arXiv:2305.00956v1 [cs.IT] 1 May 2023

面向能量-时间纠缠量子密钥分发的非二元 LDPC 码设计

Debarnab Mitra、Lev Tauz、Murat Can Sarihan、Chee Wei Wong 和 Lara Dolecek 电气与计算机工程系，加利福尼亚大学洛杉矶分校，美国 电子邮箱：debarnabucla@ucla.edu、levtauz@ucla.edu、mcansarihan@ucla.edu、cheewei.wong@ucla.edu 和 dolecek@ee.ucla.edu

摘要——**在能量-时间纠缠量子密钥分发（QKD）中，两个用户根据纠缠光子对的到达时间（离散化为符号）提取共享秘密密钥。在先前的工作中，Zhou 等人提出了一种多级编码（MLC）方案，将观测到的符号分割为比特层，并利用二元低密度奇偶校验（LDPC）码对符号进行协调。尽管二进制低密度奇偶校验码能够实现低时延的密钥生成，但将符号分割为比特会由于错误传播而导致密钥生成率损失。此外，现有的低密度奇偶校验码未能充分利用 QKD 信道的特性来优化密钥率。本文首先将 MLC 方案推广为非二元（NB） MLC 方案，该方案包含由非二元符号构成的层，并使用非二元低密度奇偶校验码，从而缓解上述问题。我们表明，NB-MLC 方案为系统设计提供了灵活性。此外，我们还表明，每层采用较小符号大小的 NB-MLC 方案能够在时延与密钥率之间实现最佳折中。随后，我们提出一种联合优化非二元低密度奇偶校验码的码率与度分布的框架，该框架针对 QKD 信道进行了定制，因而能够获得高于先前工作的密钥率。**

I. 引言

量子密钥分发（QKD）为两位用户 Alice 和 Bob 在存在窃听者 Eve 的情况下，通过量子通信信道安全地共享密钥提供了一种基于物理原理的方式 [1]–[3]。能量-时间纠缠 QKD（ET-QKD）协议因能够从生成的纠缠光子对中提取多个比特而受到学界广泛研究 [3], [4]。总体而言，ET-QKD 协议包含以下步骤 [5]：i）第一步称为生成，Alice 和 Bob 利用量子信道生成原始密钥，这些密钥以符号序列表示。由于量子信道存在缺陷，Alice 和 Bob 的原始密钥在某些位置上可能不一致；ii）第二步称为信息协调 （IR），Alice 和 Bob 通过公开信道（Eve 可以访问）进行通信，以协调原始密钥；iii）第三步称为隐私放大（PA），Alice 和 Bob 根据 Eve 掌握的信息提升协调密钥的隐私性，从而生成最终的共享秘密密钥。信道编码用于信息协调步骤，以确保 Alice 和 Bob 得到相同的符号序列。与 [5], 类似，本文聚焦于协议的信息协调步骤，并假设在该步骤中通信m 比特后，隐私放大会使协调密钥的长度减少 m 比特，从而得到共享秘密密钥。系统的密钥率 定义为 Alice 和 Bob 在隐私放大后获得的共享秘密密钥的平均长度。

一种为获得高密钥率而提出的有前景的编码框架称为多级编码（MLC）方案 [5], 该方案已在诸如 [3], [6]的工作中得到研究。在 MLC 方案中，生成步骤后的符号序列被转换为多个比特层，随后使用二进制低密度奇偶校验码依次对每个比特层进行协调。二进制低密度奇偶校验码具有低复杂度和快速的译码算法，因此能够降低密钥生成的时延和复杂度。然而，MLC 编码方案会受到错误传播的影响：其中一个比特层中的译码错误会导致后续比特层出现译码错误，从而降低密钥率。与采用二进制低密度奇偶校验码的 MLC 方案不同，直接对生成符号进行编码的非二进制（NB）低密度奇偶校验码不会受到错误传播的影响。因此，NB-LDPC 码能够自然地实现更高的密钥率。然而，生成步骤中的符号可能属于大小高达 2^{10} 的伽罗瓦域，并且已知非二进制低密度奇偶校验码的迭代译码具有非常高的复杂度（关于域大小 [7]呈对数线性），从而导致密钥生成具有较高的时延。因此，在需要低时延的 QKD 应用中，例如 [8], [9], 具有大域大小的基线 NB-LDPC 码并不理想。

