连续变量量子密钥分发中 LDPC 码的研究进展

努尔比耶太外库力[1,2], 李　明[1,2*], 徐胜智[1,2], 陈慧敏[1,2]

(1. 天津师范大学 电子与通信工程学院, 天津 300387;
2. 天津师范大学 天津市无线电能传输与无线通信重点实验室, 天津 300387)

摘　要： 连续变量量子密钥分发 (Continuous-Variable Quantum Key Distribution, CV-QKD) 具有成本低、兼容性强等优势，是当前的研究热点。然而，低信噪比 (Signal-to-Noise Ratio, SNR) 环境下的数据协调效率问题仍是阻碍其大规模应用的主要挑战之一。低密度奇偶校验 (Low-Density Parity-Check, LDPC) 码作为一种先进的纠错码，在 CV-QKD 的数据后处理中显示出巨大潜力。LDPC 码通过其稀疏的校验矩阵结构和迭代解码算法，能够有效地纠正传输过程中的错误，从而提高数据协调效率。综述了光纤和自由空间 CV-QKD 中 LDPC 码的最新研究进展，并提供了该领域的研究动态。基于当前研究进展，进一步指出未来突破的方向，这些突破将最终推动 CV-QKD 技术从实验室走向实际商用。

关键词： 量子通信； 连续变量量子密钥分发； 数据协调； 低密度奇偶校验码

中图分类号： TN918　　**文献标志码：** A　　**DOI：** 10.3788/IRLA20250226

引用格式: NUERBIYE Taiwaikuli , LI Ming, XU Shengzhi, et al. Advances in LDPC codes for continuous-variable quantum key distribution: a comprehensive review[J]. ***Infrared and Laser Engineering***, 2025, 54(8): 20250226.
努尔比耶太外库力, 李明, 徐胜智, 等. 连续变量量子密钥分发中 LDPC 码的研究进展[J]. 红外与激光工程, 2025, 54(8): 20250226.

0　引　言

量子计算技术的突破性进展对传统密码体系构成了根本性威胁，促使量子密钥分发[1](Quantum Key Distribution, QKD) 成为保障通信安全的核心技术之一。QKD 有两种形式：离散变量 (Discrete Variable, DV) 协议和连续变量 (Continuous variable, CV) 协议。DV-QKD 将信息编码在单光子的离散变量上，该技术的实现依赖于高性能的单光子源和单光子探测器等昂贵设备。与此相比，CV-QKD 将信息编码在光场的连续变量上，采用标准相干激光器和平衡零差探测器，与经典相干光通信系统高度兼容。在 CV-QKD 系统中，光纤和自由空间是两种主要传输介质。光纤信道具有稳定性优势，通过低密度奇偶校验 (Low-Density Parity-Check, LDPC) 码优化显著提升了协调效率[2]。自由空间信道虽可突破距离限制，但受大气湍流严重影响[3]。针对低信噪比 (Signal-to-Noise Ratio, SNR) 环境，离散调制与自适应 LDPC 码的结合有效提升了系统性能。这一特性使得 CV-QKD 在成本、部署便捷性和网络集成度方面具有显著优势，成为构建实用化量子通信网络的重要选择。

在 CV-QKD 协议中，发送方 (Alice) 通过高斯调制或离散调制制备相干态量子信号，并将这些量子态通过量子信道传输至接收方 (Bob)。Bob 采用零差检测技术对接收信号的正交分量进行随机测量。量子信道噪声和潜在窃听会导致通信双方测量结果存在差异，需要通过经典信道进行数据协调。其中，高效纠错编码技术对提升密钥安全性和生成率至关重要。LDPC 码因其接近香农极限的优异性能，成为 QKD 系统数据协调的理想选择：在 DV-QKD 中可直接对离散比特序列进行高效纠错[4]，实现较低的误码率；而在 CV-QKD 中需先量化连续变量的测量结果，量化误差导致误码率显著高于 DV 协议。这使得 LDPC 码纠错效率成为 CV-QKD 性能的关键瓶颈，既直接影响密钥生成率，又制约安全传输距离，是 CV-QKD 实用化的主要技术挑战。

收稿日期：2025−04−25；　**修订日期：**2025−06−24

作者简介：努尔比耶太外库力，女，硕士生，主要从事自由空间连续变量量子密钥分发方面的研究。

导师(通讯作者)简介：李明，男，副教授，博士，主要从事量子保密通信、自由空间光通信方面的研究。

1962 年，GALLAGER[5] 提出了 LDPC 码。然而，直到 MACKAY[6] 等“重新发现”了 LDPC 码并证明其性能接近香农极限后，LDPC 码才引起了广泛关注和研究。LDPC 码的核心特点是其稀疏校验矩阵 $\boldsymbol{H}$，其构造方法包括随机构造和结构化构造。随机构造包括 Gallager 构造法[5]、Mackay 构造法[7] 等，结构化构造方法包括基于有限几何的设计方法[8] 和基于循环矩阵的构造方法[9] 等。尽管随机构造的 LDPC 码存在较高的编码复杂度，但其稀疏校验矩阵结构和高效的置信传播 (Belief Propagation, BP) 迭代译码算法，使其在 CV-QKD 中展现出显著优势。目前，降低编解码复杂度是该领域的关键研究方向。

1　LDPC 码在 CV-QKD 数据协调中的应用

2006 年，BLOCH 等[10] 从信道编码理论出发，将数据协调建模为带有侧信息的信道编码问题，并提出基于 LDPC 码的迭代多级编码/多级译码 (Multi-Level Coding/Multi-Stage Decoding, MLC/MSD) 协调方案。如图 1 所示，该方案将 CV-QKD 协调过程视为特殊信道编码：Alice 通过量子信道 C3 传输信号，同时通过经典信道发送 LDPC 纠错信息作为侧信息，Bob 则结合接收信号和侧信息进行纠错。这种设计的核心优势在于，通过 LDPC 编码交换替代原始数据传输，能显著提升双方数据互信息量，从而实现高效的密钥协商。码率为 R_c 的协调效率定义为：

$$\beta = \frac{R_c}{I(X;Y)} \tag{1}$$

理想情况下，若编码方案达到信道容量，则 $\beta = I(\hat{X};Y)/I(X;Y)$。因此，当编码码率 R_c 逼近 $I(\hat{X};Y)$ 时，该编码方法即为高效。

