowest

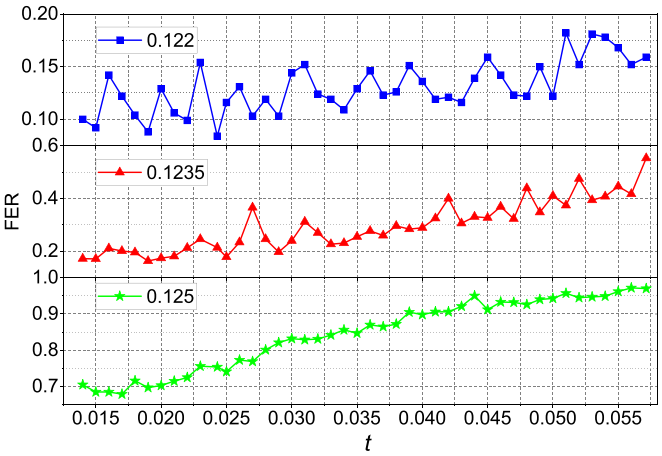

FIG. 6. FER of RL-LDPC codes vs the different degree distributions of edge type 2. The code rates for levels 2 and 3 are (0.122, 0.1235, 0.125) and 0.02, respectively. The corresponding code lengths are 820 000, 810 000, and 800 000, respectively.

FERs of 8.4%, 17.8%, and 68.8% are obtained at $t = 0.0243$, 0.025, and 0.016.

Next, we optimize the base matrix size to improve the FER. For code rates of 0.122, 0.1235, and 0.125, the fixed code lengths are 984 000, 972 000, and 960 000, respectively. Notice that the code rate remains unchanged when the number of columns and rows in the RL-LDPC code is scaled proportionally. Figure 7 shows the FER versus the base matrix sizes for level 2. The results indicate that the FER does not change monotonically with increased base matrix size and there exists an optimal base matrix size at which the FER is minimized. For code rates of 0.122, 0.1235, and 0.125, the optimal base matrix sizes are 1440×1640, 4260×4860, and 4200×4800, and the FERs are 8%, 13.9%, and 57.8%, respectively.

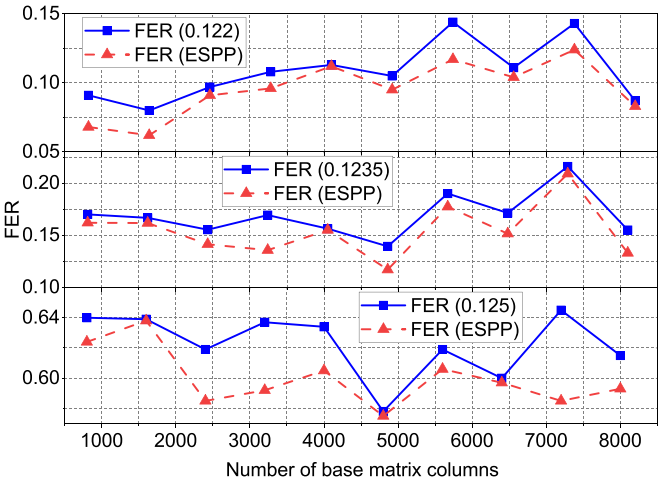

FIG. 7. FER vs the different base matrix sizes of RL-LDPC code for level 2 with (blue solid line) and without (red dashed line) ESPP at fixed code lengths of 984 000, 972 000 and 960 000, respectively. The code rates for levels 2 and 3 are (0.122, 0.1235, 0.125) and 0.02, respectively. The FER for each point is obtained by impleting 1000 simulations.

TABLE II. Performance of the proposed reconciliation scheme.