除了上述时延与密钥率之间的权衡之外，先前在 ET-QKD 协议的信息协调步骤中使用的低密度奇偶校验码（LDPC）尚未充分利用 ET-QKD 信道的特性。例如， [5] 采用了未经优化的标准 LDPC 系综。类似地，空间耦合低密度奇偶校验码、不规则重复累积码、空间耦合不规则重复累积码以及多边类型码也已在连续变量量子密钥分发（CV QKD）中得到讨论 [10], [11]。然而，这些研究主要关注二元输入加性高斯白噪声（BIAWGN）等信道模型，而这些模型与 ET-QKD 信道并不匹配 [12]。

本文所考虑的 ET-QKD 问题的一个独特性质是，系统的密钥率与码率和帧错误率 (FER) 性能都密切相关。图 2 展示了随机低密度奇偶校验码在不同码率下获得的帧错误率和密钥率。从图中可以看出，提高码率即使以更高的帧错误率为代价，也能提升密钥率；这一现象在二进制低密度奇偶校验码和非二元低密度奇偶校验码中均可观察到。此外，密钥率的最大值出现在相对较大的帧错误率 ($\sim 5\%$) 下。对于给定码率，传统的码设计方法是将帧错误率降至很小的值，而在这种情况下，目标是联合优化码率和帧错误率，以获得最大的密钥率。

已知低密度奇偶校验码的度分布会影响其帧错误率性能。基于码阈值的低密度奇偶校验码度分布优化技术（例如，[13]）会针对固定码率优化度分布，因此并不直接适用于当前需要联合优化码率和帧错误率的 ET-QKD 问题

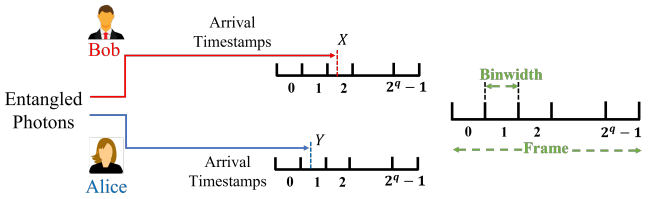

图 1：QKD 系统模型。光子的到达时间采用脉冲位置调制进行离散化。每帧包含 2^q 个时间槽，帧间隔称为分箱宽度。

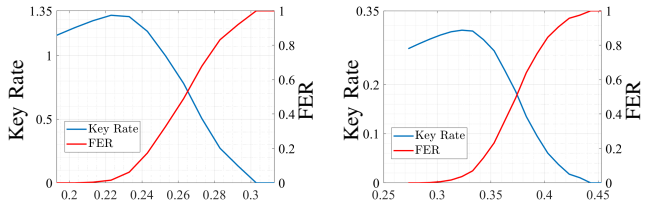

图 2：密钥率和帧错误率随码率的变化。左图：(2^q) 中的非二元低密度奇偶校验码；右图：二元低密度奇偶校验码。两幅图中的密钥率均在帧错误率约为 0.05 时达到最大值。

此外，优化后的度分布是针对非量子密钥分发信道设计的（例如，[13] 中的二元输入加性高斯白噪声信道），正如我们在第五节所展示的那样，这些度分布无法带来较高的密钥率。

在本文中，我们采用双管齐下的方法，缓解上述时延与密钥率之间的权衡问题，以及考虑 ET-QKD 信道特性的码设计问题。首先，我们将 [5] 的 MLC 方案推广为非二元 MLC 方案：在生成步骤之后，将符号拆分为多个层，每层中的非二元符号属于较小的伽罗瓦域。NB-MLC 方案可根据每层的符号大小，在时延与密钥率之间实现自然权衡，从而为系统设计提供灵活性。此外，我们表明，与全二元方案 [5] 以及不进行分层的全非二元方案相比，每层符号大小较小的 NB-MLC 方案能够获得更高的密钥率。其次，我们提出一种基于差分进化 [14] 的联合码率与度分布优化（JRDO）框架，用于构造 NB-MLC 方案各层中的非二元低密度奇偶校验码。JRDO 框架利用 QKD 信道信息；我们证明，与 MLC 方案 [5] 中使用的低密度奇偶校验码，以及采用针对传统信道（如二进制输入加性高斯白噪声信道）优化的度分布所获得的密钥率 [13] 相比，该框架能够获得更高的密钥率。本文其余部分安排如下：第二节介绍预备知识和系统模型；第三节描述 NB-MLC 方案；第四节介绍 JRDO 框架；第五节给出仿真结果；最后，第六节总结全文。