在协调中，高斯信道容量定义为：

$$C = \frac{1}{2}\log_2(1+SNR) \tag{2}$$

式中：SNR 为信噪比。CV-QKD 系统的信噪比通常极低，传统编码方法难以实现高效协调，因此高效编码方案的设计成为 CV-QKD 的研究重点。根据传输信道特性，CV-QKD 可分为光纤和自由空间两类系统，LDPC 码设计需针对性解决不同挑战：光纤系统主要优化信道损耗和噪声下的译码性能，而自由空间系统需重点解决大气湍流和环境干扰带来的信号随机起伏问题。

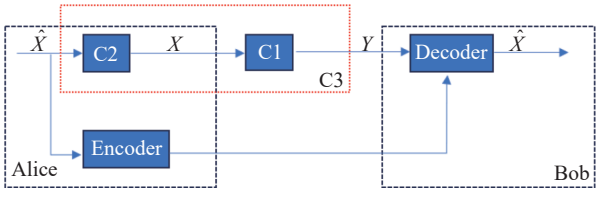

图 1　信道编码角度分析数据协调原理框图

Fig.1　Reconciliation based on channel coding theory

2　光纤 CV-QKD 数据协调中的 LDPC 码

本节系统综述光纤 CV-QKD 系统中 LDPC 码的研究进展。首先，梳理传统 LDPC 码在数据协调中的应用，重点讨论其在低信噪比环境下的性能优化；其次，总结多边型 LDPC 码 (MET-LDPC) 的纠错性能优势；最后，评述基于低速率原图的 LDPC 码设计新思路。

2.1　传统 LDPC 码

2006 年，BLOCH 等[10] 首次将 LDPC 码用于 CV-QKD 系统数据协调中，并通过外信息转移 (EXtrinsic Information Transfer, EXIT) 图表和密度演化对 LDPC 码进行了优化。如图 2 所示，迭代 MLC/MSD-like 协调方案在信噪比 1.76 dB 及量化间隔 16 时，采用 0.86 码率可使协调效率达 88.7%，较文献 [11] 提升 9.7%。理论上，LDPC 码通过密度演化[12] 可逼近信道容量，但实际性能仍存在显著差距，且高纠错概率往往需以牺牲编码码率为代价，然而降低码率会暴露过多比特信息。文献 [10] 基于 EXIT 图[13] 的编码选择策略有效解决了码率与信息泄露的平衡问题，但未涉及计算复杂性的实际约束，这一关键因素直接影响高速密钥分发的实现，亟需深入研究。

LODEWYCK 等[14] 在 2007 年提出的基于 LDPC 码的多级反向协调算法，为光纤 CV-QKD 系统后处理优化提供了重要解决方案。该协调算法具体过程如图 3 所示，其通过将反向协调协议与度分布优化设计的 LDPC 码相结合，在接收端采用 BP 迭代译码算法，实现了显著的性能提升。实验表明，对于 25 km 光纤传输，采用 LDPC 码的多级反向协调实现了 88.7% 的协调效率，密钥生成速率达 2.15 kB/s。该文献提出的多级反向协调框架更为后续研究奠定了重要基础。

