时间纠缠量子密钥分发：密钥率与信息协调编码

Joseph J. Boutros，IEEE 高级会员；Emina Soljanin，IEEE 会士

arXiv:2301.00486v1 [cs.IT] 1 Jan 2023

摘要

在基于时间纠缠的量子密钥分发（QKD）中，Alice 和 Bob 通过时间分箱，从纠缠光子对（具有相同的）到达时间中提取原始密钥比特。他们各自独立地将时间离散为区间，并将这些区间组成帧。他们只保留恰有一个被占用区间的帧。因此，Alice 和 Bob 可以利用帧内被占用区间的位置生成随机密钥比特，类似于脉冲位置调制。由于存在纠缠，他们的被占用区间和密钥理应相同。然而，实际的光子探测器会受到时间抖动误差的影响。这些错误会导致 Alice 和 Bob 的密钥不一致。Alice 通过公共信道向 Bob 发送信息，以协调密钥。信息量决定了秘密密钥率。本文计算了存在探测器抖动误差时可能达到的秘密密钥率，并构造了用于信息协调的编码，以逼近这些密钥率。

索引词

量子密钥分发、密钥率、互信息、时间纠缠、时间分箱、抖动错误、软判决译码。

一、引言

密钥分发协议旨在有窃听者 Eve 存在的情况下，在相距遥远的两个（或更多）参与方 Alice 和 Bob 之间建立共享的比特序列。密钥由仅 Alice 和 Bob 知道的均匀随机独立比特组成。量子密钥分发（QKD）首先通过量子信道传输量子态。量子步骤的作用是：1）确保任何窃听行为都不会逃过检测；2）为基于纠缠的系统提供完美随机性的来源。

Joseph J. Boutros 任职于卡塔尔多哈 23874 的得克萨斯农工大学电气与计算机工程系，电子邮箱：boutros@ieee.org（参见 https://www.josephboutros.org）。Emina Soljanin 任职于美国新泽西州皮斯卡塔韦 08854 的罗格斯新泽西州立大学电气与计算机工程系，电子邮箱：（参见 https://www.ece.rutgers.edu/emina-soljanin）。本研究基于美国国家科学基金会资助的工作，资助编号为 FET-2007203。

人们已投入大量努力，力求在长距离传输中实现较高的密钥率（参见近期综述 [1],[2]）。基于时间纠缠光子的量子密钥分发方案已成为一种颇具前景的技术，主要原因是每对纠缠光子都能承载多个密钥比特，因此有望在长距离传输中实现更高的安全密钥率 [3], [4]。

基于时间纠缠的量子密钥分发（TE-QKD）方案使用自发参量下转换（SPDC），按照泊松过程生成纠缠光子对。其中一个光子发送给 Alice，另一个发送给 Bob。因此，理想情况下，Alice 和 Bob 会同时探测到各自的光子，且光子到达间隔时间服从指数分布。最常见的单光子探测器是超导纳米线单光子探测器（SNSPD），其性能最接近理想传感器。它们的暗计数率较低，这意味着在没有光子到达时，它们很少报告检测到光子。此外，它们的探测器停机时间较短 d，探测器时间抖动也较小；这种抖动表现为均值为零、方差为 σ_d^2 的高斯噪声。不幸的是，这些缺陷不可忽略：1）探测器抖动和暗计数会导致 Alice 与 Bob 的密钥不一致；2）停机时间会使原始密钥比特产生记忆效应。 [5] 最近研究了这些探测器的非理想特性造成的秘密密钥率损失。

从宏观上看，量子密钥分发主要分为两个步骤。第一步，Alice 和 Bob 使用量子信道生成原始密钥比特。由于前述非理想探测器特性，他们各自的原始密钥在某些位置可能不一致，部分内容可能已被 Eve 知晓，而且可能并非均匀随机。第二步，Alice 和 Bob 对原始密钥进行处理，以建立共享密钥。他们通过公共经典信道进行通信，协调各自原始密钥之间的差异，增强密钥相对于 Eve 所掌握信息的隐私性，并压缩各自的序列以实现均匀随机性。在协议结束时，Alice 和 Bob 1）拥有完全相同且均匀随机的（二进制）序列；2）确信只有他们自己知道这一共享序列。因此，该密钥是私密的，且难以猜测。本文重点讨论信息协调步骤。

Alice 和 Bob 通过检测纠缠光子的到达时间，获得相关的比特流（原始密钥）。然而，他们必须通过公共信道通信，才能就密钥达成一致，也就是协调彼此之间的差异。在这里，我们考虑单向信息协调方案：Alice 将有关自己序列的信息发送给 Bob，由 Bob 利用这些信息消除自己的原始密钥与 Alice 的原始密钥之间的差异。完成信息协调后，Alice 和 Bob 共享 Alice 最初的原始密钥。然而，由于公共信道上的通信，这个共享密钥并不保密。Alice 和 Bob 会进行隐私

放大来解决这一问题，从而实现保密，但密钥长度会缩短。由于 Alice 和 Bob 基于相关的光子到达时间生成秘密密钥，因此他们采用了信息论中所谓的源模型 [6, 第 22 章。3]。当窃听者可以访问公开通信，但没有相关先验信息时，该模型的保密容量等于 Alice 和 Bob 观测结果之间的互信息（参见例如 [6, 第 567] 页）。保密容量是隐私放大后密钥率的一个可实现上界。

Alice 和 Bob 根据相关的随机光子到达事件生成秘密密钥。提取这些相关信息中的密钥有很多方法。一种常用方法与脉冲位置调制（PPM）类似；例如参见 [7] 及其中的参考文献。（近期提出的一些自适应方案无需丢弃包含多个已占用区间的帧 [8], [9]。）在 PPM 中，Alice 和 Bob 同步时钟，并将各自的时间线划分为包含 N 个时间区间的帧。在 PPM 中，Alice 和 Bob 约定只保留双方都检测到单个光子到达的时间帧，并丢弃所有其他帧。这个单光子被认为占据了一个时间区间，具体取决于它在帧内到达的位置。由于光子到达间隔时间服从指数分布，每个区间是否被占据都独立于其他区间。因此，PPM 解码从每帧中提取的原始密钥比特数等于 $\log N$。

本文聚焦于会产生时间抖动误差的实用光子探测器。由于这些误差会导致 Alice 和 Bob 的密钥不一致，Alice 必须通过公共信道向 Bob 发送信息，以协调密钥。信息量决定了秘密密钥率。本文计算了存在探测器抖动误差时可达到的密钥率，并构造了用于信息协调的编码，以逼近这些密钥率。

本文的组织如下：第二节介绍符号表示，并列出本文的主要贡献。第三节介绍 TE-QKD 信道模型。第四节计算由探测抖动引起的原始密钥不一致率，第五节推导 Alice 与 Bob 的原始密钥之间的相关性。第六节计算 TE-QKD 信道的可达信息率和保密容量。第七节提出并测试若干用于信息协调的编码方案。

II. 符号表示与主要贡献

每个时间帧的分箱数 N 可以是任意大于或等于 2 的正整数；我们的命题、引理和定理对 N 没有其他限制。不过，我们的数值示例针对 $N = 2^m$, m 整数 $m \geq 1$给出。集合 $\mathbb{Z}_N$ 表示 N整数 $\{0, 1, \ldots, N-1\}$的集合。记号 $\lfloor x \rfloor$称为 x 关于 $x \in \mathbb{R}$的向下取整，是小于或等于 x的最大整数。

~ ~ ^ ^ 字母 X、 Y、 X和 Y 表示连续随机变量，而 X 和 Y 表示离散随机变量。于是， $p(\hat{y}|\hat{x})$ 表示条件概率 $\mathbb{P}(Y = \hat{y}|X = \hat{x})$。此外， $p(y|\hat{x})$ 表示条件密度 $p_{Y|\hat{X}}(y|\hat{x})$。

对于实数轴上的区间，我们采用布尔巴基的记法，其中 a 和 b 是两个实数：闭区间 $[a,b] = \{x \in \mathbb{R} : \ a \leq x \leq b\}$，半开区间 $[a,b[= [a,b] \setminus \{b\}$ 和 $]a, b] = [a,b] \setminus \{a\}$，以及开区间 $]a, b[= [a,b] \setminus \{a,b\}$。

我们使用标准的巴赫曼-朗道大 $\mathcal{O}$ 记法：

$f(\sigma) = \mathcal{O}(g(\sigma))$ 的形式化定义为： $\exists \alpha > 0, \ \exists \sigma_0 > 0, \ \forall \sigma < \sigma_0, \ |f(\sigma)| \leq \alpha |g(\sigma)|$。在本文中，诸如 $1 - \mathcal{O}(g(\sigma))$ 或 $1 + \mathcal{O}(g(\sigma))$ 这样的表达式，默认假设 $g(\sigma) > 0$ 在某个开区间 $]0, \sigma_0[$ 内。此外，我们将频繁使用 $\gamma = 1/\sigma^2$，它是抖动方差的倒数，即信噪比；在类似情况下，当 $\gamma \to \infty$ 时，我们可以写作 $f(\gamma) = \mathcal{O}(g(\gamma))$。如果两个函数 $f : \ \mathbb{R} \to \mathbb{R}$ 和 $g : \ \mathbb{R} \to \mathbb{R}$ 满足 $\lim_{\gamma \to \infty} f(\gamma)\, g(\gamma) = 1$，则称它们渐近等价。在这种情况下，我们记作 $f(\gamma) \sim g(\gamma)$。

函数 $Q(x) = \frac{1}{2} \operatorname{erfc}(\frac{x}{\sqrt{2}}) = \mathcal{O}(\exp(-x^2/2))$ 是高斯尾函数。回忆定义$Q(x) = \int_x^\infty \phi(t) dt$，其中 $\phi(t) = \frac{1}{\sqrt{2\pi}} \exp(-t^2/2)$ 是标准正态密度。此外，我们回忆二元熵函数 $H_2(x) = -x \log(x) - (1-x) \log(1-x)$，以及对称三元熵函数 $H_3(x) = -(1-2x) \log(1-2x) - 2x \log(x)$。

本文的主要贡献是从信息论和编码理论的角度，对时间纠缠量子密钥分发信道进行了完整刻画：

- 我们推导了 TE-QKD 信道的错误率，并证明 TE-QKD 信道的表现类似于 $1/2$ 阶分集的中上衰落信道，见命题1。
- 我们求得了 Alice 和 Bob 的帧均有效时各分箱的精确先验概率，见引理 2。
- 我们推导了软输出 TE-QKD 信道中给定 Alice 光子分箱时 Bob 光子位置的精确条件密度，见定理 1。输出密度的表达式也已确定，见式 (32)。
- 我们确定了离散（硬输出）TE-QKD 信道转移概率的表达式，见推论1。
- 我们给出了软输出 TE-QKD 信道的后验概率的精确表达式，见定理2。

- 我们推导出互信息 $I(X;Y)$（硬输出）的精确公式，并在小噪声区间得到了简化表达式，见式（33）、（34）、（40）和命题 2-c。
- 互信息 $I(X;Y)$（软输出）的精确公式见式 (41)。我们还确定了计算最大速率 $I(X;Y)$ 所需的所有概率密度，并给出了小噪声区间内简洁的对数公式表达式，见定理 3 和推论 2。

- 最后一节，即第七节，展示了采用代数硬判决译码和概率软判决译码时，使用里德-所罗门码、BCH 码和低密度奇偶校验码等短码及中等长度纠错码所获得的显著编码增益。

III. 脉冲位置调制信道模型

设 X 和 Y 分别表示 Alice 端和 Bob 端接收光子的时间位置。图 1 展示了该量子密钥分发方案的示意图。

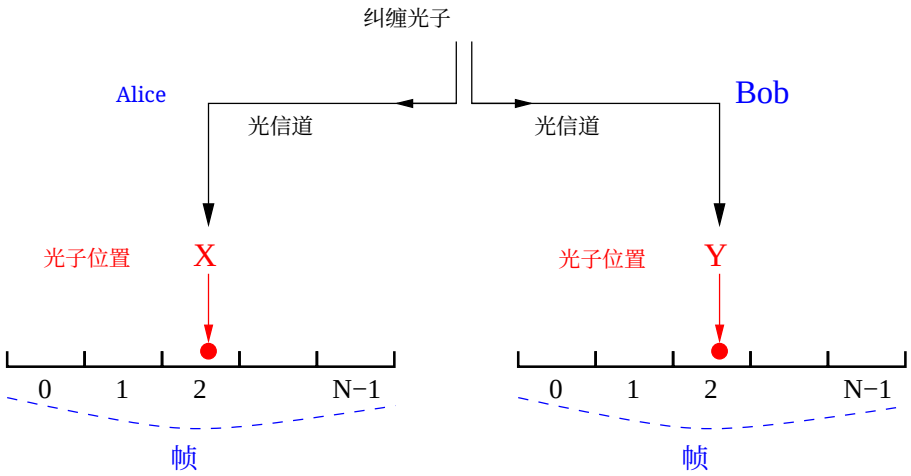


图 1. 基于时间纠缠的量子密钥分发，每帧包含 N 个分箱，每个区间包含 $\log_2(N)$ 个二进制位。

我们采用以下数学模型描述两个时间纠缠光子的位置：

$$\tilde{X} = U + Z_1, \quad \tilde{Y} = U + Z_2, \tag{1}$$

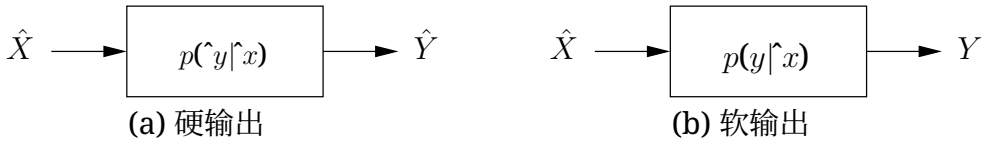
其中，Z_1 和 Z_2 是相互独立且同分布的 $\mathcal{N}(0,\sigma^2)$ 加性高斯噪声，用于模拟探测抖动。U 是区间 $[0,N[$ 上的实数均匀随机变量，其中整数 $N = 2^m$ 表示每帧分箱数，m 表示每个光子的比特数。Alice 和 Bob 通过公共信道通信，并约定当 X 和 Y 落在区间 $[0,N[$ 内时，该帧为有效帧。他们会丢弃空帧以及包含多个接收光子的帧。根据模型 (1)，一帧对 Alice 和 Bob 双方均有效的概率为 $\mathbb{P}(X,Y \in [0,N[)$。令 X 和 Y 分别表示

˜ ˜ ˆˆX和 Y在区间 $[0, N[$,内的取值，并令 X和 Y表示帧内的分箱编号，即

$$\tilde{X} = X, \quad \text{for } \tilde{X} \in [0, N[, \qquad \tilde{Y} = Y, \quad \text{for } \tilde{Y} \in [0, N[, \tag{2}$$

$$\hat{X} = \lfloor X \rfloor \in \mathbb{Z}_N, \qquad \hat{Y} = \lfloor Y \rfloor \in \mathbb{Z}_N. \tag{3}$$

从信息论的角度来看，我们区分 Alice 与 Bob 之间的两种通信信道：(a) 代数（硬输出）信道，(b) 实数（软输出）信道，两者的输入均为离散的 ˆN 元 X ，如图2所示。



