# A Comprehensive Survey on LDPC Code Design for CV-QKD

**Mauro Queiroz Nooblath Neto**[*,1], **Guilherme Vergne de Oliveira**[1], **Micael Andrade Dias**[2,1], **Nelson Alves Ferreira Neto**[1], **Francisco Revson Fernandes Pereira**[1], **Valéria Loureiro da Silva**[1]

[1] *QuIIN – Quantum Industrial Innovation, Centro de Competência Embrapii Cimatec, SENAI CIMATEC, Salvador, BA, Brazil*

[2] *Department of Electrical and Photonics Engineering, Technical University of Denmark, 2800 Lyngby, Denmark*

[*] *Corresponding author: mauro.neto@fieb.org.br*

**Abstract: Continuous-Variable Quantum Key Distribution (CV-QKD) represents a promising technology for secure communication, but its practical implementation heavily relies on highly efficient information reconciliation (IR) to extract a secret key from correlated quantum data shared over noisy channels. Low-density parity-check codes (LDPC) have emerged as the state-of-the-art solution for this task due to their capacity-approaching performance. However, designing LDPC codes that perform reliably in the very low signal-to-noise ratio (SNR) regime of CV-QKD, while preserving practical implementation complexity, remains a major challenge. This work presents a comprehensive survey of LDPC code design methodologies for CV-QKD, with particular emphasis on three key structural classes: Quasi-Cyclic (QC-LDPC), Multi-Edge Type (MET-LDPC), and their hybrid form (QC-MET-LDPC).**

**Keywords: Quantum Key Distribution, Continuous-Variable, Low-Density-Parity-Check Codes, Information Reconciliation, Code Design, Quantum Communication**

**Abbreviations: CV-QKD, LDPC, IR, QC-LDPC, MET-LDPC, QC-MET-LDPC.**

## 1. Introduction

A typical continuous variables quantum key distribution (CV-QKD) protocol consists of three main stages: quantum state transmission, information reconciliation (IR), and privacy amplification. In quantum state transmission, Alice sends a sequence of $N$ very low-intensity coherent states to Bob, who performs detection and obtains a correlated, but not identical sequence. Discrepancies arise due to quantum channel noise, detection imperfections, and potential eavesdropping. Given the extremely low signal-to-noise ratio (SNR) inherent to these systems, the IR phase becomes particularly challenging. Its goal is to ensure that Alice and Bob share an identical and secure key by employing error-correcting codes — most notably, Low-Density Parity-Check (LDPC) codes, defined by sparse parity-check matrices $H$ of size $(n-k)\times n$, with code rate $R_{code} = \frac{k}{n}$. In low-SNR regimes, very high redundancy is required to achieve reliable reconciliation, leading to large matrix dimensions (on the order of $10^6$) and a significant computational burden during decoding. This complexity negatively impacts the performance of the Belief Propagation (BP) algorithm and limits the real-time secret key rate, posing a major challenge to the scalability of CV-QKD systems. Consequently, the design of LDPC code structures optimized for low-SNR and efficient hardware implementation is essential for advancing practical CV-QKD deployments.

This paper aims to provide an overview of the most relevant results and recent advancements in the field of CV-QKD systems, with a focus on

LDPC code methods applied to IR techniques. The structure of this paper is organized as follows: Section 2 presents the fundamentals of CV-QKD and reconciliation techniques. Section 3 describes LDPC codes and quasi-cyclic construction. Section 4 approach about LDPC codes specifically designed for CV-QKD, including MET-LDPC codes and enonder/decoder architectures. Section 5 reviews practical applications and performance results. Lastly, Section 6 concludes the paper with final remarks.

## 2. CV-QKD and Reconciliation

CV-QKD is a promising branch of quantum cryptography protocols, where information is encoded in the quadratures of coherent states of light, allowing the use of conventional optical receivers [1]. In contrast to discrete variable QKD (DV-QKD) protocols, the CV-QKD approach offers greater compatibility with current optical infrastructures, such as fiber-optic networks and integrated photonic components [2].