Code rate (level 2)	Iterations (level 2)	Code rate (level 3)	Iterations (level 3)	β (%)	FER (%)	Key rate (bits/pulse)
0.1	11	0.02	25	77.79	5.2	——
0.122	56	0.02	25	92.05	6.2	0.0193
0.1235	91	0.02	25	93	11.7	0.0195
0.125	140	0.02	25	94	57.8	0.01

To further optimize the reconciliation performance, we exploit ESPP. After running the layered sum-product decoding algorithm, if a decoding error is detected, the ESPP erases the symbol with the lowest LLR in the code word. The erased symbols are then recalculated by solving the linear equations derived from the sparse coefficient matrix. As shown in Fig. 7, the FERs of the information reconciliation are effectively decreased by using the ESPP. For code rates of 0.122, 0.1235, and 0.125, the FERs reach 6.2%, 11.7%, and 57.5%, respectively.

Table II lists the performance of the proposed reconciliation scheme after the above optimizations. The reconciliation efficiency increases with the code rate from 77.79% to 94.0%, whereas the FER and the average number of iterations increase from 5.2% to 57.8%, and 11 to 140, respectively. It is known that high reconciliation efficiency and low FER are desired to achieve a high secret key rate for QKD. The number of iterations is proportional to the consumption of computing resources during the information reconciliation.

To estimate the performance of the proposed reconciliation scheme for hard-decision 8-PSK discrete modulation CV-QKD, we calculate the achievable secret key rate at SNR $= 0.15$ by using the numerical convex optimization techniques [20,32]. The relevant simulation parameters are modulation amplitude $\alpha = 1$, channel transmission $T = 0.316$ (corresponding to a 25-km standard single-mode fiber), detection efficiency $\eta = 0.52$, electronic noise $v_{el} = 0.06$, and equivalent excess noise $\varepsilon = 0.03$. For code rates of 0.1 (level 2) and 0.02 (level 3), no positive key rate can be achieved due to the low reconciliation efficiency. For code rates of 0.122 and 0.02, a secret key rate of 0.0193 bits/pulse is achieved with a reconciliation efficiency of 92.05% and a FER of 6.2%. The maximized secret key rate of 0.0195 bits/pulse is obtained at the code rates of 0.1235 and 0.02, which makes the best trade-off between the reconciliation efficiency and the FER.

VI. SUMMARY AND OUTLOOK

In this paper, we propose a slice reconciliation scheme for hard-decision 8-PSK discrete modulation CV-QKD. The proposed scheme quantizes and encodes raw keys into multilevel binary sequences and decodes with the MLC-MSD approach. The channel capacity and optimal code rate are determined at each level by calculating the conditional mutual information between Alice and Bob. We design RL-LDPC codes and optimize their degree distribution of edge type 2 and the size of the base matrix. To further decrease the FER, ESPP is introduced. Finally, reconciliation efficiencies of 92.05% and 93% with FERs of 6.2% and 11.7% are achieved at an

SNR of 0.15. Then, we apply the reconciliation scheme to the hard-decision 8-PSK discrete modulation CV-QKD with a 25-km transmission distance. The resulting secret key rates are 0.0193 and 0.0195 bits/pulse under realistic experimental parameters.

Our information reconciliation scheme can be extended to M-PSK modulation straightforwardly. In this case, Bob quantizes his data in the phase space to obtain m discrete symbols, which are then converted into multilevel binary bit strings with optimal mapping. Next, the generated binary bit strings are processed using the approaches of MLC and MSD. The current work focuses on the application of the proposed information reconciliation scheme to the reverse reconciliation scenario rather than direct reconciliation, since reverse reconciliation offers superior performance in terms of transmission distances and potential for practical applications. It is worth noting that our information reconciliation scheme is applicable to both direct and reverse reconciliation scenarios. Nonetheless, a thorough examination of the direct reconciliation 8-PSK CV-QKD protocol's performance lies beyond the scope of this study and is reserved for future investigation. In the future work, we will also extend the current scheme to more complex modulation constellations, such as quadrature amplitude modulation and amplitude-phase shift keying.

ACKNOWLEDGMENTS

We thank H. Yang and S. Li for helpful discussions. This work was supported by the National Natural Science Foundation of China (Grants No. 62205188 and No. 62175138) and the Quantum Science and Technology-National Science and Technology Major Project (Grant No. 2021ZD0300703).

