entropy

IMPACT FACTOR 2.0

Indexed in: PubMed

CITESCORE 5.2

Article

Rate-Adaptive Information Reconciliation for CV-QKD Systems at Low Signal-to-Noise Ratios

Huiting Fu, Jisheng Dai, Yan Feng, Han Hai, Huayong Ge, Peng Huang and Xue-Qin Jiang

Special Issue

Recent Advances in Continuous-Variable Quantum Key Distribution

Edited by

Prof. Dr. Xueqin Jiang and Dr. Peng Huang

MDPI

https://doi.org/10.3390/e28010010

entropy

MDPI

Article

Rate-Adaptive Information Reconciliation for CV-QKD Systems at Low Signal-to-Noise Ratios

Huiting Fu [1], Jisheng Dai [1], Yan Feng [2], Han Hai [1], Huayong Ge [1,*], Peng Huang [3] and Xue-Qin Jiang [1,*]

[1] College of Information and Intelligent Science, Donghua University, Shanghai 201620, China; 2232249@mail.dhu.edu.cn (H.F.); jsdai@dhu.edu.cn (J.D.); hhai@dhu.edu.cn (H.H.)
[2] College of Electronic and Information, Shanghai Dianji University, Shanghai 201306, China; fengyan@sdju.edu.cn
[3] State Key Laboratory of Advanced Optical Communication Systems and Networks, Institute for Quantum Sensing and Information Processing, Shanghai Jiao Tong University, Shanghai 200240, China; huang.peng@sjtu.edu.cn
* Correspondence: gehuayong@dhu.edu.cn (H.G.); xqjiang@dhu.edu.cn (X.-Q.J.)

Abstract

In continuous-variable quantum key distribution (CV-QKD) systems, information reconciliation (IR) is a crucial step that significantly affects the secret key rate (SKR). The fixed-rate error-correcting codes used in IR are highly sensitive to changes in the signal-to-noise ratio (SNR) and cannot maintain a high reconciliation efficiency in practical CV-QKD systems. To address this issue, we first propose a rate-adaptive IR protocol, namely Threshold-based IR (TIR), which changes the code rate of low-density parity-check (LDPC) codes by selectively revealing bits with lower reliability and adjusting their log-likelihood ratios (LLRs). Then, we propose a rate-adaptive IR protocol, namely Sorting-based IR (SIR), which not only adjusts the code rate according to variations in SNR, but also enables the CV-QKD systems to achieve high reconciliation efficiency over a wide range of SNRs. Furthermore, we perform an analysis of the protocols in terms of code rate, reconciliation efficiency, and complexity. The simulation results demonstrate that the proposed protocols outperform other rate-adaptive IR protocols, achieving a reconciliation efficiency higher than 98.5% in the SNR range below −20 dB and maintaining a certain SKR in long-distance transmission.

Keywords: continuous-variable quantum key distribution; information reconciliation; reconciliation efficiency; secret key rate; log-likelihood ratios

1. Introduction

Quantum key distribution (QKD) [1–3] is among the most practical implementations of quantum-information technologies, enabling two spatially separated parties, Alice and Bob, to share random keys in an untrusted environment and theoretically guaranteeing unconditional security [4]. Currently, QKD technology falls into two mainstream types: discrete-variable QKD (DV-QKD) [1,2] and continuous-variable QKD (CV-QKD) [5]. In DV-QKD systems, key information is used to encode the polarization or phase of a single-photon state; in contrast, in CV-QKD systems, the encoding process targets the amplitude and phase quadrature states [6]. CV-QKD systems have attracted considerable research interest due to their compatibility with conventional telecommunication infrastructure [7]. Recent studies have mainly focused on enhancing secure transmission distances and optimizing the secret key rate (SKR) in CV-QKD systems [8,9].

Academic Editor: Osamu Hirota

Received: 31 October 2025
Revised: 17 December 2025
Accepted: 19 December 2025
Published: 20 December 2025

Quantum transmission and post-processing make up a typical CV-QKD system [8]. Bob uses a homodyne or heterodyne detector to test quantum states at random during the quantum transmission [10]. Base sifting [11], parameter estimation [12], information reconciliation (IR) [13,14], and privacy amplification [15] are the four primary processes of post-processing, which is used to obtain secret keys from both parties. Among these, IR is considered the primary technical bottleneck, limiting the transmission distance and the SKR of the system. Ongoing research aims to improve reconciliation efficiency and reduce the frame error rate (FER), thereby improving the SKR [16]. Currently, slice reconciliation [17] and multidimensional reconciliation [18] are currently widely utilized reconciliation techniques.

Considering finite-size effects [12], high-performance error-correcting codes with long block lengths are typically employed in IR to achieve a high reconciliation efficiency. Specifically, multi-edge-type low-density parity-check (MET-LDPC) codes [19,20], as a generalization of LDPC codes [20], have demonstrated near-Shannon-limit performance, which can achieve a high reconciliation efficiency at low signal-to-noise ratios (SNRs). However, fixed-rate LDPC codes cannot maintain a high reconciliation efficiency under fluctuating SNR conditions in practical CV-QKD systems [6,21,22]. Raptor codes [23] and spinal codes [24] with the rateless property can achieve a high reconciliation efficiency over a wider range of SNRs, but require a higher decoding complexity compared to LDPC codes. The rate-adaptive LDPC codes in [16] maintain over 96% reconciliation efficiency by modifying a fixed-size parity-check matrix, though this fixed size is a limitation. The multiple decoding attempt (MDA) protocol was proposed [25], which reveals bits randomly after decoding failure to adjust log-likelihood ratios (LLRs), thereby changing the code rate. However, we follow the definition of bit reliability as proposed in [26], and it has been experimentally demonstrated that bits with lower reliability are significantly more likely to be erroneous, and thus are key contributors to decoding failure.