(a) 硬输出 (b) 软输出

图 2. 硬判决译码 (a) 和软判决译码 (b) 的信道模型。

在不使用纠错码的情况下，这些信道上的信息速率为 $\log_2(N) = m$ 比特/信道使用 (bpcu)。主要信道参数 γ 是一个信噪比参数 (SNR)，定义为

$$\gamma = \frac{E_s}{\sigma^2} = \frac{1}{\sigma^2}, \tag{4}$$

其中，平均符号能量 $E_s = 1$ 是每个传输光子的归一化能量开销。另一个量子密钥分发信道参数是 $\overline{\gamma}$，称为归一化信噪比，其中加性高斯噪声的标准差以帧长 N 进行归一化，因此其定义为

$$\overline{\gamma} = \frac{1}{(\sigma/N)^2} = \frac{N^2}{\sigma^2}, \quad \overline{\gamma}(dB) = \gamma(dB) + 20\log_{10}(N). \tag{5}$$

我们将错误概率和信息速率表示为 N 以及信噪比 γ 或归一化信噪比 $\overline{\gamma}$的函数。为简化分析，将帧内的时间槽宽度设为 1，即除第 VI-B 节外，所有章节中的帧宽均为 N 。引入时间尺度，将 γ 和 N 转换为物理参数后，即可轻松地将该数学模型转换为代表实验室实验的物理模型。在第 VI-B 节中，分箱数量为无穷（分箱构成连续统），帧长为单位长度，并且在这个特殊的量子密钥分发信道中，$\gamma = \overline{\gamma}$ 同时具有软输入和软输出。

IV. 探测抖动下的原始密钥不一致率

ˆˆ 我们考虑错误概率 $P_e(\gamma) = \mathbb{P}(X \neq Y)$。概率 P_e 表征图2中信道 (a) 的质量，该信道由其转移概率 $p(\hat{y}|\hat{x})$ 定义。后者将在第 VI 节中完全确定。在本节中，我们关注的是确定 $P_e(\gamma)$ 关于信噪比 P_e 的表达式，其中每帧的分箱数为 γ。

其中每帧的分箱数为 N。

ˆ令 $\pi_i = \mathbb{P}(X = i)$、 $i \in \mathbb{Z}_N$ 表示帧中唯一光子落入分箱编号 i 的先验概率。那么，错误概率的精确表达式为

$$P_e(\gamma) = \sum_{i=0}^{N-1} \pi_i \sum_{\substack{j=0 \\ j\neq i}}^{N-1} p(\hat{y} = j|\hat{x} = i) = \frac{1}{N} \sum_{i=0}^{N-1} \mathbb{P}(\hat{Y} \neq \hat{X}|\hat{U} = i), \tag{6}$$

其中 ˆ $U = \lfloor U \rfloor$。由于 U 在 $[0, N)$ 中均匀分布，我们得到 $\mathbb{P}(\hat{U} = i) = \mathbb{P}(U \in [i, i + 1)) = \frac{1}{N}$，这解释了上面最后一个等式中的因子。作为第一步，本节通过对 U 进行条件化，利用式 (6) 最右侧的等式求解 $P_e(\gamma)$。为避免像第V和VI节中推导精确表达式时那样出现繁琐的表达式，我们假设 γ 足够大（ σ^2 足够小），从而可以忽略帧中的边界效应。因此，这里不区分 X 和 X （分别也不区分 Y 和 Y），并采用如下近似：在以 U 为条件时， X 和 Y 均服从独立同分布的高斯分布。

ˆ ˆ 命题1. 符号错误概率 $P_e(\gamma) = \mathbb{P}(X \neq Y)$ 关于信噪比 γ 和每帧分箱数 N 的函数由下式给出

$$P_e(\gamma) = \frac{2}{\sqrt{\pi}} \times \left(1 - \frac{1}{N}\right) \times \gamma^{-\frac{1}{2}} + \mathcal{O}(\exp(-\frac{\gamma}{4})). \tag{7}$$

ˆ 证明：令 $V = U - U$，则 V服从均匀分布$[0, 1]$。设 $p(i \to j|v)$ 表示在给定 $U = i$ 和 $V = v$的情况下，落入区间 ˆj的概率，其中 $i, j \in \mathbb{Z}_N$。若 $X = U + Z_1$ 仍留在区间i 内，而 $Y = U + Z_2$ 离开并进入区间 j, $j \neq i$，则发生符号错误。由于两种加性高斯噪声 Z_1 和 Z_2 相互独立，此类事件的概率为 $p(i \to i|v) \times p(i \to j|v)$。此外，若 X 和Y都离开并进入两个不同的区间 ℓ 和 j，也会发生错误，其概率为 $p(i \to \ell|v) \times p(i \to j|v)$。于是，条件符号错误概率为

$$P_e(i, v) = 2 \left[\sum_{\substack{j=0 \\ j\neq i}}^{N-1} p(i \to i|v)p(i \to j|v) + \sum_{\substack{\ell=0 \\ \ell\neq i}}^{N-1} \sum_{\substack{j=0 \\ j\neq i, j\neq \ell}}^{N-1} p(i \to \ell|v)p(i \to j|v) \right].$$

因子 2 源于交换两个字母 X 和 Y 时的对称性。如图3所示，我们将忽略左侧区间和右侧区间以外的分箱。被忽略的分箱与区间 ˆ$U = i$ 的距离至少为 1.0。它们对应的错误概率为 $Q(1/\sigma) = \mathcal{O}(\exp(-1/(2\sigma^2))) = \mathcal{O}(\exp(-\frac{\gamma}{2}))$.

为进一步简化符号，定义 p_1、 p_2 和 p_3，其中

$$p_1 = p(i \to i|v) = 1 - Q\left(\frac{v}{\sigma}\right) - Q\left(\frac{1-v}{\sigma}\right), \tag{8}$$

$$p_2 = p(i \to i-1|v) = Q\left(\frac{v}{\sigma}\right), \tag{9}$$

and

$$p_3 = p(i \to i+1|v) = Q\left(\frac{1-v}{\sigma}\right), \tag{10}$$

我们得到

$$P_e(i,v) = \mathcal{O}(\exp(-\frac{\gamma}{2})) \ + \begin{cases} 2[p_1p_2 + p_1p_3 + p_2p_3], & \text{for } i = 1 \dots N-1, \\ 2p_1p_3, & \text{for } i = 0, \\ 2p_1p_2, & \text{for } i = N-1. \end{cases}$$

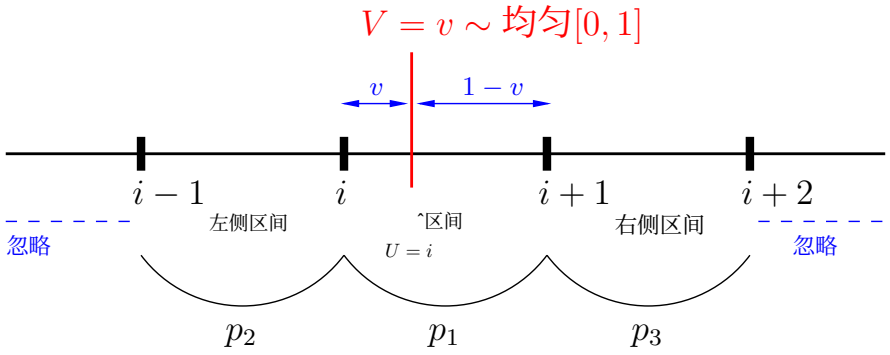


图 3. 区间位置错误概率示意图。

现在，对 v 积分，

$$\mathbb{P}(\hat{Y} \neq \hat{X}|\hat{U} = i) = \int_0^1 P_e(i,v)\ dv.$$

然后，应用 (6) 并使用 $\int_0^1 p_1p_2dv = \int_0^1 p_1p_3dv$，最终得到

$$P_e(\gamma) = \frac{1}{N}\sum_{i=0}^{N-1}\int_0^1 P_e(i,v)\ dv \tag{11}$$

$$= 4\left(1-\frac{1}{N}\right)\int_0^1 p_1p_2\ dv + 2\left(1-\frac{1}{N}\right)\int_0^1 p_2p_3\ dv\ + \mathcal{O}(\exp(-\frac{\gamma}{2})). \tag{12}$$

(12) 中的两个积分包含三种类型的积分。下面我们逐步处理它们。

$$I_1 = \int_0^1 Q\left(\frac{v}{\sigma}\right)\ dv = \frac{\sigma(1-e^{-1/2\sigma^2})}{\sqrt{2\pi}} + Q\left(\frac{1}{\sigma}\right)\ = \frac{\sigma}{\sqrt{2\pi}} + \mathcal{O}(\exp(-\frac{\gamma}{2})).$$

$$I_2 = \int_0^1 \left[Q\left(\frac{v}{\sigma}\right)\right]^2 dv = \frac{2\sqrt{2}\sigma - 2\sigma(1-2Q(\sqrt{2}/\sigma)) + 4\sqrt{\pi}Q^2(1/\sigma) - 4\sqrt{2}\sigma e^{-1/2\sigma^2}Q(1/\sigma)}{4\sqrt{\pi}}$$
$$= \frac{(\sqrt{2}-1)\sigma}{2\sqrt{\pi}} + \mathcal{O}(\exp(-\gamma)).$$

$$I_3 = \int_0^1 Q\left(\frac{v}{\sigma}\right)\ Q\left(\frac{1-v}{\sigma}\right)\ dv \le \int_0^1 \exp\left(\frac{-v^2-(1-v)^2}{2\sigma^2}\right)\ dv\ =\ \mathcal{O}(\exp(-\frac{\gamma}{4})),$$

因为 $v^2+(1-v)^2 \ge \frac{1}{2}$ 适用于 $v \in [0,1]$。 I_1 和 I_2 利用$\frac{dQ(x)}{dx} = -\phi(x)$这一事实，通过分部积分求得。 I_3 没有更简单的形式。我们对 I_3 给出的上界足以回答当前命题。将 I_1、 I_2和 I_3 代入 (12) 后，可得命题所述的 (7)，其中$\sigma = \gamma^{-\frac{1}{2}}$。

■

表达式 $\frac{2}{\sqrt{\pi}} \times \left(1-\frac{1}{N}\right) \times \gamma^{-\frac{1}{2}}$与 $\mathbb{P}(\hat{Y} \neq \hat{X})$ 的蒙特卡罗模拟结果完全吻合，即使信噪比低至 20 分贝（错误率接近 10^{-1}）也是如此。图4展示了不同每帧分箱数下的错误概率 $P_e(\gamma)$ 曲线，范围从每个光子 1 比特到每个光子 4 比特。将图4中的每条曲线向右平移 $20\log_{10}(N)$ 分贝后，即可得到错误概率随归一化信噪比 $P_e(\bar{\gamma})$ 变化的曲线。

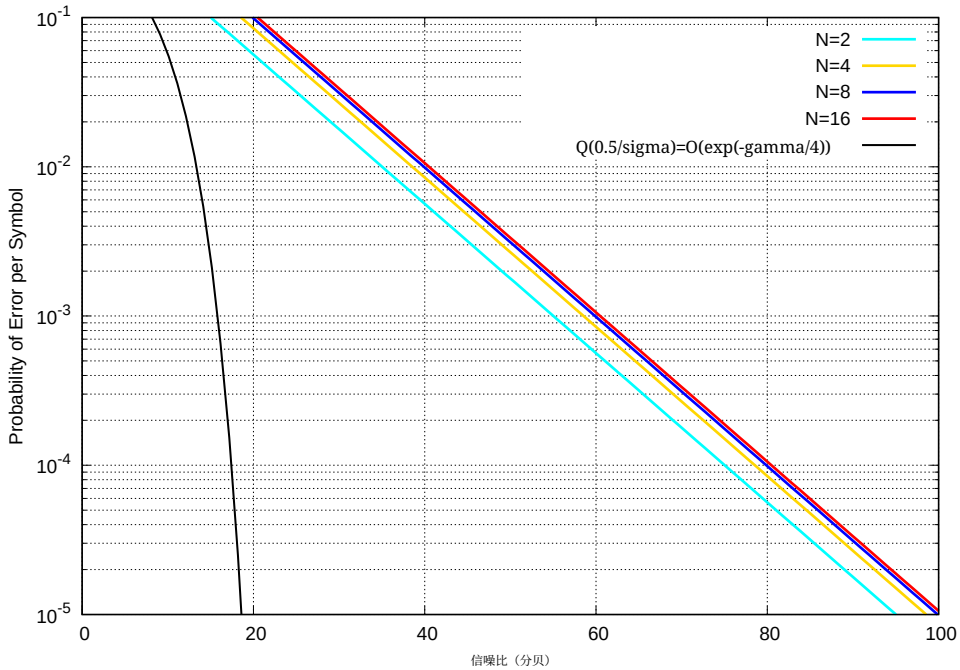


图4. 符号错误概率与信噪比的关系，$\log_2(N)$ 比特/光子，未进行编码。

V. 原始密钥之间的相关性

$\tilde{X}$ 的条件密度可直接由 (1) 得出，

$$p_{\tilde{X}|U}(\tilde{x}|u) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(\tilde{x}-u)^2}{2\sigma^2}\right), \quad \tilde{x} \in \mathbb{R}. \tag{13}$$

在给定 $U=u$ 的条件下， X 和 Y 相互独立。因此，对 (13) 积分后，

$$\mathbb{P}(\tilde{X},\tilde{Y}\in[0,N[|u)=\mathbb{P}(\tilde{X}\in[0,N[|u)^2=\left[Q\left(-\frac{u}{\sigma}\right)-Q\left(\frac{N-u}{\sigma}\right)\right]^2.$$

因此，Alice 和 Bob 的帧均有效的概率为

$$\begin{aligned}\mathbb{P}(\tilde{X},\tilde{Y}\in[0,N[)&=\int_0^N\left[Q\left(-\frac{u}{\sigma}\right)-Q\left(\frac{N-u}{\sigma}\right)\right]^2 p_U(u)\,du\\&=\frac{1}{N}\int_0^N\left[Q\left(-\frac{u}{\sigma}\right)-Q\left(\frac{N-u}{\sigma}\right)\right]^2 du.\end{aligned}\tag{14}$$

˜ X 的密度也可通过对 u积分得到，这等价于对 U 和 Z_1的密度进行卷积，我们得到

$$p_{\tilde{X}}(\tilde{x})=\int_0^N p_{\tilde{X}|U}(\tilde{x}|u)\cdot\frac{1}{N}\,du=\frac{1}{N}\left[Q\left(\frac{-\tilde{x}}{\sigma}\right)-Q\left(\frac{N-\tilde{x}}{\sigma}\right)\right],\quad \tilde{x}\in\mathbb{R}.\tag{15}$$

˜由于 X是 X截断到区间 $[0,N[$,后的版本，在以 $U+Z_1\in[0,N[$,为条件时， X 的密度˜可通过缩放 X的密度确定，即

$$p_{X|U}(x|u)=\frac{p_{\tilde{X}|U}(x|u)}{\int_0^N p_{\tilde{X}|U}(t|u)\,dt}=\frac{\frac{1}{\sqrt{2\pi\sigma^2}}\exp\left(-\frac{(x-u)^2}{2\sigma^2}\right)}{\left[Q\left(-\frac{u}{\sigma}\right)-Q\left(\frac{N-u}{\sigma}\right)\right]},\qquad x,u\in[0,N[,\tag{16}$$

and

$$p_X(x)=\frac{p_{\tilde{X}}(x)}{\int_0^N p_{\tilde{X}}(t)\,dt}=\frac{Q\left(-\frac{x}{\sigma}\right)-Q\left(\frac{N-x}{\sigma}\right)}{\int_0^N\left[Q\left(-\frac{t}{\sigma}\right)-Q\left(\frac{N-t}{\sigma}\right)\right]\,dt},\qquad x\in[0,N[.\tag{17}$$