During the quantum stage of the protocol, the transmiter (Alice) sends to the receiver (Bob) a sequence of coherent states whose amplitudes are modulated according to a continuous Gaussian distribution. Bob, in turn, uses a detector (homodyne or heterodyne) to measure one or both quadratures of the received states. Due to the nature of the quantum channel, attenuation and noise effects, as well as possible eavesdropping (by Eve), the values obtained by Bob are only correlated with those sent by Alice, not identical [1].

To extract a common and secure key, an Information Reconciliation (IR) step is necessary, which consists of correcting errors between the correlated data using error-correcting codes. In long-distance CV-QKD, reconciliation must be performed efficiently even under extreme conditions, such as very low signal-to-noise ratios (SNR).

The reconciliation efficiency is expressed by a factor $\beta \in [0,1]$, which represents how close the reconciliation process is to the ideal efficiency imposed by Shannon's limit. The higher the value of $\beta$, the higher the secret key generation rate, defined as [3]:

$$R_{key} = \beta I_{AB} - \chi_{BE} \tag{1}$$

where $I_{AB}$ is the mutual information between Alice and Bob, and $\chi_{BE}$ is the maximum information Eve can obtain about Bob's key. Therefore, the choice of reconciliation technique directly affects both security and practical viability. Among the existing techniques, the following, whose main characteristics are summarized in Table 1, stand out:

**Slice Reconciliation:** maps continuous samples into multiple binary slices to apply binary codes at each layer [1].

**Multilevel Coding / Multistage Decoding**

**(MLC-MSD):** organizes bits into layers of decreasing reliability, applying codes with varying redundancy per level [1, 4].

**Multidimensional Reconciliation:** uses linear transformations, such as orthogonal rotations or Hadamard matrices, to maximize correlation efficiency between samples and enable the use of high-performance binary error-correcting codes [2, 4, 5].

Multidimensional reconciliation has become the most effective approach for low SNR regimes, such as those encountered in long-distance CV-QKD. This technique facilitates the use of efficient binary codes, such as LDPC, reducing the error rate (BER) and improving the key rate [1, 2].

## 3. LDPC Codes

Low Density Parity Check (LDPC) codes are among the most promising strategies for application in the Information Reconciliation (IR) stage, as they enable performance close to the Shannon limit and are widely employed in noisy communication systems. The parity-check matrix $H$ can be represented by a bipartite graph known as Tanner graph, denoted by $\mathscr{G}$, composed of two sets of nodes: the variable nodes $V_j$, associated with the columns of the parity-check matrix, and the check nodes $C_i$, corresponding to the rows of the matrix [6]. A connection between a variable node $j$ and a check node $i$ is established when the element $H(i,j) = 1$, indicating the existence of an edge between these nodes.

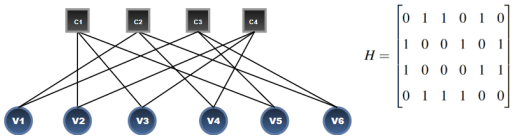


**Figure** 1: Tanner graph and its corresponding binary parity-check matrix.

The number of edges connected to the vertices of $\mathscr{G}$ is referred to as the vertex degree. Its distribution is defined by a pair of polynomials, $\lambda(x) = \sum_i \lambda_i x^i$ and $\rho(x) = \sum_i \rho_i x^i$, where $\lambda_i$ and $\rho_i$ respectively denote the fraction of variable and check nodes of degree $i$ in the Tanner graph $\mathscr{G}$ [6].

### 3.1. Quasi-Cyclic LDPC

The LDPC Quasi-cyclic codes (QC-LDPC) represents a structured LDPC code class, in which the parity-check matrix $H$ is built from circulant blocks. In other words, permutations of the identity matrix are made from a base matrix $B$ that indicates the number of rotations applied to each identity matrix. This structure allows a compact representation, facilitating efficient hardware implementation and significantly reducing the computational cost of encoding and decoding, which is essential for CV-QKD systems with large block sizes.

