SCIENCE CHINA
Information Sciences

• LETTER •

August 2025, Vol. 68, Iss. 8, 180510:1–180510:2
https://doi.org/10.1007/s11432-024-4480-x

Special Topic: Quantum Information

Effective rate-adaptive reconciliation for CV-QKD using QC-MET-LDPC codes

Kun ZHANG[1], Jia HOU[1,2*], Xue-Qin JIANG[3,4,5*], Jisheng DAI[3], Peng HUANG[4,5,6] & Guihua ZENG[4,5,6]

[1]*School of Electronic and Information Engineering, Soochow University, Suzhou 215006, China*
[2]*Yangtze Delta Region Institute (Quzhou), University of Electronic Science and Technology of China, Quzhou 324000, China*
[3]*College of Information Science and Technology, Donghua University, Shanghai 201620, China*
[4]*Hefei National Laboratory, Hefei 230088, China*
[5]*Shanghai Research Center for Quantum Sciences, Shanghai 201315, China*
[6]*State Key Laboratory of Advanced Optical Communication Systems and Networks, Center of Quantum Sensing and Information Processing (QSIP), Shanghai Jiao Tong University, Shanghai 200240, China*

Received 9 December 2024/Revised 20 March 2025/Accepted 4 June 2025/Published online 4 July 2025

Citation Zhang K, Hou J, Jiang X-Q, et al. Effective rate-adaptive reconciliation for CV-QKD using QC-MET-LDPC codes. Sci China Inf Sci, 2025, 68(8): 180510, https://doi.org/10.1007/s11432-024-4480-x

Secret key rate (SKR) and transmission distance are critical performance metrics for continuous-variable quantum key distribution (CV-QKD) systems [1]. Reconciliation efficiency, a key parameter of the information reconciliation [2] procedure using error correction codes in CV-QKD post-processing, directly impacts these two performance metrics. Specifically, higher reconciliation efficiency leads to a greater SKR and longer transmission distance. However, fluctuating signal-to-noise ratio (SNR) conditions in practical channels may degrade the reconciliation efficiency or impair the error correction performance [3]. For instance, in fixed-rate reconciliation schemes, an increase in SNR typically causes practical reconciliation efficiency to deteriorate. This adversely affects the SKR and transmission distance of CV-QKD systems. Conversely, a decrease in SNR degrades error correction performance. This can result in a high frame error rate (FER) and almost zero SKR [4].

In this study, we propose a rate-adaptive reconciliation scheme by designing low-density parity-check (LDPC) codes with a wide range of rate adaptability and flexible block lengths. This scheme aims to achieve high reconciliation efficiency, thereby meeting the demands of practical CV-QKD systems. We first design a seed matrix of relatively small size according to the degree distribution of multi-edge type (MET) LDPC codes, which exhibits excellent error-correcting performance. Then, the size of the seed matrix is adjusted based on the required code rate to obtain the target matrix. Finally, the target matrix serves as the base matrix for constructing quasi-cyclic (QC) MET-LDPC codes with the desired block lengths. The 0s and 1s in the base matrix are replaced with appropriately sized zero matrices or circulant permutation matrices. The designed codes require only one seed matrix to achieve a high reconciliation efficiency over a wide range of SNRs. Additionally, due to the QC structure, the designed codes are convenient for memory storage and facilitate parallel accelerated processing.

Scheme. The proposed rate-adaptive reconciliation scheme needs to determine the block length and code rate of the LDPC code. The number of raw data used for key establishment must match the block length of the LDPC code. The code rate R of the LDPC code needs to be appropriately designed to achieve a high reconciliation efficiency $\beta = R/C(\eta)$, where $C(\eta) = 0.5\log_2(1+\eta)$ represents the channel capacity with the SNR being η. The overall framework of the proposed rate-adaptive reconciliation scheme can be summarized as follows.

(1) A MET-LDPC degree distribution with a code rate of 0.01995 is designed, which provides excellent error-correcting performance and is ideal for QC structuring. Using the progressive edge-growth algorithm [5], we construct a Raptor-like seed matrix based on this MET-LDPC degree distribution. The details are provided in Appendix A.

(2) Once the required block length and code rate for the MET-LDPC code are determined, the seed matrix is adjusted to a target matrix to meet the code rate requirement. The seed matrix $\boldsymbol{H}_{\mathrm{RL}}$ with a Raptor-like structure is given by

$$\boldsymbol{H}_{\mathrm{RL}} = \begin{bmatrix} \boldsymbol{A} & \boldsymbol{Z} \\ \boldsymbol{B} & \boldsymbol{I} \end{bmatrix}, \tag{1}$$

where $\boldsymbol{A}$ represents the highest-rate code part of $\boldsymbol{H}_{\mathrm{RL}}$ and $\boldsymbol{B}$ denotes the incremental redundancy code part of $\boldsymbol{H}_{\mathrm{RL}}$. Sub-matrices $\boldsymbol{Z}$ and $\boldsymbol{I}$ stand for zero and identity matrices, respectively. The code rate of adaptivity can be achieved by cutting or extending the seed matrix. Figure 1(a) illustrates the principle of increasing the code rate. By cutting

* Corresponding author (email: houjia@suda.edu.cn, xqjiang@dhu.edu.cn)