II. 预备知识与系统模型

1) ET-QKD系统模型：如图1所示，在ET-QKD[3]，中，能量-时间纠缠光子对由第三方在生成步骤中生成。随后，Alice和Bob各自接收光子对中的一个光子，并记录所接收光子的到达时间。原始密钥信息由到达时间推导得出。在这种方法中，Alice和Bob双方先同步其时间线，然后将时间离散化为时间帧，其中每个时间帧进一步划分为大小相等的 2^q 时间槽，q 为正整数。Alice 和 Bob 仅保留双方都检测到单个光子到达的时间帧，并丢弃所有其他时间帧。随后，根据接收到的光子在每个时间帧内所处的时间槽编号，将未丢弃时间帧中的光子到达时间转换（离散化）为 $\mathbb{GF}(2^q)$ 中的一个符号。然后，将 Alice 和 Bob 接收到的离散化序列划分为块，每个块包含 N 个符号，其中 N 为码长。设$\mathbf{X} = \{X_1, \ldots, X_N\}$、$X_i \in \mathbb{GF}(2^q)$ 和$\mathbf{Y} = \{Y_1, \ldots, Y_N\}$、$Y_i \in \mathbb{GF}(2^q)$ 分别为 Alice 和 Bob 记录的长度为 N 的序列。由于生成步骤中的不完善（例如定时抖动、传输损耗 [5]），$\mathbf{Y}$ 是$\mathbf{X}$的噪声版本。我们假设序列$\mathbf{X}$ 和$\mathbf{Y}$ 是无记忆的，并且每个 Y_i 都是 ET-QKD 信道的输出，该信道由转移律 $P_{Y|X}$ 和输入 X_i表征。

基于非二元低密度奇偶校验码的简单信息协调协议在 $\mathbb{GF}(2^q)$ 中的流程如下。Alice 通过公开信道向 Bob 发送 $\mathbf{S} = \mathbf{HX}$（Eve 可以访问该信道），其中 $\mathbf{H} \in \mathbb{GF}(2^q)^{M\times N}$ 是非二元低密度奇偶校验码的校验矩阵。Bob 使用接收到的 $\mathbf{S}$ 和旁信息 $\mathbf{Y}$ 对 $\mathbf{X}$ 进行译码。在 Slepian-Wolf（SW）问题 [16] 中会遇到利用旁信息进行低密度奇偶校验译码的情况。SW 低密度奇偶校验译码与传统低密度奇偶校验信道码中使用的和积译码器非常相似，区别主要在于对数似然消息以及校验节点到变量节点的消息的初始化方式不同。有关 SW 低密度奇偶校验译码的详细信息，请参阅 [16]。非二元低密度奇偶校验码的目标是在确保向 Eve 泄露的信息最少的同时，使译码输出以较高概率等于 $\mathbf{X}$。最后，序列 $\mathbf{X}$ 就是传递至隐私放大步骤的协调密钥。上述方案的密钥率 r（每光子比特数）（类似于 [5]）如下所示：

$$r = q(1-E)\frac{N-M}{N}, \tag{1}$$

其中，E 是纳入$\mathbf{X}$解码的帧错误率。请注意，我们在式（1）中减去 M，因为 M 个符号是通过公开信道发送的，因此会因 PA 而损失。

2) ET-QKD 信道：本文使用来自实际 ET-QKD 系统测试平台 [4]的经验数据，直接估计信道转移规律 $P_{Y|X}$。对于感兴趣的读者，[12] 中的作者展示了一种建模方法，该方法能够较好地近似 ET-QKD 信道。简而言之，ET-QKD 信道是由局部信道和全局信道构成的混合信道，二者分别服从高斯分布和均匀分布。均匀分布导致我们的系统信噪比较低，进而造成较高的运行帧错误率（$\sim 1-10\%$）。请注意，ET-QKD 信道不同于加性高斯白噪声、二元对称信道等传统信道。因此，针对这些信道优化的码未必最适用于 ET-QKD 信道，我们将在第五节对此进行说明。

3）非二元低密度奇偶校验码：定义在 $\mathbb{GF}(2^q)$ 上的非二元低密度奇偶校验码由一个稀疏校验矩阵 $\mathbf{H} \in \mathbb{GF}(2^q)^{M\times N}$ 定义。矩阵 $\mathbf{H}$ 具有一个 Tanner 图表示，该表示由以下部分组成。