根据式（1）的对称性，$p_{\tilde{Y}|U}$（$\tilde{y}|u$）、 $p_{\tilde{Y}}$（$\tilde{y}$）、$p_{Y|U}$（$y|u$）和 p_Y（y）分别具有与式（13）、（15）、ˆ（16）和（17）相同的表达式，其中 $\tilde{y}\in\mathbb{R}$ 和 $y\in[0,N[$。分箱的先验概率 $\pi_i=\mathbb{P}$（$X=i$） =ℙ（$X\in[i,i+1]$）变为:

$$\pi_i=\mathbb{P}(\hat{X}=i)=\int_i^{i+1}p_X(x)\,dx=\frac{\int_i^{i+1}\left[Q\left(\frac{-x}{\sigma}\right)-Q\left(\frac{N-x}{\sigma}\right)\right]\,dx}{\int_0^N\left[Q\left(-\frac{t}{\sigma}\right)-Q\left(\frac{N-t}{\sigma}\right)\right]\,dt},\quad i\in\mathbb{Z}_N.\tag{18}$$

在高信噪比下，对于 $\sigma^2\ll 1$，我们有 $\pi_i\approx 1/N,\forall i$，因为在小噪声区间内，截断到区间 $[0,N[$的影响较小。表 I 给出了每帧 $N=8$ 个分箱数时的数值示例。ˆX 的熵非常稳定，如表格最后一列所示：在低信噪比和高信噪比下， $H($ˆ$X)=-\sum_{i=0}^{N-1}\pi_i\log_2(\pi_i)\approx\log_2(N)$。

表 I 每帧 $N=8$ 个分箱时光子分箱的先验概率。

SNR	$\pi_0,\ldots,\pi_7$	$H(\hat{X})$（比特）
10 分贝	0.112796, 0.129062, 0.129071, 0.129071, 0.129071, 0.129071, 0.129062, 0.112796	2.997655
25 分贝	0.122885, 0.125705, 0.125705, 0.125705, 0.125705, 0.125705, 0.125705, 0.122885	2.999931
40 分贝	0.124626, 0.125125, 0.125125, 0.125125, 0.125125, 0.125125, 0.125125, 0.124626	2.999998

以下引理有助于理解当 $\sigma^2 \ll 1$ 时，式 (14)-(18) 在高信噪比下的解析行为。

引理1。设 $f_\sigma(x) = Q\left(-\frac{x}{\sigma}\right) - Q\left(\frac{1-x}{\sigma}\right)$。对于 $\sigma > 0$和 $\gamma = 1/\sigma^2$，根据高斯尾函数 $Q(x)$的性质，差函数 $f_\sigma(x)$ 满足

a) $\forall x \in \mathbb{R}, f_\sigma(x) = f_\sigma(1-x) \in]0,1[$。此外，$f_\sigma(0) = f_\sigma(1) = \frac{1}{2} - \mathcal{O}(\exp(-\frac{\gamma}{2}))$。

b) 对于 $x \in]0,1[$, $f_\sigma(x) = 1 - \mathcal{O}(\exp(-\min^2(x, 1-x) \cdot \frac{\gamma}{2}))$。

c) 对于 $x < 0$，有 $f_\sigma(x) = \mathcal{O}(\exp(-x^2 \cdot \frac{\gamma}{2}))$，且当 $x > 1$时，$f_\sigma(x) = \mathcal{O}(\exp(-(x-1)^2 \cdot \frac{\gamma}{2}))$。
d) 对 f_σ和 f_σ^2进行积分，得到 $\int_0^1 f_\sigma(x)\, dx = 1 - \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{\gamma}} + \mathcal{O}(\exp(-\frac{\gamma}{2})) = 1 - \mathcal{O}(\frac{1}{\sqrt{\gamma}})$ 和 $\int_0^1 f_\sigma^2(x)\, dx = 1 - \frac{1+\sqrt{2}}{\sqrt{\pi}} \cdot \frac{1}{\sqrt{\gamma}} + \mathcal{O}(\exp(-\frac{\gamma}{4})) = 1 - \mathcal{O}(\frac{1}{\sqrt{\gamma}})$。e) $\int_{i/N}^{(i+1)/N} f_\sigma)(x)\, dx = \frac{1}{N} - \mathcal{O}(\frac{1}{\sqrt{\gamma}})$, 适用于 $i = 0$和 $i = N-1$（帧中 N个分箱里的两个边缘区间）。$\int_{i/N}^{(i+1)/N} f_\sigma)(x)\, dx = \frac{1}{N} + \mathcal{O}(\exp(-\beta\gamma))$，适用于 $i = 1 \ldots N-2$（内部区间），其中指数常数为 $\beta = \frac{1}{2}\min^2(\frac{i}{N}, 1 - \frac{i+1}{N})$。

证明：对于 a)，令 G 为标准正态随机变量。有限区间 $[-x, 1-x]$ 永远不会缩减为单个点。我们得到 $f_\sigma(x) = \mathbb{P}(G \in [-x, 1-x]) \in]0,1[$。接着，利用性质 $Q(-x) = 1 - Q(x)$，有 $f_\sigma(1-x) = Q\left(-\frac{(1-x)}{\sigma}\right) - Q\left(\frac{x}{\sigma}\right) = 1 - Q\left(\frac{1-x}{\sigma}\right) - 1 + Q\left(-\frac{x}{\sigma}\right) = f_\sigma(x)$。最后，$f_\sigma(0) = Q(0) - Q\left(\frac{1}{\sigma}\right) = \frac{1}{2} - \mathcal{O}(\exp(-\frac{\gamma}{2}))$。

对于 b)，我们写作 $f_\sigma(x) = 1 - Q\left(\frac{x}{\sigma}\right) - Q\left(\frac{1-x}{\sigma}\right)$。于是 $Q\left(\frac{x}{\sigma}\right) + Q\left(\frac{1-x}{\sigma}\right) \leq \frac{1}{2}\exp(-x^2/(2\sigma^2)) + \frac{1}{2}\exp(-(1-x)^2/(2\sigma^2)) \leq \exp(-\min^2(x, 1-x)\gamma/2)$，从而得到所述结果。这个不等式仅在 $x \in]0,1[$ 时对我们有用，以保持指数衰减。

对于 c)，$x < 0$，因此 $1 - x > -x > 0$。于是 $f_\sigma(x) \leq Q\left(\frac{-x}{\sigma}\right) \leq \frac{1}{2}\exp(-x^2/(2\sigma^2)) = \mathcal{O}(\exp(-x^2\gamma/2))$。对于 $x > 1$，证明过程类似。

如 I_1 命题1的证明中所述，对 $Q(ax)$ 的原函数 $a, x \in \mathbb{R}$ 通过分部积分确定。我们得到

$$\int Q(ax)dx = xQ(ax) - \frac{1}{\sqrt{2\pi a^2}} \exp(-a^2x^2/2) + c, \quad \text{where } c \text{ is the integration constant.} \tag{19}$$

对于 d)，$\int_0^1 f_\sigma(x)\, dx = \int_0^1 \left[1 - Q\left(\frac{x}{\sigma}\right) - Q\left(\frac{1-x}{\sigma}\right)\right] dx = 1 - 2I_1 = 1 - \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{\gamma}} + \mathcal{O}(\exp(-\frac{\gamma}{2}))$，其中 I_1 根据式（19）求得。

如 I_2 中命题1的证明所述，$[Q(ax)]^2$, $a, x \in \mathbb{R}$ 的原函数同样通过分部积分并应用式 (19) 求得。我们得到

$$\int Q^2(ax)dx = xQ^2(ax) - \sqrt{\frac{2}{\pi a^2}}Q(ax)\exp(-a^2x^2/2) + \frac{1}{\sqrt{\pi a^2}}Q(ax\sqrt{2}) + c. \tag{20}$$

然后，$\int_0^1 f_\sigma^2(x)dx = 1 - 4I_1 + 2I_2 + 2I_3 = 1 - 4 \times \frac{\sigma}{\sqrt{2\pi}} + 2 \times \frac{\sqrt{2}-1}{2\sqrt{\pi}}\sigma + \mathcal{O}(\exp(-\frac{\gamma}{4}))$，其中 I_2 根据式 (20) 求得，而 $I_3 = \mathcal{O}(\exp(-\frac{\gamma}{4}))$ 如前所示。至此，d) 的证明完成。

e) 的证明主要基于 (19)，并考虑了帧内的区间位置。我们有

$$
\begin{aligned}
I_4 &= \int_{i/N}^{(i+1)/N} f_\sigma(x)\, dx = \int_{i/N}^{(i+1)/N} \left[1 - Q\left(\frac{x}{\sigma}\right) - Q\left(\frac{1-x}{\sigma}\right)\right] dx \\
&= \frac{1}{N} - \int_{i/N}^{(i+1)/N} Q\left(\frac{x}{\sigma}\right) dx - \int_{1-(i+1)/N}^{1-i/N} Q\left(\frac{x}{\sigma}\right) dx \\
&= \frac{1}{N} - \left[\frac{(i+1)}{N} Q\left(\frac{i+1}{N\sigma}\right) - \frac{i}{N} Q\left(\frac{i}{N\sigma}\right) - \frac{\sigma}{\sqrt{2\pi}} e^{-\frac{\gamma}{2}\frac{(i+1)^2}{N^2}} + \frac{\sigma}{\sqrt{2\pi}} e^{-\frac{\gamma}{2}\frac{i^2}{N^2}}\right] \\
&\quad - \left[(1 - \frac{i}{N}) Q\left(\frac{1 - \frac{i}{N}}{\sigma}\right) - (1 - \frac{i+1}{N}) Q\left(\frac{1 - \frac{i+1}{N}}{\sigma}\right) - \frac{\sigma}{\sqrt{2\pi}} e^{-\frac{\gamma}{2}(1-\frac{i}{N})^2} + \frac{\sigma}{\sqrt{2\pi}} e^{-\frac{\gamma}{2}(1-\frac{i+1}{N})^2}\right].
\end{aligned}
$$

若 $i = 0$ 或 $i = N-1$, $I_4 = \frac{1}{N} - \frac{\sigma}{\sqrt{2\pi}} = 1 - \mathcal{O}(\frac{1}{\sqrt{\gamma}})$，所有指数衰减项都被 $\mathcal{O}(\frac{1}{\sqrt{\gamma}})$ 吸收。对于中间分箱，$i = 1 \ldots N-2$, $I_4 = \frac{1}{N} + \mathcal{O}(e^{-\frac{\gamma}{2}\frac{i^2}{N^2}}) + \mathcal{O}(e^{-\frac{\gamma}{2}(1-\frac{i+1}{N})^2})$，所有衰减更快的项都被这两个较大的 $\mathcal{O}$ 吸收。因此，$I_4 = \frac{1}{N} + \mathcal{O}(e^{-\beta\gamma})$，其中指数常数为 $\beta = \frac{1}{2}\min^2(i/N, 1-(i+1)/N)$。

■

$f_\sigma(x)$ 的收敛在区间 $[0,1]$ 上并不一致。$f_\sigma(x)$ 在点 $x = 0$ 和 $x = 1$ 附近逐点收敛至 0（在 $[0,1]$ 外）或 1（在 $[0,1]$ 内）的速度非常慢。在高信噪比下，两个 $Q()$ 函数之差表现为平方函数，其积分以 $1/\sqrt{\gamma}$ 的速率缓慢趋近于 1。

将 u/N 代入 u 、将 σ/N 代入 σ后，对式（14）—（18）应用引理1，可得以下等式，其中 $\tilde{x}$、x、$u \in]0$、$N[$和 $i \in \mathbb{Z}_N$：

$$
\begin{aligned}
\mathbb{P}(\tilde{X}, \tilde{Y} \in [0, N[) &= 1 - \mathcal{O}(\frac{1}{\sqrt{N^2 \cdot \gamma}}) = 1 - \mathcal{O}(\frac{1}{\sqrt{\overline{\gamma}}}), \\
p_{\tilde{X}}(\tilde{x}) &= \frac{1}{N} - \mathcal{O}(\exp(-\min^2(\frac{\tilde{x}}{N}, 1 - \frac{\tilde{x}}{N}) \cdot \frac{\overline{\gamma}}{2})), \\
p_{X|U}(x|u) &= \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(x-u)^2}{2\sigma^2}\right) \cdot (1 + \mathcal{O}(\exp(-\min^2(\frac{u}{N}, 1 - \frac{u}{N}) \cdot \frac{\overline{\gamma}}{2})), \\
p_X(x) &= \frac{1}{N} \cdot (1 - \mathcal{O}(\exp(-\min^2(\frac{x}{N}, 1 - \frac{x}{N}) \cdot \frac{\overline{\gamma}}{2})) \cdot (1 + \mathcal{O}(\frac{1}{\sqrt{\overline{\gamma}}})), \\
\pi_i &= (\frac{1}{N} \pm \mathcal{O}(g(\overline{\gamma}))) \cdot (1 + \mathcal{O}(\frac{1}{\sqrt{\overline{\gamma}}})),
\end{aligned}
$$

其中，$g(\overline{\gamma})$ 的趋零速率取决于 i，如引理所述。下文中许多表达式的高信噪比特性可通过应用引理1中列出的结果来确定。

为了完成对 Alice 与 Bob 之间量子密钥分发信道的分析，有必要求出软输出和硬输出数学模型中的似然 $p_{Y|\hat{X}}(y|x)$ 以及转移概率 $p_{\hat{Y}|\hat{X}}(\hat{y}|x)$

如图2所示。我们采用与从（13）到（17）类似的方法，先对 U 进行积分，然后在区间 $[0, N[$ 上截断。

Lemm ˜a 2. 已知 Alice 的帧有效，即 $X \in [0, N[$, U 的密度变为 *es*

$$p_{U|\tilde{X}\in[0,N[}(u) = \frac{Q\left(\frac{-u}{\sigma}\right) - Q\left(\frac{N-u}{\sigma}\right)}{\int_0^N \left[Q\left(\frac{-t}{\sigma}\right) - Q\left(\frac{N-t}{\sigma}\right)\right] dt} = p_{U|\tilde{Y}\in[0,N[}(u), \quad u \in [0, N[, \tag{21}$$

其中，$p_{U|\tilde{Y}\in[0,N[}(u)$ 是在 Bob 的帧有效的条件下 U 的密度。此外，当两个帧均有效时，先验概率 $\{\hat{}\pi_i\}_{i=0}^{N-1}$ 为

$$\hat{\pi}_i = \mathbb{P}(\hat{X} = i|\tilde{Y} \in [0, N)) = \frac{\int_0^N \left[Q\left(\frac{i-u}{\sigma}\right) - Q\left(\frac{i+1-u}{\sigma}\right)\right] \cdot \left[Q\left(\frac{-u}{\sigma}\right) - Q\left(\frac{N-u}{\sigma}\right)\right] du}{\int_0^N \left[Q\left(\frac{-u}{\sigma}\right) - Q\left(\frac{N-u}{\sigma}\right)\right]^2 du.} \tag{22}$$

证明：令 应用贝叶斯法则，同时省略下标以简化记号 ：

$$p(u|\tilde{X} \in [0, N[) = \frac{\mathbb{P}(\tilde{X} \in [0, N)|u) \times p_U(u)}{\mathbb{P}(\tilde{X} \in [0, N[)}.$$

由（13）式可得 $\mathbb{P}(\tilde{X} \in [0, N[|u) = Q\left(\frac{-u}{\sigma}\right) - Q\left(\frac{N-u}{\sigma}\right)$。

由（15）式可得 $\mathbb{P}(\tilde{X} \in [0, N[) = \frac{1}{N}\int_0^N \left[Q\left(\frac{-t}{\sigma}\right) - Q\left(\frac{N-t}{\sigma}\right)\right] dt.$

最后，将 $p_U(u) = 1/N$ 代入，即可得到引理 (21) 给出的结果。等式 $p_{U|\tilde{X}\in[0,N[}(u) = p_{U|\tilde{Y}\in[0,N[}(u)$ 则源于我们模型中 Alice 与 Bob 之间的对称性。