现有协调方案[10, 14-15] 用于从连续变量中提取二进制信息，其核心步骤是对连续变量进行量化，随后对离散变量执行纠错处理。理论上，当量化在高维空

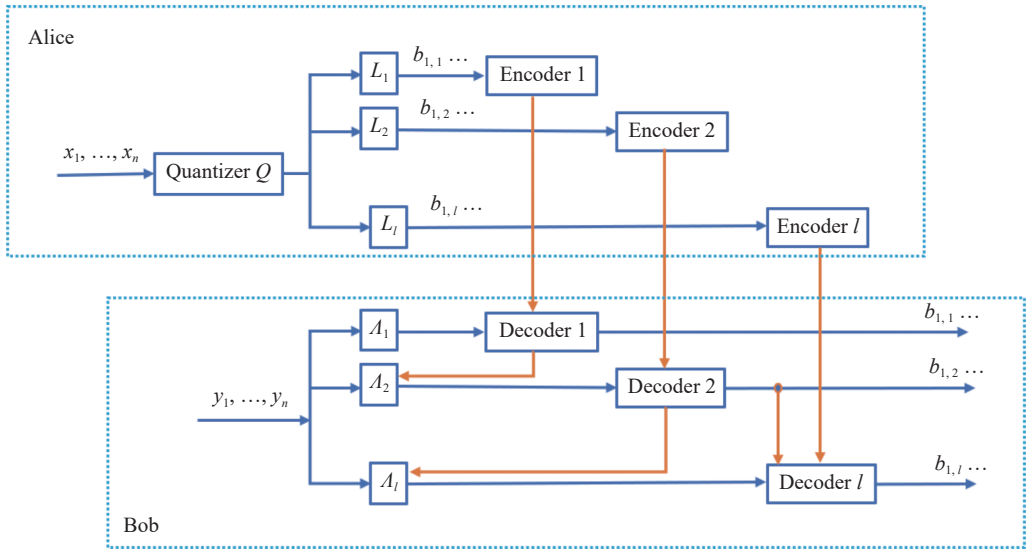

图 2 MLC/MSD-like 协调方案框图

Fig.2 Diagram of the MLC/MSD-like reconciliation scheme

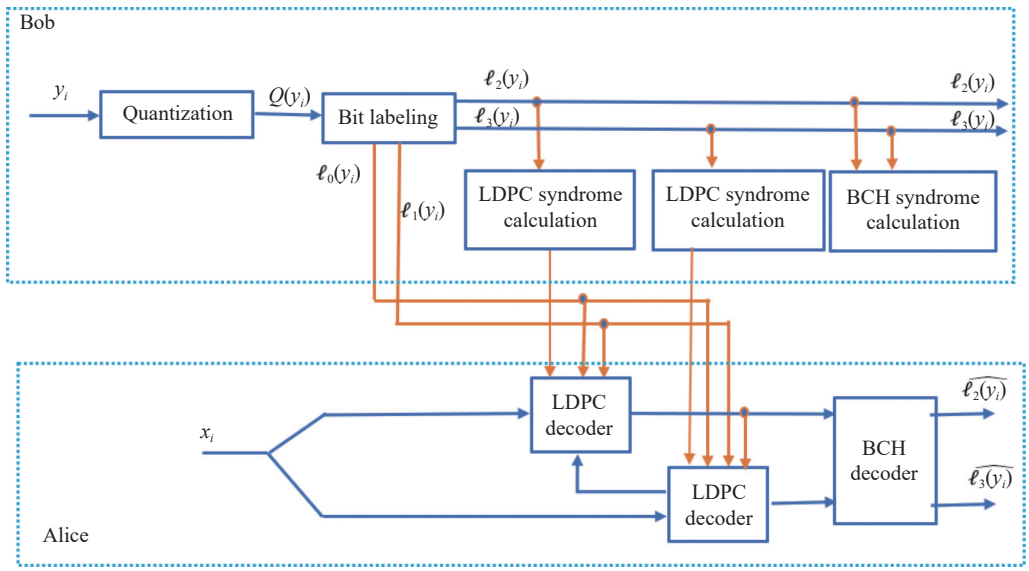

图 3 基于 LDPC 编码的多级反向协调原理框图

Fig.3 Diagram of the multi-level reverse reconciliation based on LDPC coding

间 $\mathbb{R}^d (d \gg 1)$ 中实施时，该方法能够实现每脉冲超 1 bit 的信息传输，并提取全部可用信息。然而，在实际应用中，当$d \gg 1$时，计算复杂度急剧增加，导致该方法的实用性受限。因此，先前协议通常采用$d = 1$，致使协调效率较低，传输范围限制在约 30 km。2008 年，LEVERRIER 等[16]对这一问题进行了探讨，提出基于八元代数特性的八维 $(\mathbb{R}^8)$ 协调方案。该方案的核心思路是将传统离散协调扩展至多维域，其具体实现架构如图 4 所示。研究发现，归一化的随机向量$\boldsymbol{x}/|\boldsymbol{x}|$在$\mathbb{R}^d$的单位球面$S^{d-1}$上具有均匀分布。如果该球面码均匀分布，则可以等价于 DV-QKD 协议中的二

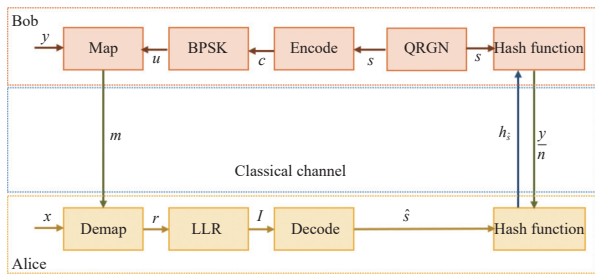

图 4 多维协调原理框图

Fig.4 Diagram of the multi-dimensional reconciliation

进制变量，从而能应用 DV-QKD 的一些特点。在球形编码中将二进制编码转换为二进制球形编码，典型方法是通过将$\mathbb{F}_2^n$映射到n维球面上的同构图像。映射过程为$\mathbb{F}_2^n \longrightarrow S^{n-1} \subset \mathbb{R}^n, (b_1, \cdots, b_n) \longrightarrow ((-1)^{b_1}/\sqrt{n}, \cdots, (-1)^{b_n}/\sqrt{n})$，如图 5 所示，其中$X_1$和$X_2$表示 Alice 发送的两个连续状态。多维协议[16]是在编码之前进行巧妙的旋转，将信息映射到球面上，球面可以很好地分离和保持对称性。

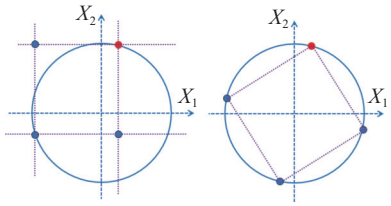

图 5 将$\mathbb{F}_2^n$映射到 n 维球面上的同构图像方法示意图

Fig.5 schematic of the isomorphic mapping method from $\mathbb{F}_2^n$ to an n-dimensional spherical surface

BAI 等[17]在 2017 年提出了一种基于高性能不规则 LDPC 码的优化协调方案。该方案采用离散的密度演化算法优化节点度分布，针对不同码率需求分别设计编码方案：低码率直接采用随机构造的长块 LDPC 码，高码率则通过准循环扩展技术从基础矩阵生成。实验结果表明，该方案在信噪比 1~3 dB 范围内实现了超 95% 的协调效率，同时帧误码率控制在 24% 以下。这一突破显著提升了 CV-QKD 系统的协调性能，为长距离量子密钥分发提供了有效的技术解决方案。

2.2　MET-LDPC 码

高斯调制 CV-QKD 协议在低信噪比 (SNR<0.1) 下的协调效率急剧下降至 70% 以下[2]。针对这一限制，2011 年，LEVERRIER 等[18]提出了非高斯调制方案。该研究通过四态协议[19]结合优化的纠错编码，显著提升了 CV-QKD 系统在长距离传输中的性能，但该方案存在调制方差受限的问题[18-19]。为此，JOUGUET 等[20]提出了基于 MET-LDPC[21]码的多维协调方案，其中多边 (MET) 指的是 LDPC 码 tanner 图中校验节点与变量节点连接的边数。该方案采用 MET-LDPC 码在极低码率 (0.02) 和低信噪比 (0.029) 下实现了 96.9% 的协调效率，理论上可以将传输距离扩展至 140 km。随后，学者们首次实验演示了 80 km 的传输距离[22-23]。