The matrix $H$ can be represented by the base matrix $B$ of dimensions $m_b \times n_b$, whose elements $b_{i,j} \in -1, 0, 1, 2, \ldots, Q-1$ indicate the shift applied to an identity matrix of dimensions $Q \times Q$. Thus, the value $-1$ denotes a null block ($Q \times Q$

| Technique | Best for | SNR (dB) | Computational Complexity | Reconciliation Efficiency |
|---|---|---|---|---|
| Multidimensional | Long distances | Low ($-20$–$0\,dB$) | High | High ($\geq 95\%$) |
| MLC-MSD | Medium distances | Medium ($-3$–$5\,dB$) | Medium | High ($\geq 94\%$) |
| Slice Reconciliation | Short distances | High ($> 5\,dB$) | Low | Medium (90–93%) |

**Table** 1: Comparison of the main reconciliation techniques in CV-QKD.

matrix of zeros), and the other values represent the number of positions in which the identity matrix should be circularly shifted to form the corresponding set [7].

This model allows the generation of large matrices using only the base matrix and the parameter $Q$, making QC-LDPC a highly scalable alternative. Moreover, the quasi-cyclic structure preserves the sparsity of the parity-check matrix, which is crucial for the good performance of the decoding algorithm.

Another advantage of the QC structure is its systematic encoding process based on the base matrix. The techinique involves generating the codeword divided into $Q$ sized sets, replacing matrix multiplication operations by circular shifts (a characteristic of multiplication by a rotated identity matrix) [7].

## 4. LDPC codes for CV-QKD

In the IR stage of CV-QKD systems, error correction is essential to ensure key agreement between Alice and Bob, given that quantum signals are highly susceptible to noise due to the low signal-to-noise ratio (SNR) of the channel [1]. LDPC codes are widely employed in this phase, and for scenarios involving extremely low SNR, new design approaches for these codes are required. In this context, Multi-Edge Type LDPC (MET-LDPC) codes stand out for their flexibility in tuning the degree distributions through multiple edge types in the Tanner graph, enabling optimization for low-rate regimes and performance close to the Shannon limit [2, 5]. When combined with Quasi-Cyclic (QC) constructions, these codes allow for efficient implementations with reduced latency and computational complexity—features that are highly desirable for practical CV-QKD applications.

### 4.1. LDPC Multi-Edge Type

Multi-Edge Type LDPC (MET-LDPC) codes generalize both regular and irregular LDPC codes by introducing multiple edge types in the Tanner graph, allowing greater flexibility in defining the degree distributions of the nodes. This unified structure enables efficient modeling of codes with both uniform and non-uniform distributions, adapting them to varying channel conditions. A key advantage of MET-LDPC codes over conventional LDPC codes is their ability to achieve performance close to the Shannon limit, particularly

in low-rate regimes such as Information Reconciliation (IR) in CV-QKD systems, where they operate robustly even under extremely low SNR conditions [8].

The formal description of a MET-LDPC code family is given by two multivariate polynomials:

$$\Omega(\vec{x}) = \sum_d \Omega_d x_1^{d_1} x_2^{d_2} \cdots x_t^{d_t} \tag{2}$$

$$\Psi(\vec{x}) = \sum_d \Psi_d x_1^{d_1} x_2^{d_2} \cdots x_t^{d_t} \tag{3}$$

where $\Omega(\vec{x})$ and $\Psi(\vec{x})$ describe the variable nodes and parity-check nodes, respectively. Unlike single-variable polynomials, as described in Section 1, these polynomials have multiple variables, each corresponding to a distinct edge type. The multivariate representation allows describing codes with $t$ types of connections, characterized by degree vectors $[d_1, d_2, \ldots, d_t]$, where each component $d_i$ indicates the number of sockets associated with edge type $i$. The coefficients $\Omega_d$ and $\Psi_d$ thus denote the fractions of variable and check nodes exhibiting the corresponding connection profiles defined by the degree vector [8].