˜在确定给定 Bob 的有效帧 ˜ 条件下 X 的密度后，可推导出先验概率 $\hat{}\pi_i$ $Y \in [0, N)$。

$$\begin{aligned} p_{\tilde{X}|\tilde{Y}\in[0,N)}(\tilde{x}) &= \int_0^N p_{\tilde{X}|U,\tilde{Y}\in[0,N[}(\tilde{x}|u) \cdot p_{U|\tilde{Y}\in[0,N[}(u)\ du \\ &= \int_0^N p_{\tilde{X}|U}(\tilde{x}|u) \cdot p_{U|\tilde{Y}\in[0,N[}(u)\ du, \end{aligned} \tag{23}$$

其中这两个因子分别由 (13) 和 (21) 给出。对于 $i = 0, \ldots, N-1$，先验概率 $\hat{}\pi_i = \mathbb{P}(X \in [i, i+1)|Y \in [0, N))$ 变为，

$$\begin{aligned} \hat{\pi}_i &= \int_i^{i+1} p_{X|\tilde{Y}\in[0,N[}(x)\ dx = \int_i^{i+1} \frac{p_{\tilde{X}|\tilde{Y}\in[0,N[}(x)}{\int_0^N p_{\tilde{X}|\tilde{Y}\in[0,N)}(\tilde{x})\ d\tilde{x}}\ dx \\ &= \frac{\int_{x=i}^{i+1}\int_{u=0}^N p_{\tilde{X}|U}(x|u) \cdot p_{U|\tilde{Y}\in[0,N[}(u)\ du\ dx}{\int_{\tilde{x}=0}^N \int_{u=0}^N p_{\tilde{X}|U}(\tilde{x}|u) \cdot p_{U|\tilde{Y}\in[0,N[}(u)\ du\ d\tilde{x}} \\ &= \frac{\int_{u=0}^N \left[Q\left(\frac{i-u}{\sigma}\right) - Q\left(\frac{i+1-u}{\sigma}\right)\right] \cdot p_{U|\tilde{Y}\in[0,N)}(u)\ du\ dx}{\int_{u=0}^N \left[Q\left(\frac{-u}{\sigma}\right) - Q\left(\frac{N-u}{\sigma}\right)\right] \cdot p_{U|\tilde{Y}\in[0,N)}(u)\ du\ d\tilde{x}}. \end{aligned}$$

将 $p_{U|\tilde{Y}\in[0,N[}(u)$ 替换为其在 (21) 中的表达式后，即可得到 (22)。 ■

引理 2 表明，将光子落在帧外的情况排除后，均匀密度 $p_U(u) = \frac{1}{N}$ 会转变为 (21) 中的非均匀密度。此外，在加入 Bob 的帧有效这一条件后，(18) 中的先验概率 π_i 会变为 (22) 中的 $\hat{}\pi_i$。π_i 和 $\hat{}\pi_i$ 已将 Alice 拥有有效帧这一情况考虑在内。下一个引理将用于推导信道似然表达式。

$\hat{}$ 引理 3. 给定 $X = i$ 时 U 的条件密度为

$$p(u|\hat{X} = i) = \frac{Q\left(\frac{i-u}{\sigma}\right) - Q\left(\frac{i+1-u}{\sigma}\right)}{\int_0^N \left[Q\left(\frac{i-t}{\sigma}\right) - Q\left(\frac{i+1-t}{\sigma}\right)\right] dt}, \quad u \in [0, N), \tag{24}$$

对于 $i = 0, \ldots, N-1$。此外，当 Bob 获得有效帧时，在给定 Alice 的分箱编号 i 的条件下，U 的密度为

$$p(u|\hat{X} = i, \tilde{Y} \in [0, N)) = \frac{\left[Q\left(\frac{i-u}{\sigma}\right) - Q\left(\frac{i+1-u}{\sigma}\right)\right] \cdot \left[Q\left(\frac{-u}{\sigma}\right) - Q\left(\frac{N-u}{\sigma}\right)\right]}{\int_0^N \left[Q\left(\frac{i-t}{\sigma}\right) - Q\left(\frac{i+1-t}{\sigma}\right)\right] \cdot \left[Q\left(\frac{-t}{\sigma}\right) - Q\left(\frac{N-t}{\sigma}\right)\right] dt}. \tag{25}$$

$\hat{}\tilde{}$证明：X 和 X 的存在，例如在写出 $X = i$ 时，要求 $X \in [0, N)$。不应忘记这个隐含假设。应用贝叶斯法则，

$$p(u|\hat{X} = i) = p(u|\hat{X} = i, \tilde{X} \in [0, N)) = \frac{\mathbb{P}(\hat{X} = i|u, \tilde{X} \in [0, N)) \times p(u|\tilde{X} \in [0, N))}{\pi_i}.$$

分子中的第一项可展开如下

$$\begin{aligned}\mathbb{P}(\hat{X} = i|u, \tilde{X} \in [0, N) = \mathbb{P}(X \in [i, i+1)|u, \tilde{X} \in [0, N)) &= \frac{\mathbb{P}(\tilde{X} \in [i, i+1)|u)}{\mathbb{P}(\tilde{X} \in [0, N)|u)} \\ &= \frac{Q\left(\frac{i-u}{\sigma}\right) - Q\left(\frac{i+1-u}{\sigma}\right)}{Q\left(\frac{-u}{\sigma}\right) - Q\left(\frac{N-u}{\sigma}\right)}.\end{aligned}$$

分子中的第二项由引理 2 中的式（21）给出。在代入 π_i 的表达式后

由式 (18) 可得

$$p(u|\hat{X} = i) = \frac{Q\left(\frac{i-u}{\sigma}\right) - Q\left(\frac{i+1-u}{\sigma}\right)}{\int_i^{i+1} \left[Q\left(\frac{-t}{\sigma}\right) - Q\left(\frac{N-t}{\sigma}\right)\right] dt},$$

读者可通过变量替换证明

$$\int_i^{i+1} \left[Q\left(\frac{-t}{\sigma}\right) - Q\left(\frac{N-t}{\sigma}\right)\right] dt \;=\; \int_0^N \left[Q\left(\frac{i-t}{\sigma}\right) - Q\left(\frac{i+1-t}{\sigma}\right)\right] dt. \tag{26}$$

由此得到引理 (24) 中给出的结果。

(25) 的证明与 (24) 的证明步骤类似。首先，利用贝叶斯法则和 (14)，我们得到 U 的条件密度，

$$p(u|\tilde{X}, \tilde{Y} \in [0, N)) = \frac{\left[Q\left(\frac{-u}{\sigma}\right) - Q\left(\frac{N-u}{\sigma}\right)\right]^2}{\int_0^N \left[Q\left(\frac{-t}{\sigma}\right) - Q\left(\frac{N-t}{\sigma}\right)\right]^2 dt}. \tag{27}$$

其次，我们求出 Alice 的光子分箱的条件概率，

$$\begin{aligned}\mathbb{P}(\hat{X}=i|u,\tilde{X},\tilde{Y}\in[0,N)) &= \frac{\mathbb{P}(\tilde{X}\in[i,i+1),\tilde{Y}\in[0,N)|u)}{\mathbb{P}(\tilde{X},\tilde{Y}\in[0,N)|u)} \\ &= \frac{\left[Q\left(\frac{i-u}{\sigma}\right)-Q\left(\frac{i+1-u}{\sigma}\right)\right]\cdot\left[Q\left(\frac{-u}{\sigma}\right)-Q\left(\frac{N-u}{\sigma}\right)\right]}{\left[Q\left(\frac{-u}{\sigma}\right)-Q\left(\frac{N-u}{\sigma}\right)\right]^2}.\end{aligned}$$

最后，我们使用上述 $\mathbb{P}(X=i|u,X,Y\in[0,N))$ 和 $p(u|X,Y\in[0,N))$ 的表达式，以及引理 2 中的式 (22)，

$$p(u|\hat{X}=i,\tilde{Y}\in[0,N)) = \frac{\mathbb{P}(\hat{X}=i|u,\tilde{X},\tilde{Y}\in[0,N))\times p(u|\tilde{X},\tilde{Y}\in[0,n))}{\hat{\pi}_i}$$

从而得到本引理中的式 (25)。 ■

如我们在引理 3 的证明中针对 X 所述， Y的存在性假设 $Y\in[0,N)$。我们特意在下一条陈述中似然函数的下标里提醒读者注意条件 $Y\in[0,N)$。

定理 1. 假设 Alice 和 Bob 均获得有效帧，则软输出 QKD 信道模型的似然 $p(y|x)=p_{Y|\hat{X},\,\tilde{Y}\in[0,N)}(y|x)$ 可表示为

$$p_{Y|\hat{X},\tilde{Y}\in[0,N)}(y|\hat{x}=i) \;=\; \frac{\int_0^N \frac{1}{\sqrt{2\pi\sigma^2}}\exp\left(-\frac{(y-u)^2}{2\sigma^2}\right)\cdot\left[Q\left(\frac{i-u}{\sigma}\right)-Q\left(\frac{i+1-u}{\sigma}\right)\right]\,du}{\int_0^N\left[Q\left(\frac{-t}{\sigma}\right)-Q\left(\frac{N-t}{\sigma}\right)\right]\cdot\left[Q\left(\frac{i-t}{\sigma}\right)-Q\left(\frac{i+1-t}{\sigma}\right)\right]\,dt}, \tag{28}$$

对于 $i=0,\ldots,N-1$, $y\in[0,N)$。为简便起见，后续各节将式 (28) 中的似然记作 $p(y|X=i)$。

证明：在可能的情况下，我们省略密度函数中的下标，以简化符号表示。我们先进行边缘化，然后再截断 $p(\tilde{y}|u)$。

$$\begin{aligned}p(y|\hat{X}=i,\tilde{Y}\in[0,N)) &= \int_0^N p(y,u|\hat{X}=i,\tilde{Y}\in[0,N))\,du \\ &= \int_0^N p(y|u,\hat{X}=i,\tilde{Y}\in[0,N))\cdot p(u|\hat{X}=i,\tilde{Y}\in[0,N))\,du \\ &= \int_0^N p(y|u)\cdot p(u|\hat{X}=i,\tilde{Y}\in[0,N))\,du, \end{aligned}\tag{29}$$

积分 (29) 中的左侧因子 $p(y|u)$ 是由 (13) 中的密度截断得到的（将 x 替换为 y），右侧因子则由引理 (3) 求得。

$$p(y|\hat{X}=i,\tilde{Y}\in[0,N)) = \int_0^N \frac{p(\tilde{y}=y|u)}{\int_0^N p(\tilde{y}|u)d\tilde{y}}\cdot p(u|\hat{X}=i,\tilde{Y}\in[0,N))\,du,$$

$$= \int_0^N \frac{\frac{1}{\sqrt{2\pi\sigma^2}}\exp\left(-\frac{(y-u)^2}{2\sigma^2}\right)}{Q\left(\frac{-u}{\sigma}\right)-Q\left(\frac{N-u}{\sigma}\right)} \cdot \frac{\left[Q\left(\frac{i-u}{\sigma}\right)-Q\left(\frac{i+1-u}{\sigma}\right)\right]\cdot\left[Q\left(\frac{-u}{\sigma}\right)-Q\left(\frac{N-u}{\sigma}\right)\right]}{\int_0^N \left[Q\left(\frac{i-t}{\sigma}\right)-Q\left(\frac{i+1-t}{\sigma}\right)\right]\cdot\left[Q\left(\frac{-t}{\sigma}\right)-Q\left(\frac{N-t}{\sigma}\right)\right]\,dt}\,du.$$

化简项 $Q\left(\frac{-u}{\sigma}\right)-Q\left(\frac{N-u}{\sigma}\right)$ 后，我们便得到所述结果。 ■

硬输出量子密钥分发信道模型的转移概率 $p_{i,\ j}=\mathbb{P}(Y=j|X=i)$，可通过对前述定理所建立的软输出条件概率密度函数 Y 直接积分得出。

推论1. 在 Alice 的光子落入区间 i 的条件下，Bob 的光子落入区间 j 的概率为

$$p_{ij} \ = \ \mathbb{P}(\hat{Y}=j|\hat{X}=i)=\frac{\int_0^N \left[Q\left(\frac{j-u}{\sigma}\right)-Q\left(\frac{j+1-u}{\sigma}\right)\right]\cdot\left[Q\left(\frac{i-u}{\sigma}\right)-Q\left(\frac{i+1-u}{\sigma}\right)\right]\,du}{\int_0^N \left[Q\left(\frac{-t}{\sigma}\right)-Q\left(\frac{N-t}{\sigma}\right)\right]\cdot\left[Q\left(\frac{i-t}{\sigma}\right)-Q\left(\frac{i+1-t}{\sigma}\right)\right]\,dt},\quad i,j\in\mathbb{Z}_N. \quad (30)$$

证明：对 Bob 的光子位置 y 从 j 到 $j+1$ 对式 (28) 积分，然后交换两个积分的顺序，即可得到本推论给出的结果。 ■

最后，我们给出适用于软判决译码的后验概率表达式，例如低密度奇偶校验码的置信传播译码、线性分组码的有序统计译码，或卷积码的维特比译码。令 $APP(i) \ \hat{=}\ APP(X=i) \ = \mathbb{P}(X=i|Y=y)$ 表示在 $i=0\ldots N-1$ 条件下 Alice 的光子分箱编号 i 的后验概率。下一个定理给出表达式 $APP(i)$，该表达式用于我们在第七节提出的编码/译码方案。

定理2. 给定 Bob 一侧的光子位置 $Y=y$，Alice 的光子属于分箱编号 i 的概率为

$$APP(i)=\frac{\int_0^N \frac{1}{\sqrt{2\pi\sigma^2}}e^{-\frac{(y-u)^2}{2\sigma^2}}\cdot\left[Q\left(\frac{i-u}{\sigma}\right)-Q\left(\frac{i+1-u}{\sigma}\right)\right]\,du}{\int_0^N \frac{1}{\sqrt{2\pi\sigma^2}}e^{-\frac{(y-t)^2}{2\sigma^2}}\cdot\left[Q\left(\frac{-t}{\sigma}\right)-Q\left(\frac{N-t}{\sigma}\right)\right]\,dt},\quad i\in\mathbb{Z}_N. \quad (31)$$

证明：注意到 $X,Y\in[0,N)$，应用贝叶斯法则可得

$$\mathbb{P}(\hat{X}=i|Y=y)=\frac{p(y|\hat{X}=i)\cdot\mathbb{P}(\hat{X}=i)}{p(y)}.$$

定理所述结果可通过以下三个步骤得出。

(i) 对 $p(y|X=i)$ 使用定理 1 中的 (28)。(ii) 对先验 $\mathbb{P}(X=i)$ 使用 (22)。(iii) 最后，在截断Y的密度后，$p(y)=p_{Y|\tilde{X}\in[0,N)}(y)=p_{\tilde{Y}|\tilde{X}\in[0,N)}(\tilde{y}=y)/\int_0^N p_{\tilde{Y}|\tilde{X}\in[0,N)}(t)\,dt$。密度 $p_{\tilde{Y}|\tilde{X}\in[0,N)}(\tilde{y})$ 可由 (23) 得出，同时交换字母 x（分别为 X）和 y（分别为 Y），

结合 (13) 和 (21),

$$p(y)=\frac{\int_0^N \frac{1}{\sqrt{2\pi\sigma^2}}e^{-\frac{(y-u)^2}{2\sigma^2}}\cdot\left[Q\left(\frac{-u}{\sigma}\right)-Q\left(\frac{N-u}{\sigma}\right)\right]du}{\int_0^N\left[Q\left(\frac{-t}{\sigma}\right)-Q\left(\frac{N-t}{\sigma}\right)\right]^2dt}. \tag{32}$$