传统 LDPC 码的设计主要针对二进制对称信道，其效率特性呈现明显的"阶梯效应"：每种编码方案仅在特定误码率区间内保持高效，且最大协调效率仅能在接近编码阈值时实现。这种局限性导致 LDPC 码难以适应 CV-QKD 系统中宽范围变化的误码率需求，从而制约其在数据协调中的整体性能。为解决这一问题，WANG 等[24]于 2018 年首次提出了一种自适应码率协调方案。该方案采用打孔 (puncturing) 和缩短 (shortening) 技术[25]，动态调整打孔位 (P) 和缩短位 (S) 实现码率自适应 (原理如图 6 所示)，有效解决了传统固定码率 MET-LDPC 码[20]的性能局限。实验[24]表明，这种动态调整机制在 SNR 波动环境下仍能保持稳定的高效协调性能，显著提升系统的鲁棒性。当码率分别为 0.1、0.05 和 0.02 时，相应的协调效率可达到 93.5%、95.4% 和 96.4%。

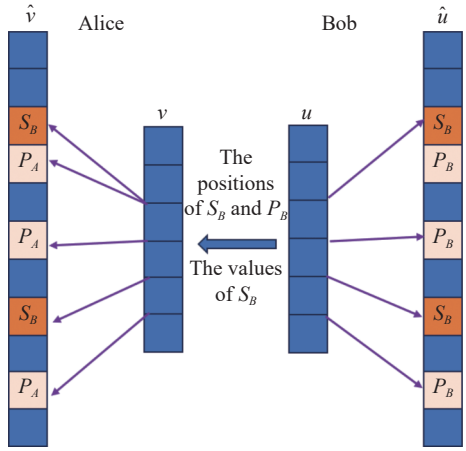

图 6 打孔和缩短技术原理框图

Fig.6 Schematic of the puncturing and shortening technologies

WANG 等[26]在 GPU 加速的 MET-LDPC 码纠错方面取得了重要突破。主要内容如下：首先，采用 GPU 并行计算架构，实现了 64 个码字同步解码；其次，优化了 BP 解码算法，降低计算复杂度；最后，重构了奇偶校验矩阵 $\boldsymbol{H}$ 的存储结构，将其分为变量节点和映射关系两个文件存储，有效改善了内存访问连续性。实验结果表明，在 10^6 码长和 100~200 次迭代条件下，系统在码率 0.1、0.05 和 0.02 时分别实现了 30.39 Mbits/s、21.23 Mbits/s 和 16.41 Mbits/s 的解码速度 (实验配置见图 7)。这项技术不仅解决了长码字解

码的内存瓶颈问题，更为 CV-QKD 系统实时高效纠错提供了切实可行的解决方案。

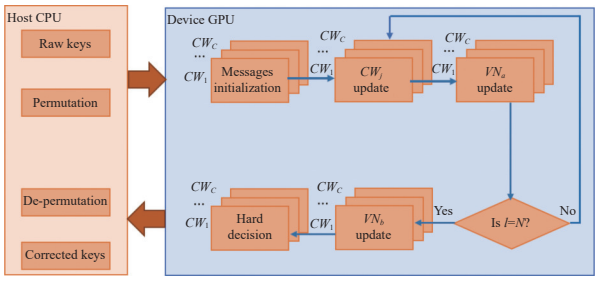

图 7 基于 GPU 的并行解码过程原理框图

Fig.7 Principle of the GPU-based parallel decoding process

2018 年，MILICEVIC 等[27]提出了一种基于 GPU 加速的 QC-MET-LDPC 设计方案。该方案采用的循环码设计与 QC-LDPC[9]相似，但针对量子通信的特殊需求进行了优化，显著提升了硬件解码效率。研究团队在 NVIDIA GeForce GTX1 080 GPU 平台上对所提方案进行验证，充分利用 GPU 的并行计算能力，实现了 7.16 kbit/s 的信息吞吐量。实验结果表明，在 142 km 的最大传输距离下，采用码率 0.02 的 QC-MET-LDPC 码可实现 6.64×10^{-8} bit/pulse 的密钥速率和 99% 协调效率的优异性能。

2020 年，LI 等[28]提出了基于 GPU 的分层解码方案，并实现了 QC-MET-LDPC 码解码效率的显著提升。该研究主要创新性设计如下：1) 优化了奇偶校验矩阵的存储结构，采用子矩阵合并技术减少内存占用；2) 实现了多码字并行解码架构，充分利用 GPU 计算资源。实验数据表明，在 10^6 码长条件下，该方案对码率 0.1 (100 次迭代)、0.05 (150 次迭代) 和 0.02 (200 次迭代) 的 LDPC 码分别实现了 64.11 Mbits/s、48.65 Mbits/s 和 39.51 Mbits/s 的解码速度，与文献[26-27]相比提升约 2 倍。

2021 年，MANI 等[29]提出了基于 G-EXIT 图[30]的 MET-LDPC 码优化方案，显著提升了 CV-QKD 系统性能。该研究针对高斯调制特性，设计了一系列具有优异渐近性能的 MET-LDPC 码 (码率 0.1、0.05、0.02 和 0.01)。实验结果表明，在码率 0.02 和信噪比 5.93 dB 下实现了 98.8% 协调效率，较传统方法[20]提升显著。特别在 0.01 码率时突破 170 km 传输距离，误码率 0.26 以下仍保持 95% 协调效率，为长距离量子通信提供了关键技术支撑。

2022 年，WANG 等[31]实现了城域 CV-QKD 系统的重大突破，通过高效后处理方案 (包括多维协调、优化的 MET-LDPC 纠错码和高效隐私放大算法) 在 5~25 km 传输距离内实现了 Gbps 量级的密钥速率。实验结果显示，采用线性信道假设和半定规划两种安全分析方法时，密钥速率分别达到 52.48~190.54 Mbps 和 21.53~233.87 Mbps，且协调效率始终保持在 95% 以上。该研究首次验证了高密钥率 CV-QKD 系统在城域范围内的可行性，为未来大规模量子保密通信网络的建设提供了重要的技术支撑。