DATA AVAILABILITY

The data that support the findings of this article are not publicly available upon publication because it is not technically feasible and/or the cost of preparing, depositing, and hosting the data would be prohibitive within the terms of this research project. The data are available from the authors upon reasonable request.

[1] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Rev. Mod. Phys. **92**, 025002 (2020).
[2] 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. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Adv. Opt. Photon. **12**, 1012 (2020).
[3] C. Portmann and R. Renner, Rev. Mod. Phys. **94**, 025008 (2022).
[4] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nature (London) **557**, 400 (2018).
[5] X. Zhong, J. Hu, M. Curty, L. Qian, and H.-K. Lo, Phys. Rev. Lett. **123**, 100506 (2019).
[6] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, S.-L. Han, Q. Yu, K. Liang, F. Zhou, X. Yuan, M.-S. Zhao, T.-Y. Wang, X. Jiang, L. Zhang, W.-Y. Liu *et al.*, Nature (London) **589**, 214 (2021).
[7] 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, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, and Z.-F. Han, Nat. Photon. **16**, 154 (2022).
[8] Y. Liu, W.-J. Zhang, C. Jiang, J.-P. Chen, C. Zhang, W.-X. Pan, D. Ma, H. Dong, J.-M. Xiong, C.-J. Zhang, H. Li, R.-C. Wang, J. Wu, T.-Y. Chen, L. You, X.-B. Wang, Q. Zhang, and J.-W. Pan, Phys. Rev. Lett. **130**, 210801 (2023).
[9] L. Zhou, J. Lin, Y. Jing, and Z. Yuan, Nat. Commun. **14**, 928 (2023).
[10] W. Li, L. Zhang, Y. Lu, Z.-P. Li, C. Jiang, Y. Liu, J. Huang, H. Li, Z. Wang, X.-B. Wang, Q. Zhang, L. You, F. Xu, and J.-W. Pan, Phys. Rev. Lett. **130**, 250802 (2023).
[11] Y. Tian, P. Wang, J. Liu, S. Du, W. Liu, Z. Lu, X. Wang, and Y. Li, Optica **9**, 492 (2022).
[12] S. Liu, Z. Lu, P. Wang, Y. Tian, X. Wang, and Y. Li, npj Quantum Inf. **9**, 92 (2023).
[13] Z. Chen, X. Wang, S. Yu, Z. Li, and H. Guo, npj Quantum Inf. **9**, 28 (2023).
[14] F. Ji, P. Huang, T. Wang, X. Jiang, and G. Zeng, Photon. Res. **12**, 1485 (2024).
[15] A. A. E. Hajomer, I. Derkach, N. Jain, H.-M. Chin, U. L. Andersen, and T. Gehring, Sci. Adv. **10**, eadi9474 (2024).
[16] S. Liu, Y. Tian, Y. Zhang, Z. Lu, X. Wang, and Y. Li, Optica **11**, 1762 (2024).
[17] S. Yang, Z. Yan, H. Yang, Q. Lu, Z. Lu, L. Cheng, X. Miao, and Y. Li, EPJ Quantum Technol. **10**, 40 (2023).
[18] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).
[19] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).
[20] J. Lin, T. Upadhyaya, and N. Lütkenhaus, Phys. Rev. X **9**, 041064 (2019).
[21] S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, Phys. Rev. X **9**, 021059 (2019).
[22] H. Wang, Y. Li, Y. Pi, Y. Pan, Y. Shao, L. Ma, Y. Zhang, J. Yang, T. Zhang, and W. Huang, Commun. Phys. **5**, 162 (2022).
[23] D. Pereira, M. Almeida, M. Facão, A. N. Pinto, and N. A. Silva, Opt. Lett. **47**, 3948 (2022).
[24] Y. Tian, Y. Zhang, S. Liu, P. Wang, Z. Lu, X. Wang, and Y. Li, Opt. Lett. **48**, 2953 (2023).
[25] F. Roumestan, A. Ghazisaeidi, J. Renaudier, L. T. Vidarte, A. Leverrier, E. Diamanti, and P. Grangier, J. Lightwave Technol. **42**, 5182 (2024).
[26] A. A. E. Hajomer, F. Kanitschar, N. Jain, M. Hentschel, R. Zhang, N. Lütkenhaus, U. L. Andersen, C. Pacher, and T. Gehring, Light Sci. Appl. **14**, 255 (2025).
[27] A. Leverrier, arXiv:2310.17548.