由 M 个校验节点（CN）和 N 个变量节点（VN）组成，分别对应$\mathbf{H}$的行和列。如果$\mathbf{H}$ 中的相应元素非零，则校验节点与变量节点之间通过一条边相连，并且该边还标记有对应的非零元素。编码的变量节点与校验节点之间的连接关系由度分布 $L(x) = \sum_d L_d x^d$ 和$P(x) = \sum_d P_d x^d$表示，其中 L_d 和 P_d 分别表示连接到度为 d的变量节点和校验节点的节点比例。该编码的码率 R由 $R = 1 - \frac{L'(1)}{P'(1)}$给出。编码的帧错误率（FER）性能取决于度分布$L(x)$ 和 $P(x)$。在本文中，我们对码率 R 和变量节点度分布 $L(x)$进行优化。对于给定的 R 和 $L(x)$，我们找到一种双元素分布 $P(x)$，使其对应的码率为 R。现在，对于度分布 $L(x)$ 和 $P(x)$，从符合这些度分布的低密度奇偶校验码集合中随机选取校验矩阵$\mathbf{H}$，并使用 $\mathbb{GF}(2^q)$中的一个非零元素，以均匀随机的方式为每条边赋予标记 [15] 。在下一节中，我们提出用于信息协调（IR）的非二元多层编码方案（NB-MLC）。

III. 非二进制多级编码

NB-MLC方案通过整数参数 a在密钥率 r与密钥生成的时延/复杂度之间实现权衡， $1 \le a \le q$。令 b 和 r 为满足 $q = ab + r$的整数，其中 $b = \lfloor \frac{q}{a} \rfloor$，而 r是 q除以 a所得的余数。Alice接收到的X中的每个符号 X都是$\mathbb{GF}(2^q)$的一个元素。我们将 X 拆分为 $b+1$ 个符号(X_1、 X_2、 $\ldots X_{b+1}$)，其中 $X_i \in \mathbb{GF}(2^a)$ $1 \le i \le b$，并且 $X_{b+1} \in \mathbb{GF}(2^r)$，使用单射映射 u： $\mathbb{GF}(2^q) \to \mathbb{GF}(2^a)^b \times \mathbb{GF}(2^r)$。通过上述转换，我们将序列X拆分为 $b+1$层（X_1, X2、.....、X_{b+1}），其中$X_i \in \mathbb{GF}(2^a)^N$， $1 \le i \le b$，且$X_{b+1} \in \mathbb{GF}(2^r)^N$。令 α_i 表示第 i层中符号的比特大小。我们有 $\alpha_i = a$、 $1 \le i \le b$ 和 $\alpha_{b+1} = r$。对于每一层 i，我们使用一个NB-LDPC码H_i，其中$H_i \in \mathbb{GF}(2^{\alpha_i})^{m_i \times N}$，对于 $1 \le i \le b+1$成立。现在，Alice通过设置$S = \{S_1, S2、\ldots..、S_{b+1}\}$ 来生成消息S，使得$S_i = H_i X_i$， $1 \le i \le b+1$，并通过公开信道将其发送给Bob。Bob利用S和Y对每一层X_i进行解码， $1 \le i \le b+1$，从而得到作为协调密钥的X。

Let $\{\widehat{X}_1^i\}^1$表示第 $\widehat{X}_1, \widehat{X}_2, \ldots, \widehat{i}-1$层的译码结果。与 [5], 类似，Bob 使用接收到的消息 $\mathbf{S}_i$、旁信息 $\mathbf{Y}$ 以及 $\widehat{\mathbf{X}}_1^{i-1}$，通过非二元低密度奇偶校验码的 SW 译码对第 $\mathbf{X}_i$ 层进行译码 [16]。第 i 层的等效信道以 $\mathbf{X}_i$ 为输入，输出 $\{\mathbf{Y}$ 、 $\mathbf{X}_1^{i-1}\}$，其转移律为 $\gamma^i := P(Y = y,\ X_1^{i-1} = x_1^{i-1} | X_i = x_i)$。我们根据 QKD 测试平台的实测数据推导出转移律 γ^i ，并在第四节中将其用于码优化。

Alice 为协调第 i 层而发送的消息 $\mathbf{S}_i$ 的大小为 m_i。令 E_i 为第 i 层的帧错误率。NB-MLC 方案的密钥率通过将各层的密钥率相加（类似于 [5]）得到，表示为

$$r = \sum_{i=1}^{b+1} \alpha_i (1 - E_i) \frac{N - m_i}{N}. \tag{2}$$

密钥率取决于层 i 中使用的 $\mathbf{H}_i$ 的码率 $R_i = \frac{N - m_i}{N}$。非二元多层编码方案中的参数 a 也会影响密钥率、时延和硬件复杂度（它们分别是解码时延之和以及所有层的复杂度之和）。请注意， $a = 1$ 给出了 [5] 的二元 MLC 方案，而 $a = q$ 则提供了一种仅有一层的完全非二元方案。随着 a 从 1 增加到 q，复杂度会单调增加。然而，正如我们在第五节所展示的，密钥率并不会随 a 单调变化。