In this paper, we propose that selectively revealing bits with lower reliability and adjusting their LLRs can change the code rate of LDPC codes. To achieve this, we first introduce a rate-adaptive IR protocol named Threshold-based IR (TIR), where bits with lower reliability below a threshold θ are disclosed. Then, we propose a Sorting-based IR (SIR) protocol, through which bits are sorted by reliability, and the least reliable bits are selectively disclosed. The SIR protocol not only adjusts the code rate according to variations in SNRs, but also achieves high reconciliation efficiency across a wide range of SNRs.

The rest of the paper is structured as follows: In Section 2, we review the fundamentals of IR in brief. In Section 3, we introduce the proposed protocols in detail. In Section 4, we perform an analysis of the proposed protocols. The simulation results of our scheme are shown and analyzed in Section 5. Finally, we conclude this paper in Section 6.

2. Preliminaries

IR serves as a crucial procedure in CV-QKD systems, which aims to accomplish error correction while minimizing leakage the information of secret keys, thereby enabling the two communicating parties to acquire symmetric secret keys. IR can be categorized into two main types: direct reconciliation and reverse reconciliation [11]. Reverse reconciliation provides longer transmission distances and maintains a specific SKR during long-distance fiber optic communication at low SNRs, in contrast to direct reconciliation [27].

Multidimensional reverse reconciliation is a popular reconciliation technique for CV-QKD systems due to its superior reconciliation efficiency at low SNRs and low capacity loss. A schematic diagram of CV-QKD systems is presented in Figure 1. The general method of information reconciliation was proposed in [18] and improved in [6,16,28,29]. After going through the data sifting and parameter estimation steps, Alice and Bob obtain correlated

quantum sequences $\mathbf{x}$ and $\mathbf{y}$; in this context, $\mathbf{y} = \mathbf{x} + \mathbf{z}$, with $\mathbf{z}$ standing for the quantum channel noise. Alice and Bob then split the sequences $\mathbf{x}$ and $\mathbf{y}$ into d-dimensional vectors, and proceed to normalize these vectors respectively.

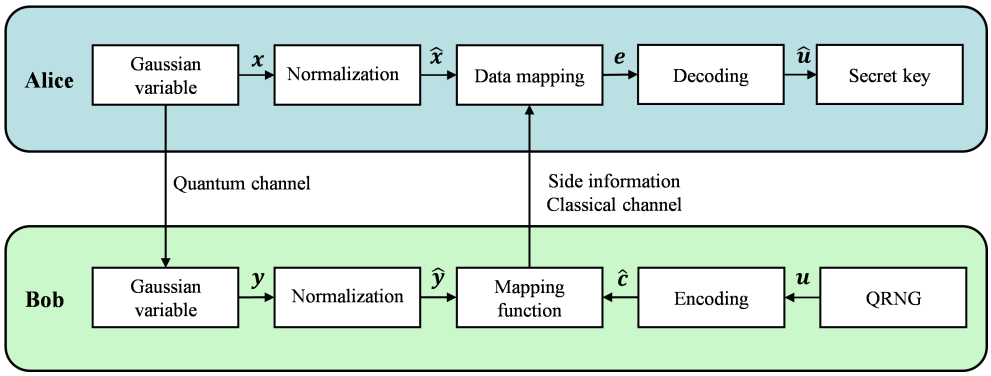

Figure 1. Multidimensional reverse reconciliation schematic diagram.

Using a quantum random number generator (QRNG), Bob creates a secret key consisting of a random binary sequence $\mathbf{u}$. The encoder employs an error-correcting code to encode $\mathbf{u}$ into $\hat{\mathbf{c}}$, and outputs side information that avoids revealing the secret key. To compute the mapping function $\mathbf{M}(\hat{\mathbf{y}}, \hat{\mathbf{c}})$ that acts as part of the side information, we utilize the encoded sequence $\hat{\mathbf{c}}$ and the normalized sequence $\hat{\mathbf{y}}$. $\mathbf{M}(\hat{\mathbf{y}}, \hat{\mathbf{c}})$ is an orthogonal transformation, defined as $\mathbf{M}(\hat{\mathbf{y}}, \hat{\mathbf{c}}) = \sum_{i=1}^{d} \alpha_i(\hat{\mathbf{y}}, \hat{\mathbf{c}})\mathbf{A}_i$, where $\alpha_i(\hat{\mathbf{y}}, \hat{\mathbf{c}}) = (\mathbf{A}_i\hat{\mathbf{y}} \mid \hat{\mathbf{c}})$; the specific form of matrix $\mathbf{A}_i$ is available in [18]. Bob then uses a classical channel to send Alice this side information. After receiving $\mathbf{M}(\hat{\mathbf{y}}, \hat{\mathbf{c}})$, Alice uses it together with the normalized sequence $\hat{\mathbf{x}}$ to obtain $\mathbf{e}$ via data mapping. Subsequently, the LDPC code and sum-product algorithm are adopted to recover $\mathbf{e}$ into the sequence $\hat{\mathbf{u}}$. Once the decoding process succeeds, Alice and Bob will share a symmetrical secret key.

The SKR of a CV-QKD system with one-way multidimensional reverse reconciliation, considering finite-size effects into account, is provided by [10]

$$K_{\text{finite}} = \frac{n}{N}(1 - P_e)[\beta I(A : B) - S_{\epsilon_{\text{PE}}}(B : E) - \Delta(n)], \tag{1}$$

where N is the total amount of data that Alice and Bob exchanged, n is the amount of data that was used to extract the keys, and the remaining portion is used for parameter estimation. P_e is the reconciliation FER, which is defined as the ratio of discarded secret keys to total secret keys. The reconciliation efficiency is measured by

$$\beta = \frac{R}{C(s)}, \tag{2}$$

where R denotes the error-correcting code rate and $C(s) = \frac{1}{2}\log_2(1 + s)$ represents the channel capacity when the SNR is set to s. $I(A : B)$ represents Alice and Bob's classical mutual information. The maximum Holevo information that Eve can receive from Bob's data is $S_{\epsilon_{\text{PE}}}(B : E)$, where ϵ_{PE} is the parameter estimate failure probability [29]. The finite-size offset factor is represented by $\Delta(n)$. According to Equation (1), an imperfect reconciliation scheme leads to a reduction in the SKR and imposes limitations on the applicable range of the protocol.