■

为保持一致，读者可以检查定理2证明末尾给出的 $p(y)$ 是否也等于由公式（22）和（28）得到的 $\sum_{i=0}^{N-1}\hat{}\pi_i\cdot p(y|\hat{}X=i)$。图5和图6分别绘出了低信噪比 $\gamma=10$ 分贝（光子探测器精度较低）和相对较高的信噪比 $\gamma=25$ 分贝（光子探测器精度较高）下的似然 $p(y|\hat{}X=i)$。在低信噪比下， $p(y|X=i)$ 呈高斯形状。信噪比较高时，其形状趋于方形。后验概率 $APP(i)$、 $i\in\mathbb{Z}_N$ 的图形与信道似然相似。

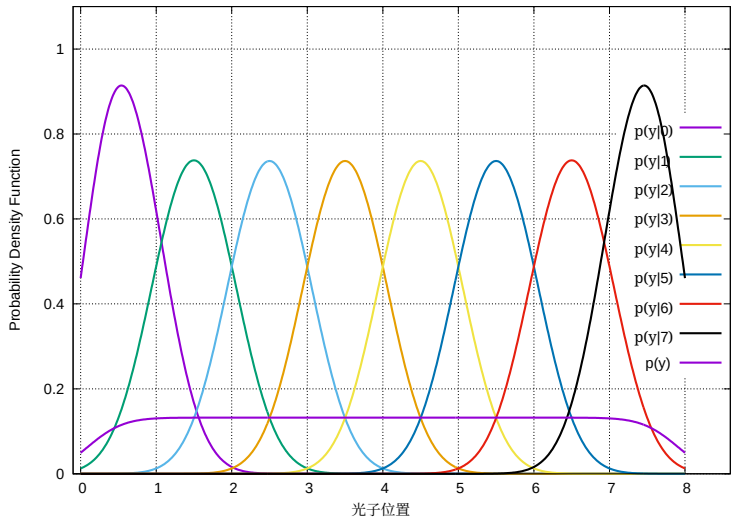


图 5. 软输出信道似然，每帧 =8 个分箱，信噪比 =10 分贝。

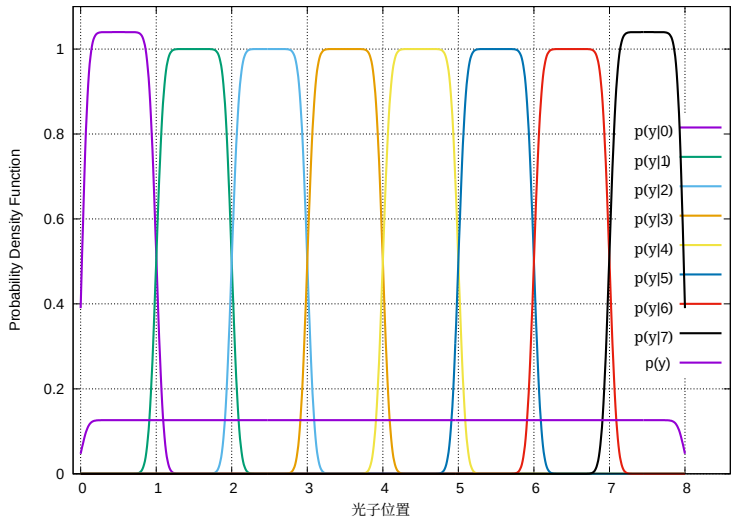


图 6. 软输出信道似然，每帧分箱数为 N=8，信噪比为 =25 分贝。

VI. 秘密密钥信息率

A. 原始密钥之间的互信息

首先，我们考虑由转移概率 $p(\hat{}y|\hat{}x) = \mathbb{P}(Y = \hat{}y|X = \hat{}x)$ 定义的代数硬输出信道的互信息。在推论1中，已推导出 $p_{ij} = p(Y = j|X = i)$ 的表达式。因此，我们可以直接计算互信息如下：

$$\begin{aligned} I(\hat{X};\hat{Y}) &= H(\hat{Y}) - H(\hat{Y}|\hat{X}) \\ &= -\sum_{i=0}^{N-1} \mathbb{P}(\hat{Y}=i)\log(\mathbb{P}(\hat{Y}=i)) \\ &\quad + \sum_{i=0}^{N-1} \mathbb{P}(\hat{X}=i) \sum_{j=0}^{N-1} \mathbb{P}(\hat{Y}=j|\hat{X}=i)\log(\mathbb{P}(\hat{Y}=j|\hat{X}=i)) \\ &= -\sum_{i=0}^{N-1} \hat{\pi}_i \log(\hat{\pi}_i) \; + \sum_{i=0}^{N-1} \hat{\pi}_i \sum_{j=0}^{N-1} p_{ij}\log(p_{ij}), \end{aligned} \tag{33}$$

$\hat{}\,\hat{}\,\hat{}\,\hat{}$ 其中，先验 $\hat{}\pi_i$ of X and Y 可由式（22）求得。图7展示了 $I(X;Y)$ 以比特为单位随信噪比变化的曲线，对应每个传输光子包含 2、3 和 4 个编码比特。正如预期，在高信噪比下，曲线趋向渐近线 $H(\hat{}X)$。事实上，熵 $-\sum_{i=0}^{N-1} \hat{}\pi_i \log(\hat{}\pi_i)$ 即使在低信噪比下也非常稳定，可用 $\log(N)$ 很好地近似。式（ 33 ）中的求和可截断到相邻区间，或截断到与其整数距离小于 D 的分箱，

$$I(\hat{X};\hat{Y}) \approx \log(N) + \frac{1}{N} \sum_{|i-j|\le D} p_{ij}\log(p_{ij}). \tag{34}$$

对于 $D = 1$ ，简化式（34）在低至 $\gamma \ge 10$ 分贝时仍是极佳的近似；对于 $D = 2$，该近似则可延伸至 $\gamma \ge 5$ 分贝。接下来的命题将进一步阐释先验概率、转移概率以及低噪声区间内离散信道互信息的行为。

命题2. 在高信噪比下，当 $\sigma^2 \ll 1$ 时，我们得到以下结果：a) 推论1中建立的硬输出量子密钥分发信道的转移概率满足：在两个极端分箱 $i = 0$ 和 $i = N-1$ 处，我们有

$$p_{0,1} = \frac{\frac{\sigma}{\sqrt{\pi}} + \mathcal{O}(e^{-\frac{\gamma}{4}})}{1 - \frac{1+\sqrt{2}}{2\sqrt{\pi}} \cdot \sigma + \mathcal{O}(e^{-\frac{\gamma}{4}})}, \tag{35}$$

其中 $p_{0,\ 1} = p_{N-1,\ N-2} = 1 - p_{0,\ 0} = 1 - p_{N-1,\ N-1}$ 和 $\sigma = 1/\sqrt{\gamma}$。

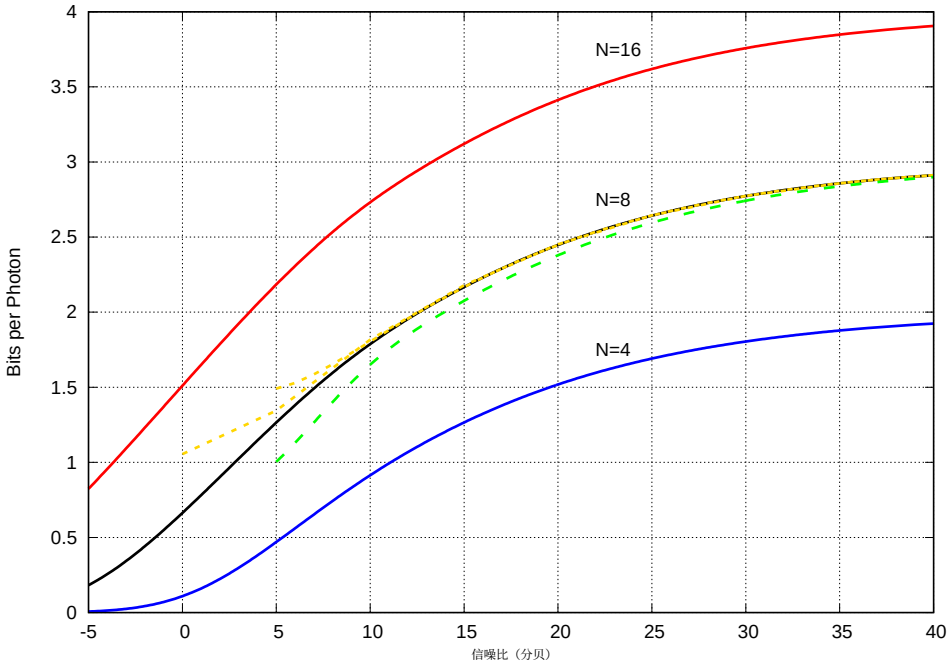


图 7。 互 信息 $I(\hat{X};\hat{Y})$，代数硬输出 TE-QKD 信道的互信息，其中 $N=4$、8、16 是每帧分箱数。

对于中间分箱 $i=2\ldots N-2$，我们有

$$p_{1,2}=\frac{\frac{\sigma}{\sqrt{\pi}}+\mathcal{O}(e^{-\frac{\gamma}{4}})}{1-\mathcal{O}(e^{-\frac{\gamma}{4}})}, \tag{36}$$

其中 $p_{1,\ 2}=p_{i,\ i+1}=p_{i,\ i-1}=(1-p_{i,\ i})/2$。对于 $|i-j|\geq 2$，其余所有转移概率 $p_{i,\ j}$均为 $\mathcal{O}(e^{-\frac{\gamma}{4}})$，在高信噪比下进行任何数值计算时都可将其强制设为 0。

b) 引理 2 中确定的先验概率满足

在两个极端分箱 $i=0$ 和 $i=N-1$ 处，我们有

$$\hat{\pi}_0=\hat{\pi}_{N-1}=\frac{1-\frac{1+\sqrt{2}}{2\sqrt{\pi}}\cdot\sigma+\mathcal{O}(e^{-\frac{\gamma}{4}})}{N\cdot\left[1-\frac{1+\sqrt{2}}{\sqrt{\pi}}\cdot\overline{\sigma}+\mathcal{O}(e^{-\frac{\gamma}{4}})\right]}, \tag{37}$$

其中分子包含 σ，而分母涉及 $\overline{\sigma}=\sigma/N$。对于中间分箱，当$i=2\ldots N-2$时，我们有

$$\hat{\pi}_i=\frac{1-\mathcal{O}(e^{-\frac{\gamma}{4}})}{N\cdot\left[1-\frac{1+\sqrt{2}}{\sqrt{\pi}}\cdot\overline{\sigma}+\mathcal{O}(e^{-\frac{\gamma}{4}})\right]}. \tag{38}$$

c) 根据 a) 和 b)，式 (33) 给出的离散输入离散输出 QKD 信道的互信息变为

$$\begin{aligned}I(\hat{X};\hat{Y})=&\frac{N-2\beta\sigma}{N(1-2\beta\overline{\sigma})}\log\left[N(1-2\beta\overline{\sigma})\right]-\frac{2(1-\beta\sigma)}{N(1-2\beta\overline{\sigma})}\log(1-\beta\sigma)\\&-\frac{2(1-\beta\sigma)}{N(1-2\beta\overline{\sigma})}H_2\left(\frac{\sigma/\sqrt{\pi}}{1-\beta\sigma}\right)-\frac{(N-2)}{N(1-2\beta\overline{\sigma})}H_3\left(\frac{\sigma}{\sqrt{\pi}}\right)+\mathcal{O}(e^{-\frac{\gamma}{4}}),\end{aligned} \tag{39}$$

其中 $\beta = \frac{1+\sqrt{2}}{2\sqrt{\pi}}$、 $\sigma = 1/\sqrt{\gamma}$ 和 $\overline{\sigma} = \sigma/N$。

证明：由于篇幅所限，我们仅详细证明 $p_{0,1}$ 的分母（也等于 $\hat{}\pi_0$ 的分子）。其余结果均可用类似的微积分方法得出。根据推论1（$i = 0, j = 1$），$p_{0,1}$ 的分母等于以下积分

$$
\begin{aligned}
I_5 &= \int_0^N \left[Q\left(\tfrac{-t}{\sigma}\right) - Q\left(\tfrac{N-t}{\sigma}\right)\right] \cdot \left[Q\left(\tfrac{-t}{\sigma}\right) - Q\left(\tfrac{1-t}{\sigma}\right)\right] \, dt \\
&= \int_0^N \left[1 - Q\left(\tfrac{t}{\sigma}\right) - Q\left(\tfrac{N-t}{\sigma}\right)\right] \cdot \left[Q\left(\tfrac{t-1}{\sigma}\right) - Q\left(\tfrac{t}{\sigma}\right)\right] \, dt \\
&= \int_0^N Q\left(\tfrac{t-1}{\sigma}\right) \, dt - \int_0^N Q\left(\tfrac{t}{\sigma}\right) \, dt + \int_0^N Q^2\left(\tfrac{t}{\sigma}\right) \, dt - \int_0^N Q\left(\tfrac{t}{\sigma}\right) Q\left(\tfrac{t-1}{\sigma}\right) \, dt \\
&- \int_0^N Q\left(\tfrac{N-t}{\sigma}\right) Q\left(\tfrac{t-1}{\sigma}\right) \, dt + \int_0^N Q\left(\tfrac{N-t}{\sigma}\right) Q\left(\tfrac{t}{\sigma}\right) \, dt \\
&= \underbrace{\int_{-1}^0 Q\left(\tfrac{t}{\sigma}\right) \, dt}_{(i)} - \underbrace{\int_{N-1}^N Q\left(\tfrac{t}{\sigma}\right) \, dt}_{(ii)} + \underbrace{\int_0^N Q^2\left(\tfrac{t}{\sigma}\right) \, dt}_{(iii)} - \underbrace{\int_0^1 Q\left(\tfrac{t}{\sigma}\right)\left(1 - Q\left(\tfrac{1-t}{\sigma}\right)\right) \, dt}_{(iv)} \\
&- \underbrace{\int_1^N Q\left(\tfrac{t}{\sigma}\right) Q\left(\tfrac{t-1}{\sigma}\right) \, dt}_{(v)} - \underbrace{\int_0^1 Q\left(\tfrac{N-t}{\sigma}\right)\left(1 - Q\left(\tfrac{1-t}{\sigma}\right)\right) \, dt}_{(vi)} \\
&- \underbrace{\int_1^N Q\left(\tfrac{N-t}{\sigma}\right) Q\left(\tfrac{t-1}{\sigma}\right) \, dt}_{(vii)} + \underbrace{\int_0^N Q\left(\tfrac{N-t}{\sigma}\right) Q\left(\tfrac{t}{\sigma}\right) \, dt}_{(viii)}.
\end{aligned}
$$