[28] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, Phys. Rev. A **77**, 042325 (2008).
[29] J. Martinez-Mateo, D. Elkouss, and V. Martin, IEEE Commun. Lett. **14**, 1155 (2010).
[30] T. Richardson and R. Urbank, *Modern Coding Theory* (Cambridge University Press, New York, 2008).
[31] S. Q. Ng, F. Kanitschar, G. Zhang, and C. Wang, arXiv:2504.08298.
[32] P. Wang, Y. Zhang, Z. Lu, X. Wang, and Y. Li, New J. Phys. **25**, 023019 (2023).
[33] G. V. Assche, J. Cardinal, and N. J. Cerf, IEEE Trans. Inf. Theory **50**, 394 (2004).
[34] Z. Bai, S. Yang, and Y. Li, Jpn. J. Appl. Phys. **56**, 044401 (2017).
[35] H. Mani, T. Gehring, P. Grabenweger, B. Ömer, C. Pacher, and U. L. Andersen, Phys. Rev. A **103**, 062419 (2021).
[36] X. Wang, Y. Zhang, S. Yu, B. Xu, Z. Li, and H. Guo, Quantum Inf. Comput. **17**, 1123 (2017).
[37] C. Zhou, X. Wang, Y. Zhang, Z. Zhang, S. Yu, and H. Guo, Phys. Rev. Appl. **12**, 054013 (2019).
[38] S. Kreinberg, I. Koltchanov, and A. Richter, in *Conference on Lasers and Electro-Optics, Washington, DC, 2020*, OSA Technical Digest (Optica, Washington, DC, 2020), p. ATh1I.6.
[39] H. Yang, S. Liu, S. Yang, Z. Lu, Y. Li, and Y. Li, Phys. Rev. A **109**, 012604 (2024).
[40] C. Zhou, X. Wang, Z. Zhang, S. Yu, Z. Chen, and H. Guo, Sci. China Phys. Mech. Astron. **64**, 260311 (2021).
[41] U. Wachsmann, R. F. H. Fischer, and J. B. Huber, IEEE Trans. Inf. Theory **45**, 1361 (1999).
[42] Y. Li, X. Zhang, Y. Li, B. Xu, L. Ma, J. Yang, and W. Huang, Sci. Rep. **10**, 14561 (2020).
[43] S.-Y. Chung, G. Forney, T. Richardson, and R. Urbanke, IEEE Commun. Lett. **5**, 58 (2001).
[44] R. Storn and K. Price, J. Global Optim. **11**, 341 (1997).
[45] H. Xiao-Yu, E. Eleftheriou, and D. M. Arnold, in *IEEE Global Telecommunications Conference (Cat. No.01CH37270), GLOBECOM'01* (IEEE, New York, 2001), Vol. 2, pp. 995–1001.
[46] H. Xiao and A. H. Banihashemi, IEEE Commun. Lett. **8**, 715 (2004).
[47] S. Lin, L. Chen, J. Xu, and I. Djurdjevic, Near Shannon limit quasi-cyclic low-density parity-check codes, in *IEEE Global Telecommunications Conference (IEEE Cat. No.03CH37489), GLOBECOM'03* (IEEE, Piscataway, NJ, 2003), Vol. 4, pp. 2030–2035.
[48] Z. Li and B. V. K. V. Kumar, A class of good quasi-cyclic low-density parity check codes based on progressive edge growth graph, in *Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers, 2004* (IEEE, Piscataway, NJ, 2004), Vol. 2, pp. 1990–1994.
[49] H. Cui, J. Lin, and Z. Wang, IEEE Trans. Circuits Syst. II **66**, 397 (2019).