3. The Proposed Protocols

In this section, we introduce two rate-adaptive IR protocols for CV-QKD systems, both of which are designed based on the principle of revealing bits with lower reliability. The schematic diagram of the protocols is shown in Figure 2.

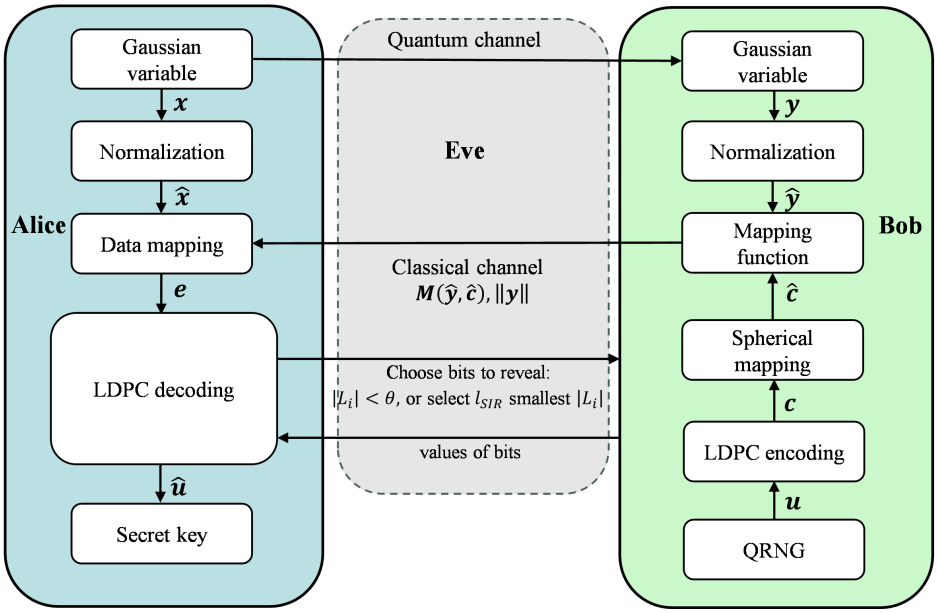

Figure 2. Schematic diagram of the proposed protocols.

3.1. Threshold-Based IR (TIR)

3.1.1. Threshold Selection

The TIR protocol involves setting a threshold θ for the reliability of the bits during the iterative decoding process. Here, define L_i as the LLR of the i-th bit and define the reliability of the i-th bit as the absolute value of L_i, denoted as $|L_i|$. The determination of the threshold θ is precisely based on the reliability value $|L_i|$ difference between erroneous bits and correct bits. To clarify how this difference supports the selection of θ, we verify this through a practical scenario: take a rate 0.02 LDPC code with SNR = -15.1 dB and analyze one hundred failed codewords. Histograms of reliability values L_i for correct bits and erroneous bits after decoding failure are drawn in Figure 3a and Figure 3b, respectively. It is shown that the reliability value $|L_i|$ of erroneous bits is obviously smaller than that of most correct bits, which can be used to distinguish them efficiently. Hence, for a failed codeword, one can set a suitable threshold θ. If the reliability value $|L_i| < \theta$, the corresponding bits are classified into the set of suspicious bits, which have a high probability of being erroneous bits and are selected to be revealed.

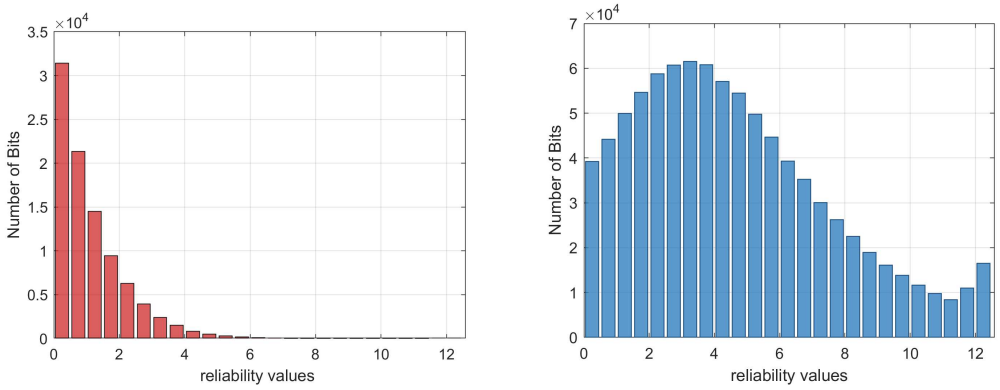

Figure 3. Histogram of decoded bits after decoding failure. (**a**) Correct bits. (**b**) Erroneous bits. The code length is 1,000,000.

3.1.2. TIR Protocol

In this paper, we adopt multidimensional reverse reconciliation. Alice and Bob both have correlated Gaussian sequences, $\mathbf{x}$ and $\mathbf{y}$, which satisfy $\mathbf{x} \sim N(0, \sigma_{\mathbf{x}}^2)^d$ on Euclidean space $\mathbb{R}^d$ and $\mathbf{y} = \mathbf{x} + \mathbf{z}$, where $\mathbf{z} \sim N(0, \sigma_{\mathbf{z}}^2)^d$ and d indicates the multidimensional IR dimension. Subsequently, they normalize $\mathbf{x}$ and $\mathbf{y}$ into $\hat{\mathbf{x}}$ and $\hat{\mathbf{y}}$, where $\hat{\mathbf{x}} = \mathbf{x}/||\mathbf{x}||$ and $\hat{\mathbf{y}} = \mathbf{y}/||\mathbf{y}||$. Here $||\cdot||$ denotes a norm of a vector. The uniform distribution of the sequences $\hat{\mathbf{x}}$ and $\hat{\mathbf{y}}$ is satisfied by their distribution on the surface of the unit sphere S^{d-1}, which centers on zero.