最后，系统在密钥率和时延方面的性能还取决于用于将符号 $X \in \mathbb{GF}(2^q)$拆分为不同层符号的映射 $u(X)$。为方便起见，我们采用以下映射。首先，将 X 转换为其二进制表示 X_b。然后，将 X_b 中的比特拆分为 $b+1$ 组，其中第 i组包含 α_i 个比特。接着，将每组 i 中的比特视为二进制表示，并将其转换回$\mathbb{GF}(2^{\alpha_i})$中的一个符号。不同映射对密钥率和时延的影响不在本文讨论范围之内，将作为未来研究的一部分。下一节将介绍基于差分进化的 JRDO 框架，用于联合优化非二元低密度奇偶校验码的码率和度分布。

IV. 联合码率与度分布优化

本节介绍用于设计校验矩阵 $\mathbf{H}_i$, $1 \le i \le b+1$ 的框架，以便将其用于具有信道转移概率$\gamma^i := P(Y = y,\ X_1^{i-1} = x_1^{i-1} | X_i = x_i)$的非二元多层编码方案的第 i层。所有层的构造方法相同，因此省略索引 i。具体而言，我们为$\mathbf{H}$ 设计变量节点度分布 $L(x)$和码率R （关于如何由 $L(x)$和 R生成非二元$\mathbf{H}$ ，请参见第二节第3部分）。信道转移概率为 γ。

我们的框架利用差分进化（DE） [14] 来寻找 $L(x)$ 和 R。DE 是一种广受欢迎且有效的基于种群的进化算法，可用于最大化（或最小化）任意函数 $f()$。该算法通过进化过程迭代改进候选解（以最大化 $f()$），并能以较低的复杂度探索广阔的设计空间。DE 已广泛用于编码理论文献，以设计适用于擦除信道 [17]、加性高斯白噪声信道 [13]、瑞利衰落信道 [18], 等的优良非规则低密度奇偶校验码。这些工作的目标是设计帧错误率（FER）较低的度分布。为实现这一目标，研究者使用 DE，通常将函数 $f()$设为码性能的某种低复杂度预测指标，例如通过密度演化 [13]得到的阈值。然而，正如第一节所述，本文的目标是最大化密钥率，而不仅仅是降低帧错误率。此外，使用码阈值优化度分布的技术适用于固定码率；我们尚未发现有先前研究能够在最大化阈值的同时联合优化码率。

本文依据式（2）中的密钥率表达式，利用 DE 联合优化度分布 $L(x)$ 和码率 R，方法是设定 $f(L(x)\ R) = (1 - E)R$。其中， E 是度分布为 $L(x)$、码率为 R 的码系综在转移律为 γ的信道上的预期帧错误率。请注意，为了能够利用 DE 对上述函数进行有效优化，计算该函数的代价必须

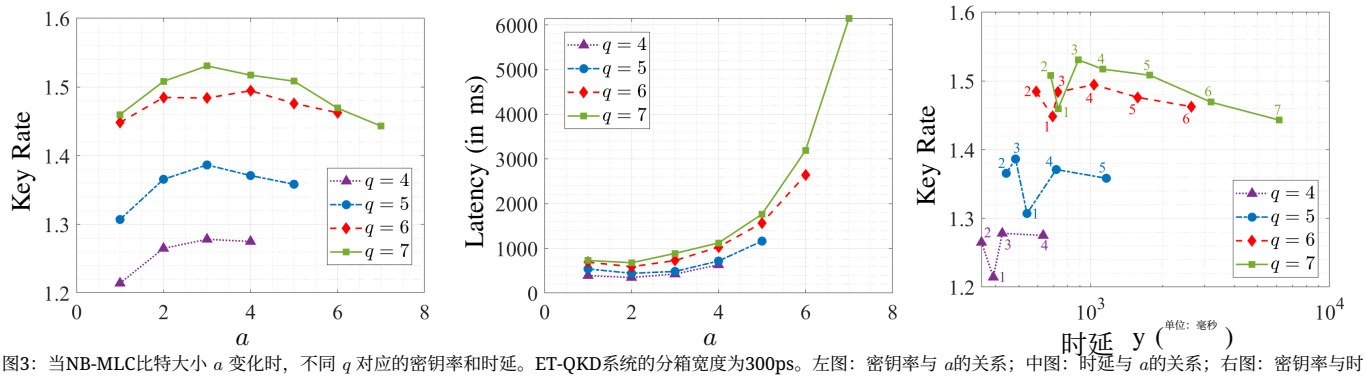

图3：当NB-MLC比特大小 a 变化时，不同 q 对应的密钥率和时延。ET-QKD系统的分箱宽度为300ps。左图：密钥率与 a的关系；中图：时延与 a的关系；右图：密钥率与时延的关系，其中曲线上每个对应特定 q 的点表示 a 的不同取值（ a 的取值标注在曲线上）。所有曲线均使用第二节第3部分中提到的低密度奇偶校验码，并采用 $L(x) = x^3$。