综上所述，光纤 CV-QKD 系统中 LDPC 码的研究进展如表 1 所示。

表 1 光纤 CV-QKD 数据协调中 LDPC 码的研究进展

Tab.1 Progress on LDPC codes for data reconciliation in fiber CV-QKD

Year	Method	Code rate	*SNR*	Reconciliation efficiency β
2006 [10]	SEC/LDPC	0.86	3	88.7%
2007[14]		0.94	-	88.7%
2008 [16]	MD/LDPC	0.26	-	89%
2011[21]	MD/MET-LDPC	0.02	0.029	96.9%
2015[23]		0.02	-	96.9%
2017[17]	SEC/LDPC	-	1/3	95.0%/95.2%
2018 [23]	MD/MET-LDPC	0.1/0.05/0.02	0.159/0.075/0.029	93.5/%95.4/%96.4%
2018[26]		0.1/0.05/0.02	0.160/0.075/0.029	93.4%/95.8%/96.9%
2018[27]	MD/QC-MET-LDPC	0.02	0.028 4	99%
2020 [29]		0.1/0.05/0.02	0.161/0.076/0.03	92.9%/94.6%/93.8%
2021[30]	MD/MET-LDPC	0.01/0.02/0.05	0.014/0.028/0.073	97.8%/98.8%/97.8%
2021[32]		0.07/0.06/0.03	0.119/0.094/0.047	95.5%/95%/95.1%
2023[34]	MD/TBP-LDPC	0.01/0.1	0.007/0.080	

2.3 低速率基于类型的原型图 LDPC 码

传统低速率 LDPC 码设计存在优化过程复杂、搜索空间大等问题[29]。因此，针对特定需求设计低速率 LDPC 码是一项艰巨的任务。降低编码设计复杂度的一种方法是采用原型图 LDPC 码。然而，在设计低速率原型图 LDPC 码时，原型图的大小会随着码率的降低呈二次方增长，导致搜索空间指数增加，使得传统的原型图数值优化技术难以应用。为了解决这一问题，GUMUS 等[32]提出了基于类型的原型图 (Type-Based Protograph, TBP) 方法，其创新在于将原型图节点划分为固定节点类型和可优化节点类型，通过约束条件保持节点度数不变。这种结构化设计方法通过调整校验节点和变量节点出现的次数，实现不同码率设计。如图 8 所示，该方法成功实现了码率 0.1 的 TBP 设计。研究表明，TBP-LDPC 码在低码率场景下展现出显著优势：在帧误码率 0.1 时实现 0.12 dB 的性能增益，且误码率随码率降低而下降。该方法对高码率编码效果较差，但通过扩展 TBP 结构可获得改善。这一成果为 CV-QKD 系统在低信噪比条件下的高效纠错编码设计提供了关键理论支撑和技术实现路径。

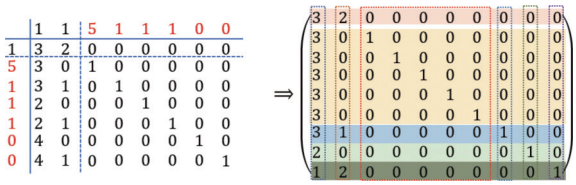

图 8 类型描述转换为速率 0.1 的 TBP 示例

Fig.8 Example of converting type description into rate 0.1 TBP

2023 年，CIL 等[33]针对降低解码复杂度进行了研究，提出了迭代相关缩放最小和算法 (Iteration-Dependent Min-Sum Algorithm, ID-MSA) 有效解决了 CV-QKD 系统解码复杂度问题。该算法通过动态调整缩放系数，在保持低复杂度的同时实现了接近和积算法 (Sum-Product Algorithm, SPA) 的性能：在帧误码率 0.1 条件下，对于码率 0.01 和 0.1 的 TBP-LDPC 码[32]，ID-MSA 与 SPA 的性能差距分别仅为 0.059 dB 和 0.068 dB，比较传统 MSA 算法提升显著 (差距从 5.2 dB 降至 0.059 dB)。然而，简化的 BP 算法 (如缩放 MSA 算法) 通常表现出次优性能[33]，这给长距离 CV-QKD 系统中的 LDPC 解码器带来了实际的硬件挑战。为此，2024 年，CIL 等人[34]提出了一种新颖的对数-对数域和积 (Log-Log Domain Sum-Product Algorithm, Log-Log Domain SPA) 算法，与传统的 SPA 相比，该算法在不增加解码迭代次数或解码复杂度的情况下，能够将信息表示的精度降低至少 25%。

同年，CIL 等[35-36]提出 Raptor-like LDPC 码，解决了 CV-QKD 系统中的码率自适应问题。该方案通过新型编码结构设计，对于给定的 *SNR*，能够在 0.01~0.2 码率范围内自适应选择码率，实现最佳协调效率 (>95%)。配套开发的开源 C++库为实际应用提供了完整解决方案，既保持了编码性能，又支持动态信道条件自适应。

3 自由空间 CV-QKD 数据协调中的 LDPC 码

光纤 CV-QKD 由于光子在传输过程中受到光纤固有损耗和双折射效应的影响，传输距离限于百千米量级。与之相比，自由空间可以提供更广阔的覆盖范围，实现千千米级的量子通信。此外，自由空间信道不受地理条件限制，适用于星地量子链路和城域量子网络的构建。然而，自由空间传输面临大气湍流和天气变化等挑战，影响信号稳定性。近年来的研究[37-39]在理论和实验层面均取得突破，为自由空间 CV-QKD 的实际应用奠定了基础。

自由空间 CV-QKD 面临的大气湍流效应主要表现为透射率起伏。研究表明，透射率随机波动特性不能用解析模型精确表征[3, 40]。这些动态信道特性对 LDPC 码的设计提出了双重需求：1) 码率的自适应调整能力以应对 *SNR* 波动；2) 增强低 *SNR* 下的纠错性能。测量设备无关的自由空间 CV-QKD 研究[41]进一步表明，后选择策略虽可提升性能，但需要 LDPC 码具备更强的动态适应能力。因此，自由空间 CV-QKD 中的 LDPC 码设计必须兼顾信道自适应性和纠错鲁棒性。近年来，自由空间 CV-QKD 数据协调中 LDPC 码的研究进展如表 2 所示。

2017 年，LOPEZ 等[42]提出了基于自适应码率的自由空间 CV-QKD 系统方案。通过实时监测自由空间光链路的 Rytov 方差调整 LDPC 码率，密钥率从 52.5 kbit/s 提升至 140 kbit/s，增加了 87.5 kbit/s。在弱到中等强度的大气湍流环境中，该自适应码率方案显