Using the QRNG, Bob generates a binary sequence $\mathbf{u}$. He then employs LDPC encoding to produce the codeword $\mathbf{c}$. However, in order to adapt $\mathbf{c}$ for multidimensional reconciliation, $\mathbf{c}$ must be converted into a binary spherical sequence $\hat{\mathbf{c}}$ by

$$\hat{c} = (\hat{c_1}, \hat{c_2}, \ldots, \hat{c_d}) \longrightarrow \left(\frac{(-1)^{c_1}}{\sqrt{d}}, \frac{(-1)^{c_2}}{\sqrt{d}}, \ldots, \frac{(-1)^{c_d}}{\sqrt{d}} \right). \tag{3}$$

After acquiring $\hat{\mathbf{y}}$ and $\hat{\mathbf{c}}$, Bob uses $\hat{\mathbf{y}}$ and $\hat{\mathbf{c}}$ to compute $\mathbf{M}(\hat{\mathbf{y}}, \hat{\mathbf{c}})$, also known as the mapping function. This mapping function satisfies the following condition: $\mathbf{M}(\hat{\mathbf{y}}, \hat{\mathbf{c}}) \cdot \hat{\mathbf{y}} = \hat{\mathbf{c}}$. Bob transmits $\mathbf{M}(\hat{\mathbf{y}}, \hat{\mathbf{c}})$ to Alice through the classical channel. Then, Alice transforms $\hat{\mathbf{x}}$ into $\mathbf{e}$ using the mapping function $\mathbf{e} = \mathbf{M}(\hat{\mathbf{y}}, \hat{\mathbf{c}}) \cdot \hat{\mathbf{x}}$.

Alice uses the parity-check matrices of the LDPC code and sum-product algorithm to recover sequence $\mathbf{e}$ into sequence $\hat{\mathbf{u}}$. During the iterative decoding process, while calculating the LLR, Alice sets a threshold θ for $|L_i|$. She identifies the set of indices $\mathcal{I} = \{i \mid |L_i| < \theta\}$ and sends $\mathcal{I}$ to Bob.

Bob determines the values of the bits in $\mathcal{I}$ and returns the values to Alice. If Bob confirms that the i-th bit is 1, Alice sets L_i to a large negative value, thereby forcing the bit to be interpreted as 1 in subsequent iterations. Conversely, if Bob confirms that the i-th bit is 0, Alice sets L_i to a large positive value, thereby forcing the bit to be interpreted as 0 in subsequent iterations. Alice continues the iterative decoding with the modified LLRs. If the decoding process is successful, Alice and Bob will possess symmetric secret keys, which are retained for final secret keys; if decoding fails, the secret keys are discarded outright to ensure the absolute security of the final secret keys.

Finally, privacy amplification decreases the information leakage that occurs through the preceding quantum and raw key generation processes. The final secret keys can thus be established by Alice and Bob using a robust randomness extraction protocol.

3.2. Sorting-Based IR (SIR)

The SIR protocol for revealing bits with lower reliability involves sorting the $|L_i|$ during the iterative decoding process and selecting a certain number of bits with lower reliability for disclosure. This protocol effectively enables adaptive reconciliation. Before IR, Alice and Bob calculate the optimal code rate R_{SIR} based on the time-varying SNR of the quantum channel. Then, they select a high-performance original LDPC code whose code rate is close to R_{SIR}. Typically, the original LDPC code rate is defined as

$$R_0 = \frac{n - m}{n}. \tag{4}$$

Here, m and n correspond to the number of rows and columns of the LDPC parity-check matrix $\mathbf{H}$, respectively. Subsequently, to achieve the target reconciliation efficiency, it is

necessary to reveal l_{SIR} bits with lower reliability so that the original code rate equals the optimal code rate. This relationship is formulated as

$$R_{\mathrm{SIR}} = \frac{(n - l_{\mathrm{SIR}}) - m}{n - l_{\mathrm{SIR}}} = \frac{n - m - l_{\mathrm{SIR}}}{n - l_{\mathrm{SIR}}}. \tag{5}$$

In the SIR protocol, the main differences from the TIR protocol are as follows: Alice uses LDPC decoding to recover sequence $\mathbf{e}$ into sequence $\hat{\mathbf{u}}$. During the iterative decoding process, while calculating the LLR, Alice takes the $|L_i|$ and sorts them in ascending order. Then, Alice identifies the indices $i_1, i_2, \ldots, i_{l_{\mathrm{SIR}}}$ corresponding to the l_{SIR} smallest values, such that $|L_1| \leq |L_2| \leq \cdots \leq |L_{l_{\mathrm{SIR}}}|$. She constructs the index set $\mathcal{I} = \{i_1, i_2, \ldots, i_{l_{\mathrm{SIR}}}\}$ and sends $\mathcal{I}$ to Bob.

4. Analysis of the TIR and SIR Protocols

In this section, we perform an analysis of the TIR and SIR protocols, focusing on their code rate, reconciliation efficiency, and complexity.

4.1. Code Rate

In CV-QKD, we need rate-adaptive and high-efficiency codes since errors must be efficiently corrected at low SNRs to increase the SKR and the secure transmission distance. The TIR protocol identifies bits with lower reliability using the threshold θ: bits with reliability $|L_i| < \theta$ are selected for revelation. Thus, the code rate is calculated as

$$R_{\mathrm{TIR}} = \frac{(n - l_{\mathrm{TIR}}) - m}{n - l_{\mathrm{TIR}}} = \frac{n - m - l_{\mathrm{TIR}}}{n - l_{\mathrm{TIR}}}, \tag{6}$$

where l_{TIR} denotes the number of revealed bits and depends on both the threshold θ and the channel SNR. This results in a passive rate adjustment: l_{TIR} varies with SNRs, since more bits have $|L_i| < \theta$ at low SNRs, which increases l_{TIR} and lowers R_{TIR}. However, in the SIR protocol, rate-adaptive adjustment of the code rate is achieved by adjusting the number of disclosed bits with lower reliability according to variations in SNRs. Specifically, it first sorts the bits in descending order of their reliability $|L_i|$ and then calculates the optimal code rate R_{SIR}, which is given by $R_{\mathrm{SIR}} = \beta \cdot C(s)$ using Equation (2). Finally, to ensure that the original code rate R_0 is equal to R_{SIR}, we reveal l_{SIR} bits with lower reliability. According to Equation (5), the l_{SIR} is calculated as

$$l_{\mathrm{SIR}} = \frac{(n - m) - R_{\mathrm{SIR}} \cdot n}{1 - R_{\mathrm{SIR}}}. \tag{7}$$

Algorithm 1 demonstrates the code rate calculation process of the SIR protocol. In summary, both the TIR and SIR protocols proposed in this paper can achieve adaptive adjustment of the code rate.