In Ref. [5], a MET-LDPC code is represented by the polynomials $\Omega$ and $\Psi$ given by equations 4 and 5. These polynomials indicate that approximately 2.25% of the nodes have 2 sockets connected by edges of type 1 and 52 sockets connected by edges of type 2, with no sockets connected by edges of type 3, and so forth. Figure 2 illustrates the structure of the LDPC code family generated by these polynomials.

$$\Omega(r,\vec{x}) = 0.0225 r_1 x_1^2 x_2^{52} + 0.0175 r_1 x_1^3 x_2^{57} + 0.96 r_1 x_3 \tag{4}$$

$$\Psi(\vec{x}) = 0.0165 x_1^4 + 0.0035 x_1^9 + 0.2475 x_2^3 x_3 + 0.7125 x_2^2 x_3 \tag{5}$$

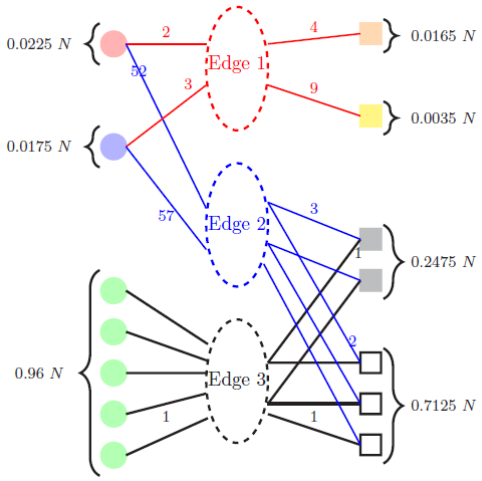


**Figure** 2: Tanner graph corresponding to the MET-LDPC code specified by polynomials 4 and 5, with variable nodes depicted as circles and check nodes depicted as squares.

Unlike the traditional Tanner graph, the structure of MET-LDPC codes features an additional layer of edge types, forming a cascaded architecture. In this configuration, the first edge type represents the irregular portion of the code, while the intermediate types connect this region to the final edges, which are in turn connected to variable and check nodes with a single socket. This organization is crucial for error correction in very low SNR scenarios, ensuring improved decoding effi-

ciency [5].

As described in Section 3.1, QC codes are defined by parity-check matrices constructed from a $q \times q$ array of cyclically shifted identity matrices and $q \times q$ zero matrices. The design of QC-MET-LDPC codes is performed by repeating the multi-edge random sampling process using a block length of $\frac{n}{q}$ instead of $n$ to obtain a base Tanner graph $\mathscr{G}_B$. The base parity-check matrix $H_B$ is derived from $\mathscr{G}_B$ by replacing each nonzero element with a randomly chosen integer from the set $[0,q)$. The matrix $H$ is then obtained from $H_B$ by substituting each nonzero value $i$ with an identity matrix $I_i$ cyclically shifted by $i$ positions [2].

### 4.2. Encoder and Decoder LDPC

Given a message $\vec{u}$ of length $k$, there are several ways to encode this message using a parity-check matrix $H$ generated by an LDPC code of dimension $(n-k) \times (n)$. This encoding produces a codeword $\vec{c}$ of length $n$. Note that since $\vec{c}$ has length $n$, the encoding process essentially consists of adding redundancy of length $(n-k)$ to the message. Typically, this is achieved by constructing a generator matrix $G$ from $H$. To obtain $G$, $H$ is transformed into the standard systematic form $H_{std}$ via a Gaussian elimination process, such that $H_{std} = [P|I]$, where $P$ is the parity portion and $I$ is an identity matrix. From $H_{std}$, the generator matrix is given by $G = [I|P^T]$, and $G$ satisfies $GH_{std}^T = 0$. The codeword is then obtained as $\vec{c} = \vec{u}G^T$ [6].