较低（因为 DE算法在每次迭代中都会以固定次数对函数 $f()$ 求值）。然而，如第 II-2 节所述，由于码的帧错误率较高（$\sim 1-10\%$），使用少量蒙特卡罗实验（例如 200–300 次）即可通过蒙特卡罗（MC）仿真轻松计算帧错误率 E。完整的 JRDO算法见算法1，其中 DiffMutation() 和 CrossOver() 过程具有 [14] 中所述的常规含义。算法1的贡献在于采用目标函数 $f(L(x)\ R) = (1-E)R$，并利用 ET-QKD 信道的高帧错误率特性，通过 MC 仿真实现对该函数的有效评估，从而使联合优化成为可能。

算法1 JRDO：联合速率与度分布优化

初始化种群 $\Pi = \{(L_1, R_1)\ldots, (L_{N_{pop}}, R_{N_{pop}})\}$
对于最大迭代次数 **执行**
  对于 $j = 1:\ N_{pop}$，**执行**
    $(L_j^m,\ R_j^m)$ =差分变异$(j,\ \Pi)$
    $(L_j^c,\ R_j^c)$ =交叉$\big((L_j^m,\ R_j^m),\ (L_j,\ R_j)\big)$
    使用蒙特卡罗仿真评估 $f(L_j^c,\ R_j^c)$
  对于 $j = 1:\ N_{pop}$ **do**
    如果 $f\ (L_j^c,\ R_j^c)\ > f\ (L_j,\ R_j)$ **则**
      更新种群：$(L_j,\ R_j) \leftarrow (L_j^c,\ R_j^c)$
输出：$(L,\ R)$，取自具有最大 $f(L,\ R)$的 Π

V. 仿真结果

本节展示非二元多层编码方案（NB-MLC）的性能，以及使用JRDO算法设计的码的性能。我们将其性能与 [5] 的多层编码方案（MLC）进行比较，同时也与 [5] 中使用的码以及针对二进制输入加性高斯白噪声信道 [13]设计的码进行比较。对于联合码率与度分布优化框架，我们优化度分布 $L(x) = \sum_{d=2}^{5} L_d$，其中设定 L_1 为零，变量节点的最大度数为5。对于非JRDO码，我们通过穷举遍历消息长度 m_i，找出并采用能产生最大密钥率的码率（针对NB-MLC方案中的特定层）。NB-MLC方案的时延按该方案所有层的译码时延之和计算。我们的仿真采用码长 $N = 2000$ 以及基于FFT的和积低密度奇偶校验译码（软件版本 [16]）。

在图3中，我们研究 MLC 位大小 a 对 QKD 系统的密钥率和时延的影响。回顾一下，QKD 系统每帧有 2^q 个时间槽，因此总位大小为 q。从图3左图可以看出，对于所有 q 的取值，密钥率关于 a 呈非单调变化，并在 a 严格介于 1 和 q 之间时达到最大值。密钥率关于 a 呈非单调变化的原因如下。增大a 的值会使非二元多层编码方案采用来自更大伽罗瓦域的非二元低密度奇偶校验码，这些码的性能更强，从而带来更好的帧错误率表现，进而提高每一层的密钥率。然而，由于分层，即使后续层出现解码失败，较早层的正确解码仍会对总体密钥率有所贡献。这种累加效应（由公式（2）所致）会随着层数增加（ a较小）而提升总体密钥率。由于上述两种效应，总体密钥率呈非单调变化。在图3中图中，我们绘制了不同 q 取值下非二元多层编码方案的时延随 a 变化的曲线。从图中可以看出，随着a 增大（接近 q），时延会显著增加。这一趋势是因为较大的a 意味着采用来自更大伽罗瓦域的非二元低密度奇偶校验码，因此解码时延也更长。请注意，随着 a 增大，解码复杂度的增加有时会被非二元多层编码方案中解码层数的减少所抵消，因此时延关于 a 呈非单调变化（图3右图也能看出这一点）。在图3右图中，我们绘制了非二元多层编码方案中不同 a 取值所实现的密钥率与时延之间的关系。从图中可以清楚地看出，较小的 a 值（3 或 4）可实现最佳折衷。进一步增大 a 会导致时延增加，而密钥率并无提升。