Algorithm 1 The code rate calculation process of the SIR protocol.

Step 1 Obtain the channel capacity C(s) based on the practical SNR.
Step 2 Determine the target reconciliation efficiency β.
Step 3 Sort the bits in descending order of reliability $|L_i|$.
Step 4 Obtain the optimal code rate R_{SIR} using Equation (2).
Step 5 Determine the l_{SIR} to disclose $R_0 \rightarrow R_{SIR}$ using Equation (7).

4.2. Reconciliation Efficiency

A higher reconciliation efficiency is required at low SNRs in order to meet the criterion that the SKR is greater than zero. From Equation (2), we know that the code rate is the

major factor affecting reconciliation efficiency. Thus, in the TIR protocol, the reconciliation efficiency is defined by Equations (2) and (6) as

$$\beta_{\mathrm{TIR}} = \frac{R_{\mathrm{TIR}}}{C(s)} = \frac{n - m - l_{\mathrm{TIR}}}{(n - l_{\mathrm{TIR}}) \cdot C(s)}. \tag{8}$$

Additionally, it can also be derived from Equation (2) that under various SNRs, fixed-rate error-correcting codes are unable to sustain high reconciliation efficiency. However, the SIR protocol adjusts the code rate according to variations in SNRs to achieve high reconciliation efficiency across a wide range of SNRs. To be specific, we first set a target reconciliation efficiency, denoted as β_{target}. Then, we determine the optimal code rate R_{SIR} under a given SNR based on Equation (2). Finally, we calculate the number of bits with lower reliability to be disclosed using Equation (7), such that the original code rate R_0 is adjusted to the optimal code rate R_{SIR}, thereby achieving a high reconciliation efficiency.

4.3. Complexity

We conduct an analysis of the time complexity and space complexity for the TIR and SIR protocols. The time complexity $\mathcal{O}(f(\alpha))$ and space complexity $\mathcal{O}(g(\alpha))$ are defined as the asymptotic time cost and storage cost of an algorithm, respectively, both of which are associated with the algorithm's scale, and specifically described using the $\mathcal{O}$-notation [30]. In this context, $f(\alpha)$ and $g(\alpha)$ are functions that characterize the growth rates of running time of the algorithm and storage demand, with both dependent on the input size α. According to the notations above, the time complexity of the TIR protocol is $\mathcal{O}(n)$, since it only requires comparator operations to determine if satisfies $|L_i| < \theta$. The computational cost thus grows linearly with the block length n, and the dominant factor is the number of decoding iterations. In comparison, the SIR protocol requires an additional sorting of the reliability. A direct sorting implementation has complexity $\mathcal{O}(n \log n)$, which increases with the block length more rapidly than the TIR protocol. In terms of space complexity, both protocols scale linearly with the block length. For the TIR protocol, the memory requirement is minimal, involving only the storage of indices of revealed bits. The SIR protocol requires additional buffers to store sorted indices and to compute the number of disclosed bits, which leads to slightly higher memory usage but still of linear order. In addition, we analyzed the complexity of other rate-adaptive reconciliation protocols, including the Raptor and MDA protocols. Raptor codes consist of an outer pre-code and an inner Luby transform (LT) code. Therefore, the two-stage architecture also presents challenges. For the Raptor protocol, the complexity of precoding increases dramatically with block length, making it unsuitable for practical applications at low SNRs [8]. Furthermore, LT code decoding requires dynamic symbol generation and confidence propagation, resulting in a complexity of $\mathcal{O}(n \log n)$, exceeding that of LDPC-based protocols. The MDA protocol, while sharing the $\mathcal{O}(n)$ complexity of the TIR protocol for random bit revelation, may require multiple decoding attempts, which multiplies the base complexity. Overall, both the TIR and SIR protocols maintain a linear order of computational and storage complexity, providing positive implications for the practical implementation of CV-QKD systems.

5. Simulation Results

In this section, we study the performance of the proposed TIR and SIR protocols, focusing on reconciliation efficiency, FER, and the SKR. We employ MET-LDPC codes in our simulations. For MET-LDPC codes, different types of edges have independent degree distribution functions. Here, the degree refers to the number of edges connected to variable nodes or check nodes. The detailed degree distribution we use in this paper is shown in Table 1, where $\nu(r, x)$ denotes the generating polynomial for the variable node

types and $\mu(x)$ denotes the generating polynomial for the check node types. For more information about the degree distribution of MET-LDPC codes, refer to [9]. The dimension d of multidimensional reconciliation is set to 8 in the simulation that follows.

Table 1. The degree distribution of MET-LDPC codes.

Code Rate	Degree Distribution
0.1	$\nu(r,x) = 0.0775r_1x_1^{20}x_2^{20} + 0.0475r_1x_1^3x_2^{22} + 0.875r_1x^3$ $\mu(x) = 0.0025x_1^{11} + 0.0225x_1^{12} + 0.03x_2^2x_3 + 0.845x_2^3x_3$
0.05	$\nu(r,x) = 0.04r_1x_1^{21}x_2^{34} + 0.03r_1x_1^3x_2^{34} + 0.93r_1x^3$ $\mu(x) = 0.01x_1^8 + 0.01x_1^9 + 0.41x_2^2x_3 + 0.52x_2^3x_3$
0.02	$\nu(r,x) = 0.0225r_1x_1^2x_2^{57} + 0.0175r_1x_1^3x_2^{57} + 0.96r_1x_3$ $\mu(x) = 0.010625x_1^3 + 0.009375x_1^7 + 0.6x_2^2x_3 + 0.36x_2^3x_3$

Figure 4 illustrates the FER performance comparison between the TIR protocol with threshold-based bit revelation and a baseline strategy that randomly reveals the same number of bits, where the 0.02 MET-LDPC code, as presented in Table 1, is used in the comparison. As observed, the method of setting the threshold θ to reveal bits consistently outperforms random revelation in the SNR range from -15.4 to -14.9 dB. This demonstrates that selectively revealing bits with $|L_i| < \theta$ significantly enhances decoding performance and reduces the FER at low SNRs.