现在我们逐一求解初等积分 (i)–(viii)。
利用 (19)，$(i) = 0 - \frac{\sigma}{\sqrt{2\pi}} + Q(\frac{-1}{\sigma}) + \frac{\sigma}{\sqrt{2\pi}} e^{-\frac{\gamma}{2}} = 1 - \frac{\sigma}{\sqrt{2\pi}} + \mathcal{O}(e^{-\frac{\gamma}{2}})$。根据 $Q(x)$ 是单调递减函数这一事实，可得 $(ii) = \mathcal{O}(e^{-(N-1)^2\frac{\gamma}{2}})$。第三个积分可直接通过 (20) 求解：$(iii) = NQ^2(\frac{N}{\sigma}) - \sigma\sqrt{\frac{2}{\pi}} Q(\frac{N}{\sigma}) e^{-N^2\frac{\gamma}{2}} + \frac{\sigma}{\sqrt{\pi}} Q(\frac{N\sqrt{2}}{\sigma}) - 0 + \sigma\sqrt{\frac{2}{\pi}} \cdot \frac{1}{2} - \frac{\sigma}{\sqrt{\pi}} \cdot \frac{1}{2}$。然后得到 $(iii) = \left(\frac{\sqrt{2}-1}{2\sqrt{\pi}}\right)\sigma + \mathcal{O}(e^{-N^2\frac{\gamma}{2}})$。$(iv) = I_1 - I_3 = \frac{\sigma}{\sqrt{2\pi}} + \mathcal{O}(e^{-\frac{\gamma}{4}})$。对于 (v)，$t^2 + (t-1)^2 \geq 1$ 在区间 $[1, N]$ 内，因此有 $(v) = \mathcal{O}(e^{-\frac{\gamma}{2}})$。(vi) 的第一部分为 $\mathcal{O}(e^{-(N-1)^2\frac{\gamma}{2}})$，第二部分也为 $\mathcal{O}(e^{-(N-1)^2\frac{\gamma}{2}})$，因为 $(N-t)^2 + (1-t)^2 \geq (N-1)^2$ 在区间 $[0, 1]$ 内。因此 $(vi) = \mathcal{O}(e^{-(N-1)^2\frac{\gamma}{2}})$。应用类似的论证，可得 $(vii) = \mathcal{O}(e^{-(N-1)^2\frac{\gamma}{4}})$ 和 $(viii) = \mathcal{O}(e^{-N^2\frac{\gamma}{4}})$。合并 (i)–(viii) 得到 $I_5 = 1 - \frac{1+\sqrt{2}}{2\sqrt{\pi}}\sigma + \mathcal{O}(e^{-\frac{\gamma}{4}})$，如前所述。

■

在高信噪比下，命题2-a) 展示了 $p_{i,j}$ 收敛到 $\frac{\sigma}{\sqrt{\pi}}$ 的速度。后者是单边差错概率，也是命题1中所述双边差错概率的一半。正如预期，在命题2-b) 中发现，对于内部区间，$\hat{}\pi_i$ 收敛到 $1/N$ 的速度要快得多。命题2-c) 中给出的高信噪比下 $I(X;Y)$ 的表达式与离散信道的精确互信息完全吻合

直到 $\gamma = 10$ 分贝，随后在低于 10 分贝的低信噪比下开始偏离。二元熵函数表示极端分箱的错误。三元熵函数表示内部区间的错误。表达式 (39) 是一种快速计算 $I(X;Y)$ 的方法，适用于中高信噪比，且无需进行任何积分。

可以探讨一下：若假设 TE-QKD 离散信道具有循环转移概率矩阵，那么近似互信息的准确度如何。在命题1的假设下，我们取：1- X 和 Y 服从高斯分布；2- 所有区间的概率均相等；3- 离散输入离散输出信道的错误概率主要由 X 和 Y 仅相隔一或两个区间的事件决定。根据 [10, 第7章 2], 中的定理7.2.1，循环离散信道的表达式为

$$I(\hat{X};\hat{Y}) \approx \log(N) + \sum_{j=-2}^{2} p_{0j} \log_2(p_{0j}), \tag{40}$$

其中$p_{01} = p_{0,\,-1} \approx \int_0^1 2p_1p_2\ dv = 2\ (I_1 - I_2 - I_3)$，$p_{02} = p_{0,\,-2} \approx \int_0^1 2p_2p_3\ dv = 2I_3$，且 p_{00} =1 − 2p_{01} − 2p_{02}。对于每帧有 $N = 8$ 个区间的情况，图7中从上到下的点线分别表示三个高信噪比近似式（39）、带有 $D = 2$的（34）以及（40）。（39）和（34）在高信噪比下符合精确互信息 I（X； Y）。（40）在 $N = 8$ 时不够紧，但每帧有 $N \geq 16$ 个区间时会更紧。

本节的第二步是计算软输出 TE-QKD ˆ ˆ ˆ 信道的互信息。我们选择写成 $I(X;Y) = H(X) - H(X|Y)$。从数值稳定性的角度来看，根据微分熵交换 X和 Y后得到的第二个表达式也等价，而且其中的所有项都已在上一节中确定。我们更倾向于采用能显现高信噪比渐近线的互信息，因此

$$I(\hat{X};Y) = H(\hat{X}) - H(\hat{X}|Y) = H(\hat{X}) + \sum_{i=0}^{N-1} \hat{\pi}_i \int_0^N p(y|\hat{x}=i) \log_2(APP(i))\ dy, \tag{41}$$

其中，先验 ˆπ_i 来自式 (22)，似然 $p(y|\hat{x} = i)$ 来自式 (28)，后验 $APP(i)$ ˆ 来自式 (31)。图 8 展示了不同每帧分箱数下，互信息 $I(X;Y)$ 随归一化信噪比 $\bar{\gamma}$ 的变化。红色上包络由下一节的定理 3 给出，它对应于时间纠缠量子密钥分发信道上可实现的最大互信息。

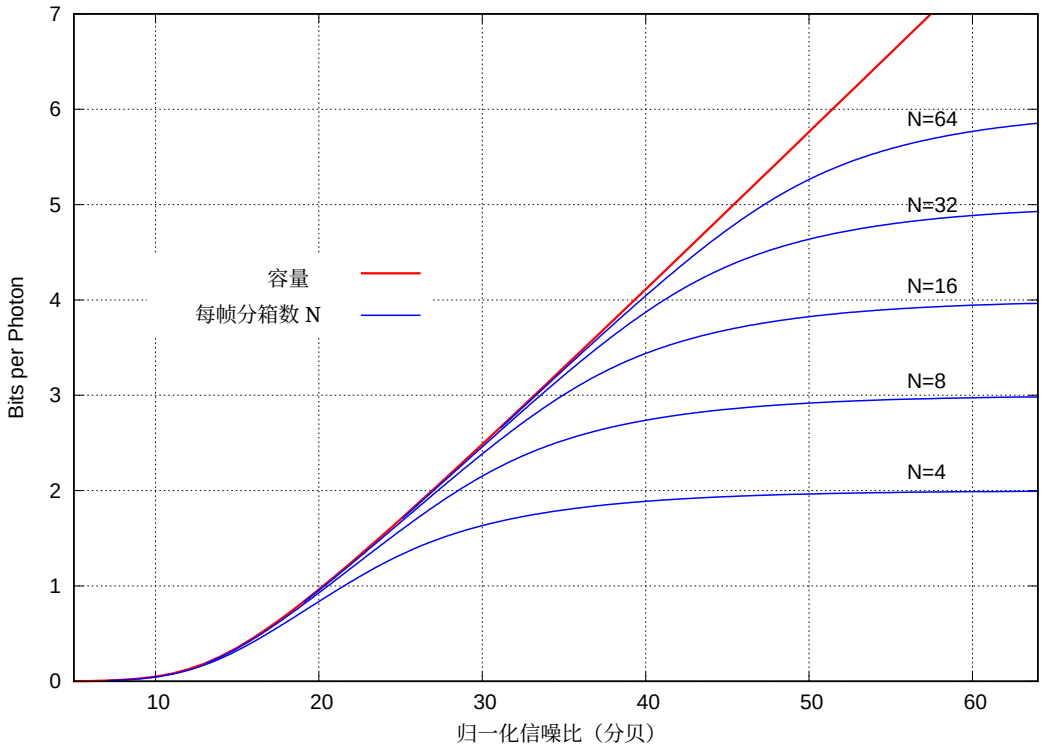


Fig. 8. 软输出量子密钥分发信道的互信息 $I(\hat{X};Y)$，对应 $N=4$、8、16 个每帧分箱数。

B. 最大保密速率

^ ^ 随机变量 X、 X 和 Y 构成马尔可夫链 $X \to X \to Y$。因此，数据处理不等式 [10, 第 2] 章给出

$$I(\hat{X};Y) \leq I(X;Y), \quad \forall\, N \geq 2. \tag{42}$$

因此，对于每帧分箱数 N 的任意取值，我们的信道 $p_{Y|\hat{X}}(y|\hat{x})$ 的速率始终不超过连续输入连续输出信道 $p_{Y|X}(y|x)$ 的速率；该信道对应于 Alice 帧中由零测度区间构成的连续统。因此，通过确定互信息 $I(X;Y)$，我们即可得到 Alice 与 Bob 之间光子信道的最大保密速率。

不失一般性，假设帧长为 1，而不是 N。现在，问题是求解 $I(X;Y)$，其中 X 和 Y 是原始光子位置 $X = X \in [0,1)$、$Y = \tilde{Y} \in [0,1)$ 的截断版本。在此模型中，式 (1) 变为 $\tilde{X} = U + \mathcal{N}(0,\sigma^2)$、 $\tilde{Y} = U + \mathcal{N}(0,\sigma^2)$， U 在 $[0,1)$ 上服从均匀分布，且两个加性高斯噪声相互独立。在区间数无限且帧长为单位长度的情况下，归一化信噪比自然定义为 $\gamma = \overline{\gamma} = 1/\sigma^2$ 。

定理 3。最大保密速率 $I(X;Y)$ 为

$$I(X;Y) = h(Y) - h(Y|X) \tag{43}$$

$$= -\int_0^1 p(y)\ \log(p(y))\ dy\ +\ \int_0^1 p(x)\int_0^1 p(y|x)\ \log(p(y|x))\ dxdy \tag{44}$$

其中，$p(x)$ 和 $p(y)$ 是将帧长 N 替换为 1 后由 (32) 得到的，

$$p(x) = p_{X|\tilde{X},\tilde{Y}\in[0,1)}(x) = \frac{\int_0^1 \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-u)^2}{2\sigma^2}} \left[Q\left(\frac{-u}{\sigma}\right) - Q\left(\frac{1-u}{\sigma}\right)\right] du}{\int_0^1 \left[Q\left(\frac{-t}{\sigma}\right) - Q\left(\frac{1-t}{\sigma}\right)\right]^2 dt}, \tag{45}$$

$$p(y) = p_{Y|\tilde{X},\tilde{Y}\in[0,1)}(y) = \frac{\int_0^1 \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(y-u)^2}{2\sigma^2}} \left[Q\left(\frac{-u}{\sigma}\right) - Q\left(\frac{1-u}{\sigma}\right)\right] du}{\int_0^1 \left[Q\left(\frac{-t}{\sigma}\right) - Q\left(\frac{1-t}{\sigma}\right)\right]^2 dt}, \tag{46}$$

$$p(y|x) = \frac{1}{\sqrt{4\pi\sigma^2}} e^{-\frac{(y-x)^2}{4\sigma^2}} \frac{\left[Q\left(\frac{0-(x+y)/2}{\sigma/\sqrt{2}}\right) - Q\left(\frac{1-(x+y)/2}{\sigma/\sqrt{2}}\right)\right]}{\int_0^1 \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-u)^2}{2\sigma^2}} \left[Q\left(\frac{-u}{\sigma}\right) - Q\left(\frac{1-u}{\sigma}\right)\right] du}. \tag{47}$$

证明：我们通过求出条件密度 $p(y|x)$ 的表达式来完成证明。事实上，对变量进行边缘化并应用贝叶斯法则后，可以写为

$$p(y|x) = p_{Y|X,\tilde{X},\tilde{Y}\in[0,1)}(y|x) = \int_0^1 p(y,u|x)\ du = \int_0^1 \frac{p(u)p(x|u)p(y|u)}{p(x)} du. \tag{48}$$

在上述积分表达式中，我们利用了由 (1) 定义的模型所得到的事实：$p(x,y|u) = p(x|u)p(y|u)$。在 (48) 中，$p(x|u)$ 和 $p(y|u)$ 均由 (16) 得到，$p(x)$ 由 (32) 得到，最后，$p(u) = p_{U|\tilde{X},\ \tilde{Y}\in[0,1)}(u)$ 由 (27) 得到；以上各式均是在将 1 代入 N 后得到的。化简 (48) 的被积函数后，我们得到 (47) 所示的 $p(y|x)$。

■

推论 2. 在高信噪比下，即 $\sigma^2 \ll 1$，或等价地 $\gamma = \frac{1}{\sigma^2} \gg 1$，最大保密速率满足

$$I(X;Y) = (1 + \mathcal{O}(\tfrac{1}{\sqrt{\gamma}})) \cdot \frac{1}{2}\log\left(\frac{\gamma}{4\pi e}\right)\ +\ \mathcal{O}\left((\tfrac{1}{\sqrt{\gamma}})^{\alpha}\right) \sim \frac{1}{2}\log\left(\frac{\gamma}{4\pi e}\right), \quad \forall \alpha \in]0,1[. \tag{49}$$

证明：证明基于巴比伦方法，需要大量微积分运算。我们先简要说明如何猜出这个极限。应用引理1并进行一些额外的代数运算后，当 $\gamma \gg 1$ 时，我们得到，在式（45）、（46）和（47）中，$p(x) \to 1$、$p(y) \to 1$ 和 $p(y|x) \to \frac{1}{\sqrt{4\pi\sigma^2}} e^{-\frac{(y-x)^2}{4\sigma^2}}$ 分别成立，其中 $x, y \in]0,1[$。然后，微分熵 $h(Y) \to 0$, $h(Y|X) \to h(\mathcal{N}(0, 2\sigma^2)) = \frac{1}{2}\log(4\pi e\sigma^2)$，因此最大保密速率满足 $I(X;Y) = h(Y) - h(Y|X) \to \frac{1}{2}\log\left(\frac{\gamma}{4\pi e}\right)$。以上简要而清晰地概述了所有相关概率密度和最大互信息在高信噪比下的收敛情况。

在高信噪比下，根据引理1，$p(x)$ 和 $p(y)$ 的分母为 $1-\mathcal{O}(\frac{1}{\sqrt{\gamma}})$。$p(y|x)$ 的分子为 $f_{\sigma/\sqrt{2}}((x+y)/2) = 1-\mathcal{O}(\exp(-\min^2\cdot\gamma))$，其中 $(x+y)/2 \in]0,1[$，min 是引理1中的 $\min((x+y)/2, 1-(x+y)/2)$。此外，$f_{\sigma/\sqrt{2}}(0) = f_{\sigma/\sqrt{2}}(1) = \frac{1}{2} - \mathcal{O}(\exp(-\gamma))$。要得出这一推论的结果，还需计算 $p(x)$ 的分子、$p(y)$ 的分子以及 $p(y|x)$ 的分母中的积分。定义如下积分

$$I_6 = I_6(x) = I_6(1-x) = \int_0^1 \frac{1}{\sqrt{2\pi\sigma^2}}\, e^{-\frac{(x-u)^2}{2\sigma^2}} \left[Q\left(\tfrac{-u}{\sigma}\right) - Q\left(\tfrac{1-u}{\sigma}\right)\right]\, du, \quad x\in[0,1]. \tag{50}$$

积分 I_6 没有闭式表达式。首先，我们研究 $I_6(x)$ 在 $x=0$ 处的情况（在 $x=1$ 处相同）。

$$\begin{aligned} I_6(0) &= \int_0^1 \frac{1}{\sqrt{2\pi\sigma^2}}\, e^{-\frac{u^2}{2\sigma^2}} \left[1 - Q\left(\tfrac{u}{\sigma}\right) - Q\left(\tfrac{1-u}{\sigma}\right)\right]\, du \\ &= \tfrac{1}{2} - Q\left(\tfrac{1}{\sigma}\right) - \int_0^1 \frac{1}{\sqrt{2\pi\sigma^2}}\, e^{-\frac{u^2}{2\sigma^2}} Q\left(\tfrac{u}{\sigma}\right)\, du - \int_0^1 \frac{1}{\sqrt{2\pi\sigma^2}}\, e^{-\frac{u^2}{2\sigma^2}} Q\left(\tfrac{1-u}{\sigma}\right)\, du \\ &= \tfrac{1}{2} - \mathcal{O}(e^{-\frac{\gamma}{2}}) - \tfrac{1}{8} - \tfrac{1}{2}Q^2\left(\tfrac{1}{\sigma}\right) - \mathcal{O}(e^{-\frac{\gamma}{4}}) \;=\; \tfrac{3}{8} - \mathcal{O}(e^{-\frac{\gamma}{4}}). \end{aligned} \tag{51}$$