In the decoding stage, the algorithm commonly used is Belief Propagation (BP), an iterative message-passing algorithm aimed at converging to a valid codeword $\vec{c}$ by updating probabilities between variable and check nodes over the Tanner graph. The most common variant of the BP algorithm is the Sum-Product algorithm. The scheme illustrated in Figure 3 details each step of this algorithm.

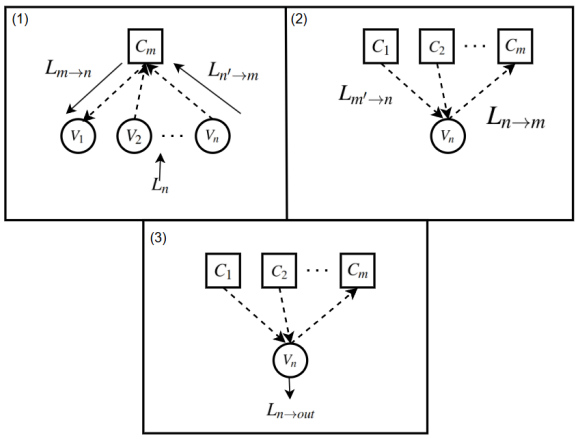


**Figure** 3: Steps of the Sum-Product Belief Propagation algorithm. (1) Message propagation from check nodes to variable nodes. (2) Backward message propagation from variable nodes to check nodes. (3) Estimates for the calculation of $\hat{c}$.

The decoding algorithm begins with **step 1**, in which the variable nodes receive the a priori *log-likelihood ratios* (LLRs) $L_n$ from the BI-AWGN channel. Next, message passing is performed from the check nodes $m$ to the variable nodes $n$, using the following equation:

$$L_{m\to n} = 2\text{arctanh}\left(\prod_{n'\in\mathscr{N}(m)\setminus n} \tanh\left(\frac{L_{n'\to m}}{2}\right)\right) \tag{6}$$

where $n' \in \mathcal{N}(m) \setminus n$ denotes the set of variable nodes connected to the check node $m$, excluding the node $n$ that is currently receiving the message.

In **step 2**, message propagation occurs in the reverse direction, from check nodes to variable nodes. For each variable node $n$, the message sent to check node $m$ is updated according to:

$$L_{n\to m} = L_n + \sum_{m' \in \mathcal{M}(n)\setminus m} L_{m'\to n}, \tag{7}$$

where $m' \in \mathcal{M}(n) \setminus m$ denotes the set of check nodes connected to the variable node $n$, excluding node $m$.

**Step 3** corresponds to the generation of the initial estimate of the codeword after the first propagation iteration. For each variable node $n$, the output value is computed as

$$L_{n\to out} = L_n + \sum_{m' \in \mathcal{M}(n)} L_{m'\to n}, \tag{8}$$

and the hard decision of the corresponding bit estimation is carried out using the rule:

$$\hat{c}_n = \begin{cases} 0, & \text{if } L_{n\to \text{out}} > 0, \\ 1, & \text{otherwise.} \end{cases} \tag{9}$$

## 5. Practical Applications

Several studies have explored advanced methods to optimize the implementation of LDPC codes, aiming to maximize reconciliation efficiency, increase system throughput, and reduce the frame error rate in CV-QKD systems. Ref. [2] proposed the use of QC-MET-LDPC codes with a block length of $10^6$ bits, enabling the reduction of decoding latency during key reconciliation over long distances. The GPU implementation demonstrated secret key generation rates of $4.10 \times 10^{-7}$ bits per pulse for distances ranging from 100 km to 160 km, with throughput up to 8.03 times higher than the upper bound on secret key rate limit, effectively removing reconciliation as a bottleneck. Additionally, Ref. [5] extended the MLC-MSD scheme to reverse reconciliation in CV-QKD, identifying optimal coding rates over a wide range of SNRs (from –20 dB to 10 dB) and introducing G-EXIT charts as an analytical tool for evaluating MET-LDPC codes. The authors demonstrated asymptotic efficiencies exceeding 98% and highlighted the superior performance of multidimensional reconciliation with $d = 8$ in extremely low SNR regimes. Finally, Ref. [9] proposed a rate-compatible MET-LDPC coding scheme based on parity bit puncturing, enabling dynamic adaptation to channel quality using a single encoder/decoder pair. The scheme significantly reduces system complexity, eliminates the need for additional error-detection codes, and extends the usable SNR range by a factor of 1.44, with up to a 2.10-fold improvement in the secret key rate. This makes Information Reconciliation (IR) more efficient and robust for practical CV-QKD applications.