在图4左侧面板中，我们比较了使用 $q = 6$ 的 QKD 系统在不同分箱宽度下的密钥率。我们比较了 $a = 1$，3 和 6 对应的密钥率。与图3类似，我们再次可以看到，在所有分箱宽度下，与 $a = 1$（使用二进制低密度奇偶校验码的 [5] 的多层编码方案）和 $a = 6$（采用完整非二元低密度奇偶校验码且不分层的方案）相比，$a = 3$ 的密钥率更高。总体而言，较小 $a > 1$ 值的非二元多层编码方案具有最佳系统性能。

在图4的中间和右侧面板中，我们比较了采用不同码构造所获得的密钥率。菱形标记的曲线对应于 [5]中使用的低密度奇偶校验码。根据 [5]，这些低密度奇偶校验码是随机构造的，每个变量节点的度均为3。请注意，

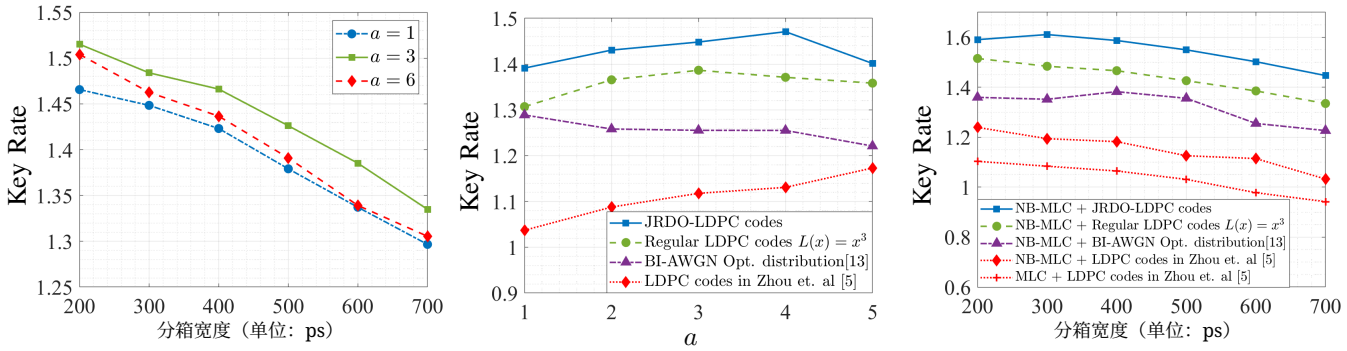

图4：左图：不同 NB-MLC 比特大小 a 下的密钥率与分箱宽度的关系。该 QKD 系统每帧包含 2^6 个时间槽；中图：不同低密度奇偶校验码下的密钥率与 a 的关系。该 QKD 系统每帧包含 2^5 个时间槽，分箱宽度为 300ps；右图：不同低密度奇偶校验码下的密钥率与分箱宽度的关系。NB-MLC 方案采用 $a = 3$。该 QKD 系统每帧包含 2^6 个时间槽。

本文考虑的低密度奇偶校验码（见第二节第3部分）的校验节点度分布不受此限制。不过，本文所考虑的低密度奇偶校验码具有仅包含两种度的校验节点度分布。三角形标记的曲线对应于 [13,表I]所给出的度分布，其变量节点最大度为5。请注意，该度分布是针对二进制输入加性高斯白噪声信道优化的。圆形标记的曲线对应于变量节点度分布规则的低密度奇偶校验码$L(x) = 3$（类似于 [5]），但其校验节点度分布仅包含两种度。最后，方形标记的曲线对应于使用JRDO算法得到的度分布。从图中可以得出以下结论。菱形标记曲线的密钥率低于圆形标记曲线。这一趋势表明，采用仅包含两种度的校验节点度分布更好（正如本文所采用的做法）。三角形标记曲线（二进制输入加性高斯白噪声信道优化的度分布）的密钥率低于采用变量节点度为3的规则低密度奇偶校验码时的密钥率（圆形标记曲线）。这一趋势表明，针对非量子密钥分发信道优化的码用于QKD信道时表现不佳。最后，在图4的中间和右侧面板中可以看到，JRDO低密度奇偶校验码（方形标记曲线）获得的密钥率最高，这是因为JRDO低密度奇偶校验码是针对QKD信道优化的。在图4右侧面板中，我们还绘出了使用 [5] 技术获得的密钥率，即多层编码方案（$a = 1$）、变量节点度为3的规则低密度奇偶校验码，且校验节点度分布不受限制（加号标记曲线）。可以看到，与 [5] 相比，我们的技术（方形标记曲线）使密钥率提高了约40%。