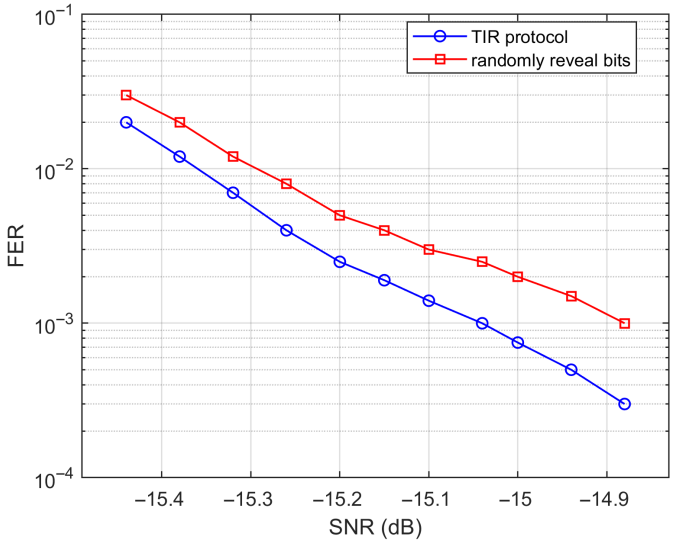

Figure 4. FER comparison between the TIR protocol and random bit revelation.

Figure 5 shows the FER performance of the SIR protocol compared with the MDA protocol [25] under varying bit revelation ratios at SNR = -15.23 dB. In the proposed SIR protocol, bits are sorted according to $|L_i|$, and the least reliable ones are selectively revealed. In contrast, the MDA protocol randomly reveals bits for LLR adjustment after decoding failure. As shown in the Figure 5, the proposed SIR protocol consistently achieves a lower FER across all tested revelation ratios. Specifically, when the bit revelation ratio exceeds 6%, the FER of the SIR protocol drops below 0.01, while the MDA protocol still maintains a relatively high FER of around 0.08. This clearly demonstrates that the proposed protocol, which reveals bits with lower reliability, outperforms the MDA protocol [25] with random bit disclosure.

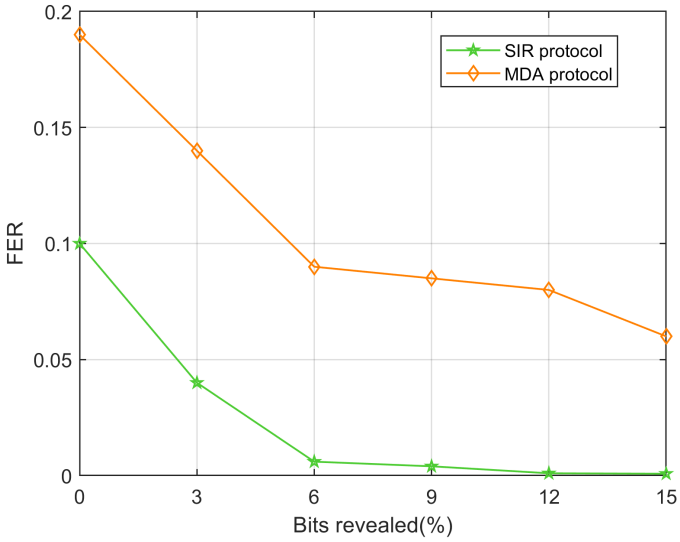

Figure 5. FER comparison under varying bit revelation ratios.

To further study the performance of our proposed SIR protocol at low SNRs, we compare the FER with the Raptor protocol in reference [6], as shown in Figure 6. The target reconciliation efficiency is set to 96% in the SNR range of -18 and -13 dB, and 95% of -12 to -10 dB. As shown in Table 2, we evaluate the number of revealed bits l_{SIR} to convert the original code rate $R_0 = 0.02, 0.05, 0.1$ into the optimal code rate R_{SIR} under various SNR conditions, in order to maintain the target reconciliation efficiency. Although Figure 6 shows the FER is relatively high, this is a reasonable trade-off to achieve high reconciliation efficiency at low SNRs. Therefore, the simulation results demonstrate that all points (FER < 1) have the desired reconciliation efficiency. In the SNR range between -18 and -10 dB, the SIR protocol has a smaller FER, indicating a greater SKR.

Table 2. The detailed results of the SIR protocol.

R_0	SNR (dB)	l_{SIR}	R_{SIR}
0.02	-18	9210	0.01089
	-17	6408	0.01368
	-16	2869	0.01718
0.05	-15	29,069	0.02156
	-14	23,605	0.02703
	-13	16,700	0.03387
	-12	8421	0.04193
0.1	-11	1005	0.05238
	-10	742	0.06531

Figure 7 presents the finite-size SKR results of the SIR protocol for a CV-QKD system with one-way reverse reconciliation. In practice, the modulation variance V_A is applied to approximate the theoretical ideal value by adjusting it in real time based on various channel characteristics. Nevertheless, it is not feasible to obtain simulation results covering the full SNR range from -20 to -10 dB. Thus, we simulate the reconciliation efficiency at low SNRs and present the simulation in Figure 7. Specifically, Figure 7 shows the finite-size SKR results for a block length of $N = 10^{12}$ at SNRs of -20, -18, -16, -14, -12, and -10 dB, respectively, while also providing the corresponding asymptotic theoretical SKR. The SKR of our adaptive SIR protocol is calculated using Equation (1), and other parameters remain consistent with those in reference [6]. Given that some bits are used for parameter

estimation, we designate half of the bits for parameter estimation and the other half for symmetric secret key extraction ($n = N/2$) in IR. The simulation results indicate that when the FER of reconciliation is 0.99, the SIR protocol can achieve a reconciliation efficiency of 98.5%, with a theoretical transmission distance exceeding 165 km.