其次，我们研究 $I_6(x)$ 在 $x\in]0,1[$ 下的情况。我们使用与引理1和命题2的证明中所使用的类似的微积分工具，得到

$$\begin{aligned} I_6(x) &= Q\left(\tfrac{-x}{\sigma}\right) - Q\left(\tfrac{1-x}{\sigma}\right) - \int_0^1 \frac{1}{\sqrt{2\pi\sigma^2}}\, e^{-\frac{(x-u)^2}{2\sigma^2}} Q\left(\tfrac{u}{\sigma}\right)\, du - \int_0^1 \frac{1}{\sqrt{2\pi\sigma^2}}\, e^{-\frac{(x-u)^2}{2\sigma^2}} Q\left(\tfrac{1-u}{\sigma}\right)\, du \\ &= f_\sigma(x) - \mathcal{O}(e^{-\frac{x^2}{4\sigma^2}}) - \mathcal{O}(e^{-\frac{(1-x)^2}{4\sigma^2}}) \;=\; 1 - \mathcal{O}(e^{-\min^2(x,1-x)\cdot\frac{\gamma}{4}}). \end{aligned} \tag{52}$$

现在，既然所有概率密度的行为都已求解，我们可以在小噪声区间内转换 $I(X;Y)$ 的表达式：

$$p(x) = \frac{I_6(x)}{1-\mathcal{O}(\frac{1}{\sqrt{\gamma}})}, \quad p(y) = \frac{I_6(y)}{1-\mathcal{O}(\frac{1}{\sqrt{\gamma}})}, \quad \text{and} \quad p(y|x) = \frac{e^{-\frac{(y-x)^2}{4\sigma^2}}}{\sqrt{4\pi\sigma^2}} \cdot \frac{f_{\sigma/\sqrt{2}}((x+y)/2)}{I_6(x)}.$$

对于 $x,y\in[0,1]$，我们区分 $I_6(x)$、$I_6(y)$ 和 $f_{\sigma/\sqrt{2}}((x+y)/2)$ 在极值点 0 和 1 附近以及区间内部的行为。因此，我们将区间分解为 $[0,1] = [0,\delta]\cup[\delta,1-\delta]\cup[1-\delta,1]$ 以进行积分。参数 δ 应在高信噪比下趋于 0，并确保 I_6 趋于 1；由此，我们根据 (52) 得出 $\delta^2\gamma$ 应趋于 0，从而得到 $\delta = (\frac{1}{\sqrt{\gamma}})^\alpha$，其中$0<\alpha<1$。最后，通过这一 δ，将 (44) 分解为

$$\begin{aligned} I(X;Y) &= -\int_\delta^{1-\delta} p(y)\log(p(y))\, dy - 2\int_0^\delta p(y)\log(p(y))\, dy \\ &\quad + \iint_{x,y\in[\delta,1-\delta]} p(x)p(y|x)\log(p(y|x)) + \iint_{x,y\notin[\delta,1-\delta]} p(x)p(y|x)\log(p(y|x)) \qquad (53) \\ &= (1+\mathcal{O}(\tfrac{1}{\sqrt{\gamma}}))\cdot\frac{1}{2}\log\left(\frac{\gamma}{4\pi e}\right) \;+\; \mathcal{O}(\delta). \qquad (54) \end{aligned}$$

由于篇幅所限，省略了证明最后一个等式所需的繁琐微积分细节。 ■

在每个光子超过 2 比特时，高斯微分熵 (49) 与上文的 $I(X;Y)$ 非常接近；在超过每个光子 3 比特后，它会变得非常精确，此时在高信噪比下与图 8 中的红色上包络线重合。(49) 中的双重方差 $2\sigma^2$ 最初在 (47) 中得到，它来源于系统模型 (1) 所定义的 Z_1 和 Z_2 的方差叠加。消去 U 后，$\tilde{}$ $\tilde{}$ $\tilde{}$ 模型变为 $Y = X + Z_1 - Z_2$。X 和 Z_1 彼此相关，因此在以 X 为条件时，密度表达式相对复杂。在小噪声区间内，这种相关性会逐渐消失，总加性高斯噪声的方差 $2\sigma^2$ $Z_1 - Z_2$ 占据主导地位，从而使互信息表现如 (49) 所示。在低信噪比和极低信噪比下，应使用定理 3 中的精确密度表达式，并通过数值积分获得 $I(X;Y)$ 的精确值及相应的信噪比界限，前提是用户接受采用相对较低的码率；而在 TE-QKD 中，通常并非如此，因为更倾向于使用高于 $1/2$ 的码率，这使我们处于中等和高信噪比区域。

VII. 密钥协调码

在第 V–VI-B 节对第 III 节所述的时间纠缠量子密钥分发信道模型进行了完整表征之后，我们现在引入纠错码，使误码率性能尽可能接近对应于最大可达速率的信息论极限。

A. 里德-所罗门码

我们考虑著名的里德-所罗门码族，并将其应用于包含 $N = 2^m$ 个分箱的帧，即每个光子 m 个编码比特。为获得足够高的纠错能力，考虑定义在 $\mathbb{F}_q$ 上的 RS 码，其中 q 足够大。每个有限域元素对应 $\log_2(q)/m$ 个光子。为简单起见，假设 $q = 2^{\ell m}$，其中 ℓ 为正整数。该 RS 码的长度为 $n = q - 1$（本原），维数为 $k = n - 2t$，因此目标码率为每个光子 $m \times \frac{k}{n}$ 个信息比特。发送一个该 $\mathcal{C}[n, k, t]_q$ RS 码的码字，需要分别向 Alice 发送总计 $n \times \log_2(q)/m$ 个光子，向 Bob 发送 $n \times \log_2(q)/m$ 个光子，且所有光子均来自有效帧。接收到 $n \times \log_2(q)/m$ 个有效帧后，Alice 将通过量子信道接收到的 $n \times \log_2(q)$ 个比特转换为一个长度为 n 的字，记为 $c + e$，其中 $c \in \mathcal{C}$ 且 $e \in \mathbb{F}_q^n$。类似地，Bob 将其接收到的 $n \times \log_2(q)$ 个比特转换为 $c + e'$，其中 $\hat{e}' \in \mathbb{F}_q^n$。在第 III 节的硬输出信道模型中，$c + e$ 写入输入端 X，而 $c + e'$ 从输出端 $\hat{Y}$ 读出。在公共信道上，Alice 向 Bob 发送伴随式 $s = (c + e)H^t$, $s \in \mathbb{F}_q^{n-k}$,

其中 H 是 $\mathcal{C}$ 的校验矩阵。给定 s 和 $c+e'$ 后，Bob 执行的协调等价于找到 Alice 的字 $c+e$。Bob 按如下步骤进行：

- 计算伴随式 $s' = (c+e')H^t$。
- 将 $s'-s$ 输入代数（Berlekamp-Massey [11]）译码器，以求得 $e'-e$。
- 从 Bob 的字中减去错误 $e'-e$，得到 $c+e'-(e'-e) = c+e$ Alice 所持有的 $\mathbb{F}_q^n$ 字。在通常的特征为 2 的有限域中，将所有减法替换为加法。

里德-所罗门码 $\mathcal{C}[n=63, k=43, t=10]_{q=64}$ 的性能如图 9 所示。传输一个码字总共需要 126 个光子，其中每个域元素携带两个光子。结果显示出显著增益，例如，协调后比特误码率 $P_{eb} = 10^{-5}$ 可获得约 58 分贝的增益。

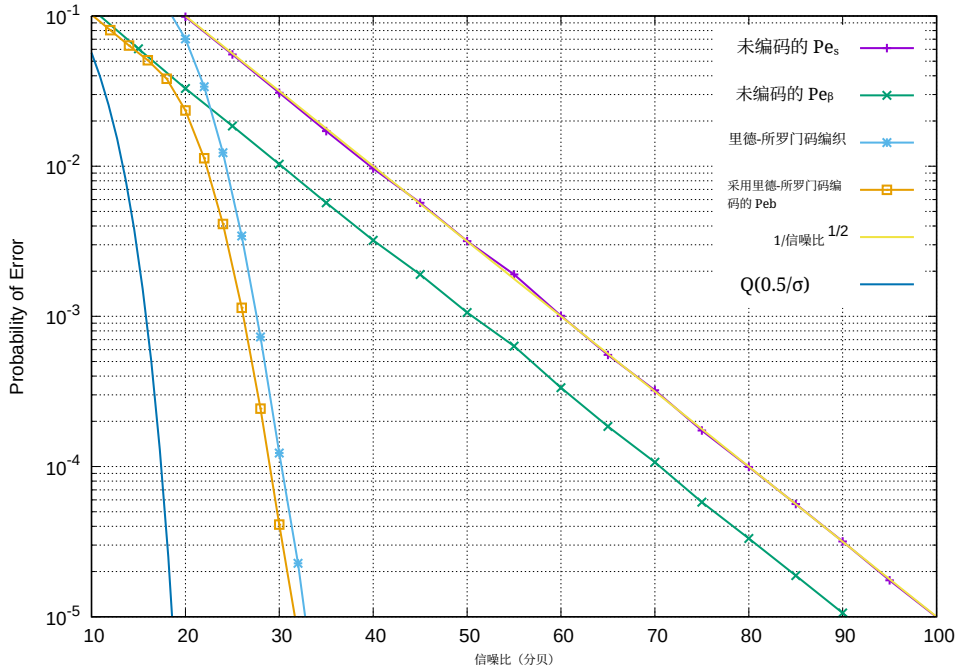


图 9. 在硬输出时间纠缠量子密钥分发信道上，RS 码 $[63, 43, t=10]_{64}$ 的性能；每帧有 $N=8$ 个分箱，每个光子传输 2.05 个信息比特。

由于代数译码器在汉明空间中采用有界距离译码，因此其分析很简单。每当信道在 $\mathbb{F}_q$ 中加入超过 t 个错误时，就会发生译码错误。通过对从 $t+1$ 到 n 个错误的情况求和，可以得到一个简单的并合界。我们按以下步骤为 RS 码建立这个界：

a) TE-QKD 信道上的未编码符号错误概率为 $P_e(\gamma) = \frac{2}{\sqrt{\pi}}(1-\frac{1}{N})\frac{1}{\sqrt{\gamma}}$。b) 对于 RS 码，每个有限域元素的输入错误概率为 $P_{in}(\gamma) = 1-(1-P_e(\gamma))^{\ell}$。

c) 在 $\mathbb{F}_q$ 中，解码后的错误概率上界为

$$P_{eRS}(\gamma) = \sum_{i=t+1}^{n} \frac{i}{n} \binom{n}{i} P_{in}^{i}(\gamma)(1 - P_{in}(\gamma))^{n-i}. \tag{55}$$

d) 解码后的符号（每个光子）错误概率为 $P_{eOut}(\gamma) = 1 - (1 - P_{eRS}(\gamma))^{1/\ell}$。e) 在对分箱进行格雷标记的情况下，Reed–Solomon 解码后的每比特错误概率可由 $P_{ebRS}(\gamma) = {}^{1}\log_2(N) P_{eOut}(\gamma)$ 很好地估算。

由 (55) 得到的错误概率 P_{ebRS} 与蒙特卡罗方法在计算机上可行的范围内完全吻合，即错误率处于区间 $[10^{-7}, 10^{-1}]$ 时。在 $P_{ebRS} = 10^{-10}$ 处，相较于未编码的每比特错误概率，编码增益高达 158 分贝！如此巨大的增益源于时间纠缠量子密钥分发信道的分集阶数。分集阶数定义为 $\lim_{\gamma\to\infty} {}^{-}\log(P_e)\ \log(\gamma)$ [12,第13-14]章。由命题1可知，TE-QKD 的分集阶数为 $_{1\ 2}$，其表现类似于具有半分集阶数的中上衰落信道。纠错码会提高分集阶数，这相当于增大 $P_e(\gamma)$ 的斜率。没有~~衰落的~~加性高斯噪声信道无论是否编码，都具有无限分集阶数，因此所有曲线看起来都相互平行。在存在衰落的情况下，高分集阶数会使信道转变为高斯信道 [13]。在实践中，分集阶数超过 8 时，其与高斯信道上 $e^{-\gamma}$ 的局部斜率几乎无法区分。对于本例，根据 (55) 可推得，代数 Reed–Solomon 解码后的分集阶数为 $(t+1)/2$。时间纠缠量子密钥分发信道上不存在渐近编码。若在更低的错误概率处测量，编码增益会增大。

B. 二进制 BCH 码

TE-QKD 信道不会产生突发错误。错误彼此独立，且解码前最常见的情况是每个光子出现一个错误比特。换言之，里德-所罗门码的二进制突发错误纠正能力并未得到利用。因此，我们建议采用与 $\mathrm{RS}[63, 43]_{64}$，具有相同二进制长度的二进制 BCH 码，即 $63 \times 6 = 378$ 个二进制位。我们从本原长度 511 开始，并逐步缩短至 378。在 $t = 13$ 处，该二进制 BCH 码的维数为 $k = 261$。此 $\mathrm{BCH}[378, 261, t = 13]_2$ 码的分集阶数为 $(t+1)/2 = 7$，优于上一节所示 RS 码的 5.5 阶。对于每帧 $N = 8$ 个分箱，每个光子的信息比特数为 $261/378 \times 3 = 2.07$比特。

在本小节中不添加任何额外图表的情况下，蒙特卡罗模拟和解析界表明，二进制 BCH $[378, 261, t = 13]$ 编码在信噪比上比 $\mathrm{RS}[63, 43]_{64}$ 编码高 3 分贝

比 at $P_{ebRS} = P_{ebBCH} = 10^{-5}$。为获得更低错误概率下的编码增益，我们提出以下非常紧的并合界：

a) 时间纠缠量子密钥分发信道上的未编码符号错误概率为 $P_e(\gamma) = \frac{2}{\sqrt{\pi}}(1 - \frac{1}{N})\frac{1}{\sqrt{\gamma}}$。由于采用格雷标记，下面$10^{-1}$ 个编码比特组成的码块中最多会出现一个比特错误，其中 $m = \log_2(N)$。每个 BCH 码字包含 n/m 个这样的码块，涉及各自独立的二进制错误。

b) BCH解码后 $\mathbb{F}_2$ 的错误概率上界变为 s

$$P_{ebBCH}(\gamma) = \sum_{i=t+1}^{n/m} \frac{i}{n} \binom{n/m}{i} P_e^i(\gamma)(1 - P_e(\gamma))^{n/m-i}. \tag{56}$$

在 $P_{ebRS} = P_{ebBCH} = 10^{-10}$处，二进制 BCH$[378, 261, t = 13]$ 码比里德-所罗门码$[63, 43]_{64}$ 码好 5 分贝。该值对应于 BCH 编码增益为 163 分贝，相对于每帧包含$N = 8$ 个区间的未编码光子而言。请注意，Bob 端对 BCH码（无论是二进制还是非二进制）的协调，与上一节中针对里德-所罗门码所述的协调方式相同：将伴随式 $s' - s$ 输入 Berlekamp-Massey解码器。