著提升了系统性能，展现了巨大的应用潜力。针对自由空间 CV-QKD 系统低信噪比问题，GUO 等[43] 提出了基于准循环累积-重复-累积 LDPC 码[44] 的方案。该方案通过优化原型图校验矩阵结构，在 0.33 码率下实现了 91.02% 的高协调效率，有效提升了系统在低信噪比和弱大气湍流条件下的纠错性能。

离散调制相较于传统的高斯调制在实验实现上具有显著的简化和规模化部署优势，但其安全性分析相对滞后。LIN 等[45] 首次从理论上研究了离散调制方案在直接协调和反向协调协议中的安全性，为后续研究奠定了重要基础。2021 年，LIU 等[46] 提出基于四元相移键控 (Quadrature Phase-Shift Keying, QPSK) 技术的 CV-QKD 协议，通过优化信息泄露控制机制，在渐近极限条件下实现了更佳的信道噪声容忍度性能，同时获得了更高的密钥速率和传输距离。为进一步突破 QPSK 调制对传输距离的限制，GUMUS 等[47] 在 2024 年创新性地提出了自适应高维协调离散调制方案 ($d > 8$)，该研究首先通过理论分析证实高维协调中概率整形正交调幅的性能逼近 QPSK，随后结合 TBP-LDPC 编码与高维协调技术，通过优化虚拟信道和穿刺技术实现码率动态自适应。研究结果表明，与传统多维协调相比，高维协调显著提高了密钥速率，最大提升幅度达 165%。此外，通过优化协调效率，密钥速率进一步提高 7.6%。

表 2 自由空间 CV-QKD 数据协调中 LDPC 码的研究进展

Tab.2 Progress on LDPC codes for data reconciliation in free-space CV-QKD

Year	Method	Code rate	*SNR*	Reconciliation efficiency β
2017, LEYVA[42]	LDPC	0.33-0.75	-	-
2020, YING[43]	QC-LDPC	0.33/0.32/0.31	0.65/0.64/0.62	91%/89%/88%
2024, KADIR[47]	TBP-LDPC	0.2-0.3	-	94%

4 结 论

文中系统综述了 CV-QKD 系统数据协调中 LDPC 码的研究进展，重点阐述了其在光纤和自由空间信道中的性能优化策略。LDPC 码凭借其接近香农极限的纠错性能，已成为提升 CV-QKD 系统数据协调效率的关键技术。在光纤信道中，传统 LDPC 码通过多级编码实现了 88.7% 以上的协调效率，而 MET-LDPC 码在极低信噪比 (*SNR*=0.029) 下更将效率提升至 96.9%，支持 140 km 长距离传输。自由空间 CV-QKD 方面，自适应码率 LDPC 码结合高维协调技术，使密钥速率最高提升 165%。硬件优化方面，GPU 并行解码技术使处理速度突破 64 Mbits/s，同时 ID-MSA 等简化算法降低了 25% 计算复杂度。

未来研究应重点关注以下方向：1) 新型 LDPC 码结构设计：重点提升低信噪比环境下的纠错性能；2) 动态信道自适应技术：优化 LDPC 码的码率自适应算法，实现对湍流等动态信道特性的实时响应。在自适应码率上可以先构造低码率的校验矩阵，后续根据所需码率选取合适维度的校验矩阵进行编码；3) 硬件加速优化：推进 GPU/FPGA 等并行计算架构在编解码过程中的应用优化；4) 量子技术协同：探索 LDPC 码与量子中继、测量设备无关协议等新技术的融合方案；5) 信道-编码协同设计：突破静态信道假设，建立基于实时湍流监测的自适应编码策略。这些研究方向将系统性地解决 CV-QKD 在复杂信道环境中的关键技术瓶颈，为构建高性能、实用化的量子通信网络提供重要支撑，加速量子通信技术的产业化进程。

参考文献：

[1] BENNETT CH, BRASSARD G. Quantum cryptography: Public key distribution and coin tossing [C]//Proceedings of the IEEE International Conference on Computers Systems and Signal Processing, 1984: 175-179.

[2] WU Zhigeng, LI Ming, YAO Zhenghao, et al. Simulation study on fluctuation characteristics of channel transmittance for free-space continuous-variable quantum key distribution quantum [J]. ***Infrared and Laser Engineering***, 2024, 53(8): 20240210. (in Chinese)

[3] LI M, CVIJETIC M. Continuous-variable quantum key distribution with self-reference detection and discrete modulation [J]. ***IEEE Journal of Quantum Electronics***, 2018, 54(5): 1-8.

[4] ELKOUSS D, LEVERRIER A, ALLAUME R, et al. Efficient reconciliation protocol for discrete-variable quantum key distribution [C]//IEEE international symposium on information theory, 2009: 1879-1883.

[5] GALLAGER R. Low density parity check codes [J]. ***IRE Transactions on Information Theory***, 1962, 8(1): 21-28.

[6] MACKAY D, NEAL R. Near Shannon limit performance of low density parity check codes [J]. ***Electronics Letters***, 1997, 33(6): 457-458.

[7] MACKAY D. Good error-correcting codes based on very sparse matrices [J]. ***IEEE transactions on Information Theory***, 1999, 45(2): 399-431.

[8] KOU Y, LIN S, FOSSORIER M P C. Low-density parity-check codes based on finite geometries: a rediscovery and new results [J]. ***IEEE Transactions on Information Theory***, 2002, 47(7): 2711-2736.

[9] FOSSORIER M P C. Quasi-cyclic low-density parity-check codes from circulant permutation matrices [J]. ***IEEE Transactions on Information Theory***, 2004, 50(8): 1788-1793.

[10] BLOCH M, THANGARAJ A, MCLAUGHLIN S W, et al. LDPC-based secret key agreement over the Gaussian wiretap channel [C]//IEEE International Symposium on Information Theory, 2006: 1179-1183.