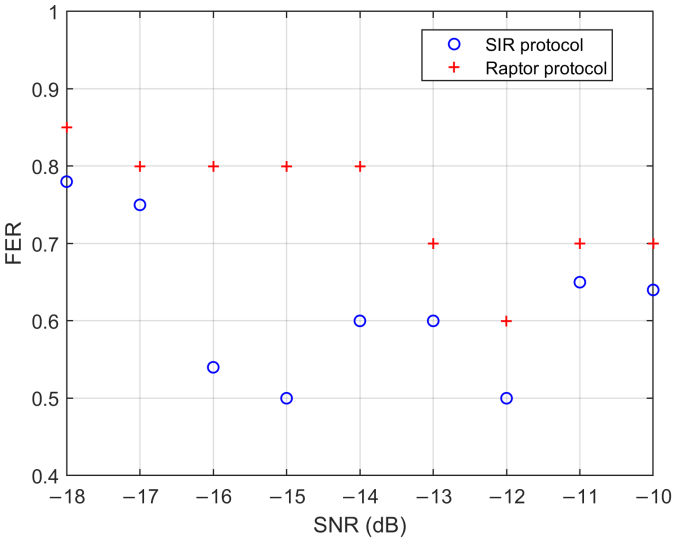

Figure 6. Comparison of FER performance between the SIR protocol and Raptor protocol at low SNRs.

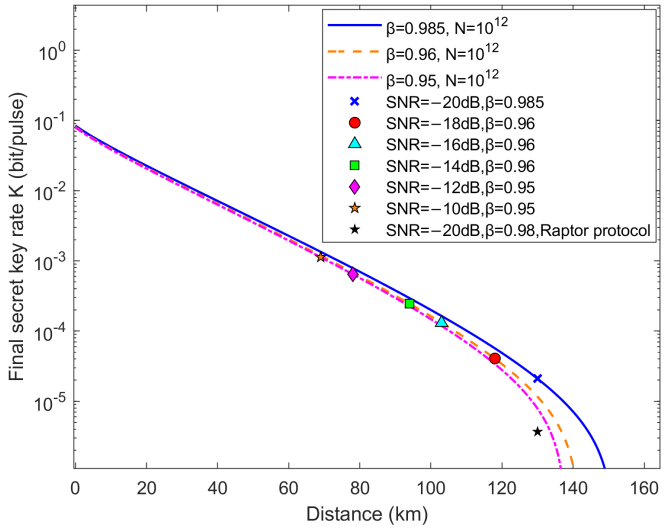

Figure 7. Finite-size secret key rate vs. distance. The cross points, circle points, triangle points, block points, rhombus points, and orange five-pointed stars correspond to our simulation results. The black five-pointed stars are derived from simulations conducted in accordance with the Raptor protocol in reference [6], with an FER of reconciliation of 0.99. The asymptotic theoretical SKRs under different SNRs are represented by a solid line, dashed line, and dot-dash line, respectively. Alice's modulation variance V_A has been optimized, and the other parameters configured are listed as follows: excess noise $\xi = 0.01$, detection efficiency $\eta = 0.6$, quantum channel attenuation factor $\alpha = 0.2$ dB/km, and electronic noise $v_{el} = 0.015$.

6. Conclusions

In this paper, we proposed two rate-adaptive IR protocols for CV-QKD systems, which dynamically adjusted the code rate and improved reconciliation efficiency at low SNRs. The TIR protocol disclosed bits with $|L_i| < \theta$, while the SIR protocol revealed a fixed number of the least reliable bits, allowing dynamic adjustment of the code rate to the time-varying nature of the quantum channel of CV-QKD systems. The analysis demonstrated the overall

effectiveness of the proposed TIR and SIR protocols in terms of key metrics including code rate, reconciliation efficiency, and complexity. The simulation results showed that selectively revealing bits with lower reliability outperformed randomly revealing bits. Moreover, the SIR protocol reduced the FER and improved reconciliation efficiency, achieving high reconciliation efficiency over a wide range of SNRs and even attaining over 98.5% efficiency when the SNR dropped below −20 dB. Furthermore, the relationship between the finite-size SKR and transmission distance confirmed the superiority of our scheme. Our work may contribute to the development of practical applications for CV-QKD systems.

Author Contributions: Conceptualization, Y.F.; methodology, X.-Q.J.; software, H.F.; validation, H.F.; formal analysis, H.F.; investigation, H.F.; resources, Y.F.; data curation, H.F. and X.-Q.J.; writing—original draft preparation, H.F.; writing—review and editing, H.F., J.D., H.G. and X.-Q.J.; visualization, H.F.; supervision, J.D., Y.F., H.H., H.G., P.H. and X.-Q.J.; project administration, H.H., P.H. and X.-Q.J.; funding acquisition, P.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China (Grant Nos. 61971276, 62071319), the Key R&D Program of Guangdong province (Grant No. 2020B0303040002), the Shanghai Municipal Science and Technology Major Project (Grant No. 2019SHZDZX01), the State Key Laboratory of Advanced Optical Communication Systems and Networks (Grant No. 2024GZKF006), and the Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0300703).

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author(s).