VI. 结论

本文研究了 ET-QKD 中的信息协调问题，并提出了一种对 [5] 多级编码（MLC）方案的推广，称为 NB-MLC，该方案使用非二元低密度奇偶校验码。我们证明，NB-MLC 方案在密钥率和时延方面为系统设计提供了灵活性，而且每层比特大小较小的 NB-MLC 方案能够在密钥率与时延之间实现最佳权衡。最后，我们提出了一种基于不同演化的框架，称为 JRDO，可联合优化 NB-MLC 方案所用低密度奇偶校验码的码率和度分布。针对 ET-QKD 信道优化的 JRDO-LDPC 码显著提高了密钥率，相较于先前工作中使用的低密度奇偶校验码有明显提升。目前的研究正致力于优化边权分布（并结合 JRDO），以进一步提高密钥率。

致谢

作者感谢美国国家科学基金会资助的 QuIC-TAQS 项目（编号 2137984）以及美国国家科学基金会资助的 EFRI-ACQUIRE 项目（编号 1741707）。

参考文献

[1] C. H. Bennett 和 G. Brassard，《量子密码学：公钥分发与抛硬币协议》，IEEE计算机、系统与信号处理国际会议，1984年。[2] H.-K. Lo、M. Curty 和 K. Tamaki，《安全量子密钥分发》，《自然·光子学》，第8卷，第8期，2014年。[3] T. Zhong 等，《采用高维编码的能量-时间纠缠光子高效量子密钥分发》，《新物理学杂志》，第17卷，第2期，2015年。[4] K.-C. Chang 等，《双光子频率梳中的648希尔伯特空间维数：形成纠缠与施密特模分解》，《npj量子信息》，第7卷，第1期，2021年。[5] H. Zhou、L. Wang 和 G. Wornell，《大字母表密钥分发的分层方案》，IEEE信息论与应用研讨会，2013年2月。[6] C. Lee 等，《用于更高速率量子密钥分发的大字母表编码》，《光学快报》，第27卷，第13期，2019年。[7] M. C. Davey 和 D. MacKay，《GF(q)上的低密度奇偶校验码》，《IEEE通信快报》，第2卷，1998年。[8] J. Martinez-Mateo、D. Elkouss 和 V. Martin，《面向高性能量子密钥分发的密钥协调》，《科学报告》，第3卷，2013年。[9] S. Wehner、D. Elkouss 和 R. Hanson，《量子互联网：未来发展愿景》，《科学》，第362卷，第6412期，2018年。[10] X.-Q. Jiang 等，《基于空间耦合低密度奇偶校验码的连续变量量子密钥分发高速协调》，《IEEE光子学杂志》，第10卷，第4期，2018年。[11] S. J. Johnson、V. A. Chandrasetty 和 A. M. Lance，《用于连续变量量子密钥分发协调的重复累积码》，IEEE澳大利亚通信理论研讨会，第18–23页，2016年。[12] S. Yang 等，《面向能量-时间纠缠量子密钥分发的高效信息协调》，IEEE阿西洛马会议信号、系统与计算机分会，2019年11月。[13] T. J. Richardson、M. A. Shokrollahi 和 R. L.Urbanke，《逼近容量的不规则低密度奇偶校验码的设计》，《IEEE信息论汇刊》，第47卷，第2期，2001年。[14] R. Storn 和 K. Price，《差分进化——一种用于连续空间全局优化的简单高效启发式方法》，《全球优化杂志》，第11卷，第4期，1997年。[15] T. Richardson 和 R. Urbanke，《现代编码理论》，剑桥：剑桥大学出版社，2008年。[16] E. Dupraz、V. Savin 和 M. Kieffer，《用于Slepian-Wolf编码的非二进制低密度奇偶校验码设计中的密度演化》，《IEEE通信汇刊》，第63卷，第1期，2015年。[17] A. Shokrollahi 和 R. Storn，《采用差分进化设计高效擦除码》，IEEE信息论国际研讨会，2000年6月。[18] J. Hou、P. H. Siegel 和 L. B. Milstein，《瑞利衰落信道中低密度奇偶校验码的性能分析与码优化》，《IEEE精选通信领域期刊》，第19卷，第5期，2001年。