[11] BLOCH M, THANGARAJ A, MCLAUGHLIN S W, et al. LDPC based Gaussian key reconciliation [C]//IEEE Information Theory Workshop-ITW'06 Punta del Este, 2006: 116-120.

[12] RICHARDSON T J, SHOKROLLAHI M A, URBANKE R L. Design of capacity-approaching irregular low-density parity-check codes [J]. ***IEEE Transactions on Information Theory***, 2001, 47(2): 619-637.

[13] TEN B S. Convergence behavior of iteratively decoded parallel concatenated codes [J]. ***IEEE Transactions on Communications***, 2001, 49(10): 1727-1737.

[14] LODWYCK J, BLOCH M, GARCIA P R, et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system [J]. ***Physical Review A***, 2007, 76(4): 042305.

[15] VAN A G, CARDINAL J, CERF N. Reconciliation of a quantum-distributed Gaussian key [J]. ***IEEE Transactions on Information Theory***, 2004, 50(2): 394-400.

[16] LEVERRIER A, ALLEAUME R, BOUTROS J, et al. Multidimensional reconciliation for a continuous-variable quantum key distribution [J]. ***Physical Review A***, 2008, 77(4): 042325.

[17] BAI Z, YANG S, LI Y. High-efficiency reconciliation for continuous variable quantum key distribution [J]. ***Japanese Journal of Applied Physics***, 2017, 56(4): 044401.

[18] LEVERRIER A, GRANGIER P. Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation [J]. ***Physical Review A***, 2011, 83(4): 042312.

[19] LEVERRIER A, GRANGIER P. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation [J]. ***Physical Review Letters***, 2009, 102(18): 180504.

[20] JOUGUET P, KUNZ J S, LEVERRIER A. Long-distance continuous-variable quantum key distribution with a Gaussian modulation [J]. ***Physical Review A***, 2011, 84(6): 062317.

[21] RICHARDSON T, URBANKE R. Multi-edge type LDPC codes [C]//Workshop Honoring Prof. Bob McEliece on His 60th Birthday, 2002: 24-25.

[22] JOUGUET P, KUNZ J S, LEVERRIER A, et al. Experimental demonstration of long-distance continuous-variable quantum key distribution [J]. ***Nature Photonics***, 2013, 7(5): 378-381.

[23] FOSSIER S, DIAMANTI E, DEBUISSCHERT T, et al. Field test of a continuous-variable quantum key distribution prototype [J]. ***New Journal of Physics***, 2009, 11(4): 045023.

[24] WANG X, ZHANG Y, LI Z, et al. Efficient rate-adaptive reconciliation for continuous-variable quantum key distribution [J]. ***Quantum Information & Computation***, 2017, 17(13-14): 1123-1134.

[25] ELKOUSS D, MARTINEZ J, LANCHO D, et al. Rate compatible protocol for information reconciliation: An application to QKD [C]//IEEE Information Theory Workshop on Information Theory, 2010: 1-5.

[26] WANG X, ZHANG Y, YU S, et al. High speed error correction for continuous-variable quantum key distribution with multi-edge type LDPC code [J]. ***Scientific Reports***, 2018, 8(1): 10543.

[27] MILICEVIC M, FENG C, ZHANG L, et al. Quasi-cyclic multi-edge LDPC codes for long-distance quantum cryptography [J]. ***NPJ Quantum Information***, 2018, 4(1): 21.

[28] LI Y, ZHANG X, LI Y, et al. High-throughput GPU layered decoder of quasi-cyclic multi-edge type low density parity check codes in continuous-variable quantum key distribution systems [J]. ***Scientific Reports***, 2020, 10(1): 14561.

[29] MANI H, GEHRING T, GRABENWEGER P, et al. Multi-edge-type low-density parity-check codes for continuous-variable quantum key distribution [J]. ***Physical Review A***, 2021, 103(6): 062419.

[30] MEASSON C, MONTANARI A, RICHARDSON T, et al. The generalized area theorem and some of its consequences [J]. ***IEEE Transactions on Information Theory***, 2009, 55(11):

4793-4821.

[31] WANG H, LI Y, PI Y, et al. Sub-Gbps key rate four-state continuous-variable quantum key distribution within metropolitan area [J]. ***Communications Physics***, 2022, 5(1): 162.

[32] GUMUS K, SCHMALEN L. Low rate Protograph-based LDPC codes for continuous variable quantum key distribution [C]//17th International Symposium on Wireless Communication Systems, 2021: 1-6.

[33] CIL E E, SCHMALEN L. Iteration-dependent scaled min-sum decoding for low-complexity key reconciliation in CV-QKD [C]//Optical Fiber Communication Conference, 2024: W4C-8.

[34] CIL E E, SCHMALEN L. Log-log domain sum-product algorithm for information reconciliation in continuous-variable quantum key distribution [C]//58th Annual Conference on Information Sciences and Systems, 2024: 1-6.

[35] CIL E E, SCHAMLEN L. Rate-adaptive protograph-based raptor-like LDPC code for continuous-variable quantum key distribution[C]//Photonic Networks and Devices, 2024: JTu1A-51.

[36] CIL E E, SCHMALEN L. An open-source library for information reconciliation in continuous-variable QKD[DB/OL]. (2024-08-01) [2025-06-24]. https://arxiv.org/abs/2408.00569.

[37] WANG Yi, LI Yuan, MA Jing, et al. Study on performance of circle polarization modulation system with coherent detection in free space optical communication[J]. ***Infrared and Laser Engineering***, 2016, 45(8): 0822004. (in Chinese)

[38] HEIM B, PEUNTINGER C, KILLORAN N, et al. Atmospheric continuous-variable quantum communication [J]. ***New Journal of Physics***, 2014, 16(11): 113018.

[39] LIAO S K, YONG H L, LIU C, et al. Long-distance free-space quantum key distribution in daylight towards inter-satellite communication [J]. ***Nature Photonics***, 2017, 11(8): 509-513.

[40] LI M, ZHANG P, WANG T. Evaluation of atmospheric coherent length of free-space optical links by using phase fluctuation [J]. ***Optics Express***, 2024, 32(5): 7243-7253.