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145. [CrossRef]
2. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301–1350. [CrossRef]
3. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in quantum cryptography. *Adv. Opt. Photonics* **2020**, *12*, 1012–1236. [CrossRef]
4. Diamanti, E.; Lo, H.-K.; Qi, B.; Yuan, Z. Practical challenges in quantum key distribution. *npj Quantum Inf.* **2016**, *2*, 16025. [CrossRef]
5. Braunstein, S.L.; Loock, P.V. Quantum information with continuous variables. *Rev. Mod. Phys.* **2005**, *77*, 513–577. [CrossRef]
6. Zhou, C.; Wang, X.; Zhang, Y.; Zhang, Z.; Yu, S.; Guo, H. Continuous-variable quantum key distribution with rateless reconciliation protocol. *Phys. Rev. Appl.* **2019**, *12*, 054013. [CrossRef]
7. Jouguet, P.; Kunz-Jacques, S.; Leverrier, A.; Grangier, P.; Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat. Photonics* **2013**, *7*, 378–381. [CrossRef]
8. Milicevic, M.; Feng, C.; Zhang, L.M.; Gulak, P.G. Quasi-cyclic multi-edge ldpc codes for long-distance quantum cryptography. *npj Quantum Inf.* **2018**, *4*, 21. [CrossRef]
9. Jouguet, P.; Kunz-Jacques, S.; Leverrier, A. Long-distance continuous-variable quantum key distribution with a gaussian modulation. *Phys. Rev. A At. Mol. Opt. Phys.* **2011**, *84*, 062317. [CrossRef]
10. Lodewyck, J.; Bloch, M.; García-Patrón, R.; Fossier, S.; Karpov, E.; Diamanti, E.; Debuisschert, T.; Cerf, N.J.; Tualle-Brouri, R.; McLaughlin, S.W.; et al.. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A At. Mol. Opt. Phys.* **2007**, *76*, 042305. [CrossRef]
11. Grosshans, F.; Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **2002**, *88*, 057902. [CrossRef]
12. Leverrier, A.; Grosshans, F.; Grangier, P. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A At. Mol. Opt. Phys.* **2010**, *81*, 062343. [CrossRef]
13. Grosshans, F.; Cerf, N.J.; Wenger, J.; Tualle-Brouri, R.; Grangier, P. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. *arXiv* **2003**, arXiv:quant-ph/0306141. [CrossRef]
14. Assche, G.V.; Cardinal, J.; Cerf, N.J. Reconciliation of a quantum-distributed gaussian key. *IEEE Trans. Inf. Theory* **2004**, *50*, 394–400. [CrossRef]

15. Bennett, C.H.; Brassard, G.; Crépeau, C.; Maurer, U.M. Generalized privacy amplification. *IEEE Trans. Inf. Theory* **2002**, *41*, 1915–1923. [CrossRef]
16. Zhou, C.; Wang, X.; Zhang, Z.; Yu, S.; Chen, Z.; Guo, H. Rate compatible reconciliation for continuous-variable quantum key distribution using raptor-like ldpc codes. *Sci. China Physics, Mech. Astron.* **2021**, *64*, 260311. [CrossRef]
17. Jouguet, P.; Elkouss, D.; Kunz-Jacques, S. High-bit-rate continuous-variable quantum key distribution. *Phys. Rev.* **2014**, *90*, 042329. [CrossRef]
18. Leverrier, A.; Alléaume, R.; Boutros, J.; Zémor, G.; Grangier, P. Multidimensional reconciliation for a continuous-variable quantum key distribution. *Phys. Rev. A At. Mol. Opt. Phys.* **2008**, *77*, 042325. [CrossRef]
19. Richardson, T.; Urbanke, R. Multi-edge type ldpc codes. In *Workshop Honoring Prof. Bob McEliece on His 60th Birthday*; California Institute of Technology: Pasadena, CA, USA , 2002; pp. 24–25.
20. Gallager, R. Low-density parity-check codes. *IRE Trans. Inf. Theory* **1962**, *8*, 21–28. [CrossRef]
21. Zhang, M.; Hai, H.; Feng, Y.; Jiang, X.-Q. Rate-adaptive reconciliation with polar coding for continuous-variable quantum key distribution. *Quantum Inf. Process.* **2021**, *20*, 318. [CrossRef]
22. Jeong, S.; Jung, H.; Ha, J. Rate-compatible multi-edge type low-density parity-check code ensembles for continuous-variable quantum key distribution systems. *npj Quantum Inf.* **2022**, *8*, 6. [CrossRef]
23. Shokrollahi, A. Raptor codes. *IEEE Trans. Inf. Theory* **2006**, *52*, 2551–2567. [CrossRef]
24. Perry, J.; Iannucci, P.A.; Fleming, K.E.; Balakrishnan, H.; Shah, D. Spinal codes. *ACM SIGCOMM Comput. Commun. Rev.* **2012**, *42*, 49–60. [CrossRef]
25. Gümüş, K.; Eriksson, T.A.; Takeoka, M.; Fujiwara, M.; Sasaki, M.; Schmalen, L.; Alvarado, A. A novel error correction protocol for continuous variable quantum key distribution. *Sci. Rep.* **2021**, *11*, 10465. [CrossRef] [PubMed]
26. Zhou, C.; Li, Y.; Ma, L.; Yang, J.; Huang, W.; Sun, A.; Wang, H.; Luo, Y.; Li, Y.; Chen, Z.; et al. Integrated high-performance error correction for continuous-variable quantum key distribution. *arXiv* **2024**, arXiv:2407.16432.
27. Grosshans, F.; Grangier, P. Reverse reconciliation protocols for quantum cryptography with continuous variables. *arXiv* **2002**, arXiv:quant-ph/0204127. [CrossRef]
28. Zhang, K.; Jiang, X.-Q.; Feng, Y.; Qiu, R.; Bai, E. High efficiency continuous-variable quantum key distribution based on atsc 3.0 ldpc codes. *Entropy* **2020**, *22*, 1087. [CrossRef]
29. Jiang, X.Q.; Xue, S.; Tang, J.; Huang, P.; Zeng, G. Low-complexity adaptive reconciliation protocol for continuous-variable quantum key distribution. *Quantum Sci. Technol.* **2024**, *9*, 025008. [CrossRef]
30. Elkouss, D.; Martínez-Mateo, J.; Martín, V. Secure rate-adaptive reconciliation. In Proceedings of the 2010 International Symposium On Information Theory & Its Applications, Taichung, Taiwan, 17–20 October 2010; IEEE: New York, NY, USA, 2010; pp. 179–184.