## 6. Conclusions

The research conducted led to the conclusion that MET-LDPC codes demonstrate superiority in extremely low SNRs, enabling the design of more efficient and adaptable reconciliation schemes under varying noise conditions. Concurrently, computational improvements of QC-LDPC solutions play a crucial role in reducing latency and increasing throughput, ensuring viable real-time implementations. These combined techniques, MET-QC-LDPC, can serve as a foundation for constructing codes applicable to various practical scenarios, including the optimization of IR in CV-QKD systems operating at very low SNRs, thereby extending the range and efficiency of QKD on long-distance optical communications. Furthermore, the concept of adaptive rates may provide a solution for implementing robust CV-QKD systems.

## Acknowlegement

This work was fully funded by the project *LDPC Code Design for Information Reconciliation in CV-QKD Optimized for Hardware Implementation*, supported by QuIIN – Quantum Industrial Innovation, the EMBRAPII CIMATEC Competence Center in Quantum Technologies. Financial resources were provided by the PPI IoT/Industry 4.0 program of the Brazilian Ministry of Science, Technology and Innovation (MCTI), under grant number 053/2023, in partnership with EMBRAPII.

## References

[1] S. Yang, Z. Yan, H. Yang, Z. Wang, Y. Liu, X. Wang, and J.-W. Pan. Information reconciliation of continuous-variables quantum key distribution: principles, implementations and applications. *EPJ Quantum Technology*, 10(1):40, 2023.

[2] M. Milicevic, C. Feng, L. M. Zhang, S. Kumar, D. Elkouss, A. Leverrier, J. M. Renes, and O. Pfister. Quasi-cyclic multi-edge LDPC codes for long-distance quantum cryptography. *npj Quantum Information*, 4(1):21, 2018.

[3] Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.*, 88:057902, Jan 2002.

[4] Anthony Leverrier, Romain Alléaume, Joseph Boutros, Gilles Zémor, and Philippe Grangier. Multidimensional reconciliation for a continuous-variable quantum key distribution. *Physical Review A*, 77(4):042325, 2008.

[5] Hossein Mani, Tobias Gehring, Philipp Grabenweger, Bernhard Ömer, Christoph Pacher, and Ulrik Lund Andersen. Multiedge-type low-density parity-check codes for continuous-variable quantum key distribution. *Physical Review A*, 103(6):062419, June 2021.

[6] T.K. Moon. *Error Correction Coding: Mathematical Methods and Algorithms*. Wiley, 2005.

[7] Nelson Alves Ferreira Neto, Joaquim Ranyere S de Oliveira, Wagner Luiz A de Oliveira, and João Carlos N Bittencourt. Vlsi architecture design and implementation of a ldpc encoder for the ieee 802.22 wran standard. In *2015 25th International Workshop on Power and Timing Modeling, Optimization and Simulation (PATMOS)*, pages 71–76. IEEE, 2015.

[8] Tom Richardson and Rüdiger Urbanke. Multi-edge type ldpc codes. *ISIT talk*, 01 2002.

[9] Seongkwang Jeong, Hyunghoon Jung, and Jeongseok Ha. Rate-compatible multi-edge type low-density parity-check code ensembles for continuous-variable quantum key distribution systems. *npj Quantum Information*, 8(6), 2022. Citado nas páginas 6, 19, 20, 23 e 27.