[41] YAO Z, LI M, WU Z, et al. Continuous-variable measurement-device-independent quantum key distribution over fluctuated free space quantum channels [J]. ***Optics Communications***, 2025, 575: 131294.

[42] LOPEZ L J A, ARVIZU M A, SANTOS A J, et al. Improved performance of the cryptographic key distillation protocol of an FSO/CV-QKD system on a turbulent channel using an adaptive LDPC encoder [J]. ***Revista Mexicana Defísica***, 2017, 63(3): 268-274.

[43] GUO Y, WANG X, XIE C, et al. Free-space continuous-variable quantum key distribution in atmospheric channels based on low-density parity-check codes [J]. ***Laser Physics Letters***, 2020, 17(4): 045203.

[44] ABBASFAR A, DIVSALAR D, YAO K. Accumulate-repeat-accumulate codes [J]. ***IEEE Transactions on Communications***, 2007, 55(4): 692-702.

[45] LIN J, UPADHYAYA T, LUTENHAUS N. Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution [J]. ***Physical Review X***, 2019, 9(4): .041064.

[46] LIU W B, LI C L, XIE Y M, et al. Homodyne detection quadrature phase shift keying continuous-variable quantum key distribution with high excess noise tolerance [J]. ***PRX Quantum***, 2021, 2(4): 040334.

[47] GUMUS K, DOU R F J, VAN V V, et al. Rate-adaptive reconciliation for experimental continuous-variable quantum key distribution with discrete modulation over a free-space optical link [J]. ***Journal of Lightwave Technology***, 2025, 43(8): 3564-3573.

Advances in LDPC codes for continuous-variable quantum key distribution: a comprehensive review

NUERBIYE Taiwaikuli [1,2], LI Ming[1,2*], XU Shengzhi[1,2], CHEN Huimin[1,2]

(1. College of Electronic and Communication Engineering, Tianjin Normal University, Tianjin 300387, China;
2. Tianjin Key Laboratory of Wireless Mobile Communications and Power Transmission, Tianjin Normal University, Tianjin 300387, China)

Abstract:

Significance Continuous-variable quantum key distribution (CV-QKD) has emerged as a prominent research focus in quantum communication, owing to its cost-effectiveness and compatibility with existing optical infrastructure. Nevertheless, achieving efficient data reconciliation under low signal-to-noise ratio (SNR) conditions remains a critical challenge impeding its widespread deployment. Low-density parity-check (LDPC) codes, recognized as a state-of-the-art error correction technique, have demonstrated significant potential for enhancing post-processing efficiency in CV-QKD systems. Leveraging their sparse parity-check matrix structure and iterative belief propagation decoding, LDPC codes enable robust error correction during quantum signal transmission, thereby optimizing the reconciliation process. This comprehensive review systematically examines recent advancements in LDPC code applications for both fiber-optic and free-space CV-QKD systems. The review analyzes key developments in code design, decoding algorithms, and implementation strategies that have contributed to improved reconciliation performance. Furthermore, The study identify promising research directions that could address current limitations and facilitate the transition of CV-QKD technology from experimental demonstrations to practical commercial applications.

Progress The evolution of LDPC codes in CV-QKD reconciliation can be categorized into three transformative phases. Initially, traditional LDPC codes demonstrated promising results, achieving reconciliation efficiencies of up to 88.7% at an SNR of 1.76 dB. However, their performance degraded significantly in ultra-low SNR regimes (<0.1 dB), limiting their applicability for long-distance quantum communication. The second phase marked a breakthrough with the introduction of multi-edge-type (MET) LDPC codes, which exhibited superior performance in low-SNR conditions. These codes achieved remarkable reconciliation efficiencies of 96.9% at an SNR of 0.029 dB, enabling secure key distribution over distances extending to 140 km. Further enhancements were realized through GPU-accelerated quasi-cyclic MET-LDPC (QC-MET-LDPC) variants, which pushed reconciliation efficiencies close to 99% while maintaining high processing speeds. For free-space CV-QKD systems, the dynamic and unpredictable nature of atmospheric turbulence poses additional challenges. Adaptive-rate LDPC codes have been developed to mitigate these effects, dynamically adjusting code rates in response to fluctuating channel conditions. These adaptive schemes have demonstrated significant improvements, boosting key rates by 87.5 kbit/s in experimental settings. Moreover, the integration of type-based-protograph (TBP) LDPC codes with high-dimensional reconciliation techniques has further enhanced performance, increasing secure key rates by up to 165% compared to traditional methods.

Conclusions and Prospects LDPC codes have firmly established themselves as the foundational technology for achieving high-efficiency reconciliation in CV-QKD systems. The development of MET-LDPC codes and structured variants such as QC-MET and TBP LDPC codes has demonstrated transformative capabilities,

delivering near-optimal reconciliation efficiencies (>96%) even in challenging low-SNR conditions (<0.03 dB). These advancements have been instrumental in extending secure transmission distances beyond 140 km in fiber-based systems while maintaining robust performance in turbulent free-space channels. Moving forward, five key research directions is critical for future development: 1) Innovative LDPC architectures, such as hybrid Quasi-Cyclic Accumulate-Repeat-Accumulate (QC-ARA) designs, to bridge the efficiency gap in ultra-low-SNR regimes (<0.01 dB); 2) Dynamic adaptation mechanisms leveraging machine learning for real-time optimization under channel fluctuations; 3) Hardware-algorithm co-design, aiming for high-throughput (>1 Gbps) FPGA/ASIC implementations with improved energy efficiency; 4) Cross-layer integration strategies that unify LDPC optimization with discrete modulation and post-processing to maximize end-to-end key rates; and 5) Synergy between quantum-classical network architectures, including quantum repeaters and measurement-device-independent protocols, to enhance scalability and practicality. To overcome these challenges, researchers must focus on optimizing LDPC code performance, developing adaptive reconciliation protocols, and improving hardware implementations. These advancements will enable the transition from experimental CV-QKD systems to practical, high-speed quantum networks, establishing LDPC codes as essential components of future-proof cryptographic infrastructure.

Key words: quantum communication; continuous-variable quantum key distribution; data reconciliation; low-density parity-check code