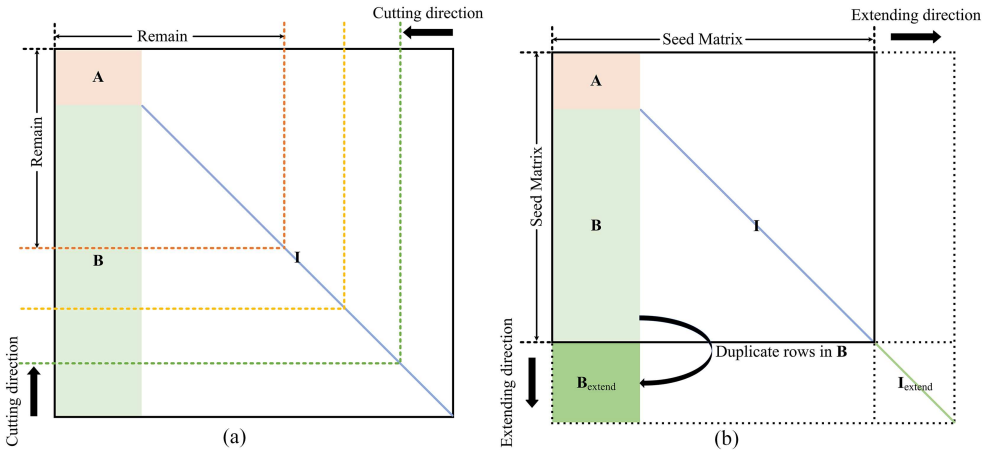

Figure 1 (Color online) Schematic diagrams of (a) the cutting operation and (b) the extending operation for a seed matrix with a Raptor-like structure.

the same number of rows and columns from the bottom-right corner of the seed matrix along a defined cutting direction, the remaining part constitutes the target matrix for achieving the required code rate. Figure 1(b) illustrates the principle of decreasing the code rate. In contrast to the simple cut operation, the code rate reduction operation requires adding the same number of rows and columns to the seed matrix along the specified extending direction. To avoid introducing additional computational resources and time delays caused by the extension operation, we simply copy the elements of $\boldsymbol{B}$ in (1) to the extended rows. Specifically, whenever the seed matrix needs to be extended by a row, a random row from $\boldsymbol{B}$ is duplicated into the extended row. The details can be found in Appendix B.

(3) QC-LDPC construction techniques are applied to the target matrix, eventually obtaining QC-MET-LDPC codes that meet the required code rates and block lengths for CV-QKD systems. With the help of the powerful parallel processing capabilities of the graphics processing unit (GPU) platform, the matrix construction and log-likelihood ratio belief propagation (LLR-BP) decoding are both accelerated. The details are presented in Appendix C.

Prior to the reconciliation process, predefined thresholds for both reconciliation efficiency and FER must be established. If the actual reconciliation efficiency falls below the predefined threshold, the cut operation is applied to increase the MET-LDPC code rate, thereby restoring the reconciliation efficiency to the threshold. Conversely, when the actual FER exceeds its predefined threshold, the extension operation is employed to reduce the MET-LDPC code rate. This enhances error-correcting capability and reduces FER. The target matrix generated through these cutting/extension operations is then utilized to construct QC-MET-LDPC parity-check matrices with required block lengths via QC-LDPC construction techniques.

Experiments. To validate the performance of the proposed rate-adaptive reconciliation scheme, we analyze its error-correction capability through LLR-BP decoding. In terms of error-correction performance, we demonstrate that the parity-check matrices constructed under varying code rates achieve both low error floors and high reconciliation efficiency across a wide SNR range. Regarding rate adaptivity, we validate that the proposed scheme maintains reconciliation efficiency above the threshold and FER below the threshold under fluctuating SNR conditions. Finally, we confirm the superiority of the scheme in both SKR and achievable transmission distance. The details of experimental results are provided in Appendix D.

Conclusion. In this study, we propose a rate-adaptive reconciliation scheme based on QC-MET-LDPC codes, which dynamically adjusts the code rate and block length of QC-MET-LDPC codes according to varying SNR values and the required block length. The proposed rate-adaptive reconciliation scheme can maintain excellent error-correcting performance in a broad SNR range, achieving a high reconciliation efficiency. The QC construction process and LLR-BP decoding are both accelerated by a GPU platform. Furthermore, the rate-adaptive reconciliation scheme could be extended to other QKD protocols, including non-Gaussian QKD protocols.

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

Supporting information Appendixes A–D. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Grosshans F, Grangier P. Continuous variable quantum cryptography using coherent states. Phys Rev Lett, 2002, 88: 057902
2 Leverrier A, Alléaume R, Boutros J, et al. Multidimensional reconciliation for a continuous-variable quantum key distribution. Phys Rev A, 2008, 77: 042325
3 Zhou C, Wang X Y, Zhang Z G, et al. Rate compatible reconciliation for continuous-variable quantum key distribution using Raptor-like LDPC codes. Sci China-Phys Mech Astron, 2021, 64: 260311
4 Zhang K, Hou J, Jiang X Q, et al. High-speed information reconciliation with syndrome-based early termination for continuous-variable quantum key distribution. Opt Express, 2023, 31: 34000–34010
5 Hu X-Y, Eleftheriou E, Arnold D M. Regular and irregular progressive edge-growth tanner graphs. IEEE Trans Inform Theor, 2005, 51: 386–398