C. 基于图的LDPC码

低密度奇偶校验码对基于偏振的QKD系统性能的重大影响，已在 [14] 中针对采用BSC信道模型的离散随机变量协调问题得到展示。低密度奇偶校验码 [15][16] 在码长、码率和解码方法方面都非常灵活。通常，低密度奇偶校验码的校验矩阵是二分Tanner图的邻接矩阵，其中包含 n 个变量节点和 $n-k$ 个校验节点，并假设该图是(d_v, d_c)-正则的。对于满足 $q > 2$的有限域 $\mathbb{F}_q$，邻接矩阵中的非零元素会被替换为来自 $\mathbb{F}_q \setminus \{0\}$的元素。低密度奇偶校验码的标准解码方法是置信传播（BP），即迭代概率解码。为尽量减少符号到比特软值转换期间的损失，可以考虑使用大域 F_q 或大环 $\mathbb{Z}/q\mathbb{Z}$ 的码 [17] 。也可以使用经过优化分箱映射的联合局部-全局LDPC码来获得良好性能 [18] ，或者采用 [19],中的多级编码，尽管这些论文考虑的是不同的量子密钥分发信道模型。本文仅展示采用(3, 9)-正则二进制低密度奇偶校验码时，LDPC码对TE-QKD的影响。码率为 $2/3$ ，当帧包含 8个分箱时，可保证每个光子交换2个比特；不过，我们考虑了一个较短的码长 $n = 384$（64×6），其长度与前几个小节给出的里德-所罗门码和BCH码相当；另外还考虑了码长为$n = 9999$ 的较长码，以展示接近香农极限的性能。

ˆ 符号/分箱的APP由(31)式求得，其中 $APP(i) = APP(X = i)$是分箱编号 i, $i \in \mathbb{Z}_N$的后验概率。随后，通过以下边缘化过程，求得二进制位 b_ℓ的APP，其中 $\ell \in \mathbb{Z}_m$, $m = \log_2(N)$

$$APP(b_\ell) = \sum_{i \in \mathbb{Z}_N \ : \ b_\ell} APP(\hat{X} = i). \tag{57}$$

上述边缘化取决于二进制标记的类型。本文仅讨论每帧 N 个分箱、每个区间采用 $_2(N)$ 位格雷标记的情况。图 10 展示了在 $n = 384$ 位和 $n = 9999$ 位时，二进制低密度奇偶校验码在 TE-QKD 软输出信道上的比特误码率与 γ 的关系。相较于 BCH$[378, 261]$ 码，在比特错误概率为 10^{-5} 时，它们分别获得了 12 分贝和 16 分贝的增益。若与未编码时间纠缠量子密钥分发相比，编码增益分别为 73 分贝和 77 分贝。在长度为 $n = 9999$ 时，该低密度奇偶校验码已达到时间纠缠量子密钥分发硬输出信道的香农极限（$\gamma_{limit} = 12.61$ 分贝），距离软输出 TE-QKD 信道的香农极限（$\gamma_{limit} = 10.45$ 分贝）也仅差 2 分贝。考虑到相较于不编码的情况，总编码增益已达 77 分贝，我们看不出为何还要使用更长的低密度奇偶校验码来争取额外的 1–2 分贝!

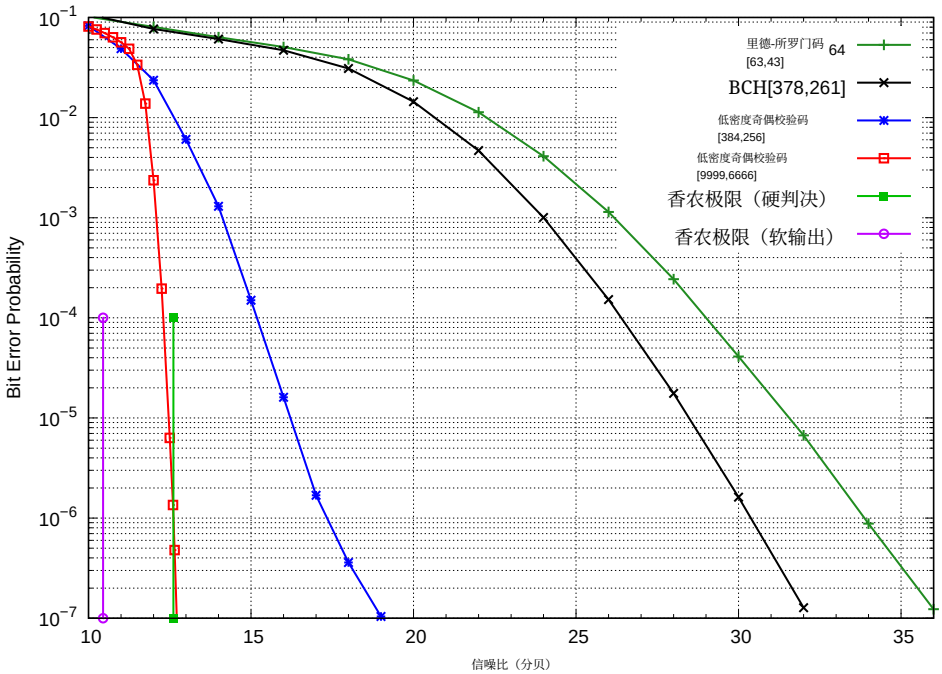


图 10. 在每帧 $N = 8$ 个分箱、每个光子传输 2.0 个信息比特的条件下，(3,9)-正则二进制低密度奇偶校验码在长度为 $n = 384$ 比特和 $n = 9999$ 比特时，于时间纠缠量子密钥分发软输出信道上的性能。

ˆ 实际上，如果实验室系统实现要求得到不含 erfc()/Q() 函数且无需积分的 $APP(X = i)$ 简化表达式，可以假设高斯密度在较小的 σ 处具有狄拉克冲激的效果，并使用 $\propto$ 符号（正比于）来简化式 (31)，因为

分母不依赖于索引 i，因此我们得到：

$$APP(i) \propto \int_0^N \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(y-u)^2}{2\sigma^2}} \cdot \left[Q\left(\frac{i-u}{\sigma}\right) - Q\left(\frac{i+1-u}{\sigma}\right) \right] du$$
$$\propto \left[Q\left(\frac{i-y}{\sigma}\right) - Q\left(\frac{i+1-y}{\sigma}\right) \right].$$

然后，根据参数 $i-y$和 $i+1-y$的符号，我们用 $\frac{1}{2}e^{-\frac{x^2}{2}}$(如果$x \geq 0$)和 $1-\frac{1}{2}e^{-\frac{x^2}{2}}$(如果 $x<0$)近似 $Q(x)$。令 $j=\lfloor Y \rfloor$为 Bob 一侧的 Y的区间位置，即 $Y \in [j, j+1[$。简化后的 APP 表达式为：

$$\text{If } i=j, \quad APP(i) \propto \left[1 - \tfrac{1}{2}e^{-\frac{(y-i)^2}{2\sigma^2}} - \tfrac{1}{2}e^{-\frac{(y-i-1)^2}{2\sigma^2}} \right], \tag{58}$$

$$\text{If } i \neq j, \quad APP(i) \propto sign(j-i) \cdot \left[\tfrac{1}{2}e^{-\frac{(y-i-1)^2}{2\sigma^2}} - \tfrac{1}{2}e^{-\frac{(y-i)^2}{2\sigma^2}} \right]. \tag{59}$$

在 TE-QKD 软输出信道上使用二进制低密度奇偶校验码的 BP 译码器时，采用式 (58)–(59) 相对于精确表达式 (31) 的损失仅为 0.25–0.30 分贝。对于超过 50 分贝的编码增益而言，这一损失微不足道。

请注意，我们没有展示低密度奇偶校验码在硬输出信道上的性能。事实上，无论信道输出是否为软输出，最优置信传播译码都相同，也就是说，在类高斯信道和类二元对称信道上使用的是同一个 BP 译码器。在比特错误率为10^{-5}时，硬输出与软输出之间的差距，对于 LDPC$[384, 256]$ 为约 8.5 分贝，对于 LDPC$[9999, 6666]$ 为约 4 分贝。假设系统实现具备最优 BP 译码器，但无法获得精确的光子位置，只能获得分箱编号。在这种情况下，实验室实现只能在硬输出信道上使用 LDPC 码，二进制数字APP表达式 (57) 变为

$$APP(b_\ell) \propto \sum_{i \in \mathbb{Z}_N \,:\, b_\ell} \hat{\pi}_i \times p_{i,j}, \tag{60}$$

其中，$j=\lfloor Y \rfloor$，$\hat{}\pi_i$ 在 σ 较小时由 (22) 或 (37)-(38) 给出，而 $p_{i,\,j}$ 在 σ 较小时由 (30) 或 (35)-(36) 给出。编码理论研究者和从业者还可以使用短码长或中等码长的卷积码、Turbo码、极化码以及其他二进制或非二进制代数码，在 TE-QKD 信道上实现较大的编码增益。

D. 不同帧长下容量极限的总结

我们通过一张表格总结时间纠缠量子密钥分发信道在硬输出和软输出条件下的重要信息论极限，以此完成本节。以信噪比表示的香农极限是

表 II 共包含七列，参数涵盖每帧 8 个分箱至每帧 64 个分箱。最后两行对应 BCH 码和低密度奇偶校验码在第 VII-B 和 VII-C 小节中所述的信噪比和标准差数值。

表 II TE-QKD 的信息论（香农）极限。

N 每帧分箱数	Bits 每个光子	$R = k/n$ 码率	信噪比极限 hard	σ/N hard	信噪比极限 软软	σ/N
8	2.0	2/3	12.61 分贝	0.029269	10.45 分贝	0.037533
16	3.0	3/4	13.29 分贝	0.013532	10.85 分贝	0.017922
32	3.0	3/5	3.88 分贝	0.019992	3.46 分贝	0.020982
32	4.0	4/5	13.61 分贝	0.0065215	11.04 分贝	0.0087670
64	4.0	2/3	4.01 分贝	0.0098474	3.58 分贝	0.010347
64	5.0	5/6	13.77 分贝	0.0032012	11.13 分贝	0.0043383
8 BCH, n=378	2.0	2/3	28.49 分贝 $P_{eb} = 10^{-5}$	0.0047034 已达到		
8 LDPC, n=9999	2.0	2/3			12.47 分贝 $P_{eb} = 10^{-5}$	0.029745 已达到

表 II 中列出的软判决译码信噪比限值似乎接近两个数值：一个信噪比约为 10–11 分贝，另一个较低的信噪比约为 3.5 分贝。硬判决译码限值高于软判决译码限值，因为 $I(X;Y) \le I(X;Y)$，差距取决于帧长和码率。当然，在较低码率（低于 $1/2$）时，硬判决与软判决之间的差距会消失；而在较高码率下，随着互信息接近渐近线 $\log_2(N)$，这一差距会增大。

软判决译码信噪比限值的两个典型值可通过式 (49) 针对较小的 σ 加以解释或说明：

$$\frac{1}{2}\log\left(\frac{\overline{\gamma}}{4\pi e}\right) = \log_2(N) - b, \tag{61}$$

其中 $\overline{\gamma} = N^2\gamma$ 和 b 是回退值。这里，表 II 中的 $b = 1$ 位或 $b = 2$ 位。然后，求解 (61) 得到 $\gamma = (4\pi e)/2^{2b}$。对于 $b = 1$，我们得到 $\gamma = 9.31$ 分贝；对于 $b = 2$，则得到 $\gamma = 3.29$。与表 II 第 6 列中的 $\hat{}$ 值相比，差异是因为 $I(X;Y)$逐渐偏离包络线 $I(X;Y)$，转而遵循自身的渐近线。我们希望，表 II 中给出的信噪比界限能对量子密钥分发领域的物理学家和编码理论研究者有所帮助。

VIII. 结论

我们研究了光子到达探测器受到时间抖动影响时，基于时间纠缠的量子密钥分发。我们对秘密密钥信息率进行了严格分析，并提出和测试了几种用于信息协调的码，以逼近最大密钥率。这些可实现的秘密密钥率远高于基于偏振纠缠的量子密钥分发所能达到的最高值。然而，实际的光子探测器还会受到其他因素的影响，例如暗电流和停机时间，这可能导致速率进一步下降。这些影响应作为未来研究的课题。

参考文献

[1] E. Diamanti、H.-K. Lo、B. Qi 和 Z. Yuan，《量子密钥分发中的实际挑战》，npj Quantum Information，第2卷，2016年11月。[2] R. Nandal、A. Nandal、K. Joshi 和 A. Rathee，《若干最具代表性的量子密钥分发协议的调查与比较》，SSRN Electronic Journal，2021年1月。[3] C. Lee、D. Bunandar、Z. Zhang、G. R. Steinbrecher、P. B. Dixon、F. N. C. Wong、J. H. Shapiro、S. A. Hamilton 和 D. Englund，《大字母表量子密钥分发的高速率现场演示》，2016年。[4] M. C. Sarihan、K.-C. Chang、X. Cheng、Y. S. Lee、T. Zhong、H. Zhou、Z. Zhang、F. N. Wong、J. H. Shapiro 和 C. W. Wong，《通过能量-时间纠缠和双光子频率梳实现高维量子密钥分发》，载于激光与电光学会议，第FTh1A.3页，美国光学学会，2019年。[5] D. B. IV、C. Cheng 和 E. Soljanin，《基于时间纠缠的量子密钥分发中非理想光子探测器的信息速率》，IEEE Trans. Commun.，已投稿，arXiv预印本 arXiv:2207.04146，2022年7月。[6] A. E. Gamal 和 Y. Kim，《网络信息论》，剑桥大学出版社，2011年。[7] T. Zhong、H. Zhou、R. D. Horansky、C. Lee、V. B. Verma、A. E. Lita、A. Restelli、J. C. Bienfang、R. P. Mirin、T. Gerrits、S. W. Nam、F. Marsili、M. D. Shaw、Z. Zhang、L. Wang、D. Englund、G. W. Wornell、J. H. Shapiro 和 F. N. C. Wong，《利用高维编码和时间-能量纠缠实现高光子效率量子密钥分发》，NEW JOURNAL OF PHYSICS，2015年。[8] H. Zhou 和 G. W. Wornell，《用于高维量子密钥分发的自适应脉冲位置调制》，载于《2013年IEEE国际信息论研讨会论文集》，土耳其伊斯坦布尔，2013年7月7日至12日，第359–363页，2013年。[9] E. Karimi、E. Soljanin 和 P. Whiting，《提高基于能量-时间纠缠的量子密钥分发中的原始密钥速率》，载于第54届阿西洛马会议：信号、系统与计算机，ACSCC 2020，美国加利福尼亚州太平洋丛林，2020年11月1日至4日，第433–438页，2020年。[10] T. M. Cover 和 J. A. Thomas，《信息论基础》，John Wiley & Sons，2006年。[11] R. E. Blahut，《用于数据传输的代数码》，剑桥大学出版社，2003年。[12] J. G. Proakis 和 M. Salehi，《数字通信》，美国：McGraw-Hill，第5版，2008年。[13] J. J. Boutros 和 E. Viterbo，《信号空间分集：一种功率和带宽高效的瑞利衰落信道分集技术》，IEEE Trans. on Information Theory，第42卷，第502–518页，1998年7月。[14] D. Elkouss、A. Leverrier、R. Alléaume 和 J. J. Boutros，《离散变量量子密钥分发的高效协调协议》，IEEE 信息论研讨会，ISIT 2009，韩国首尔，2009年6月。[15] R. G. Gallager，《低密度奇偶校验码》，美国马萨诸塞州剑桥：MIT出版社，1963年。[16] T. Richardson 和 R. Urbanke，《现代编码理论》，剑桥大学出版社，2008年。

[17] J. J. Boutros、U. Erez、J. V. Wonterghem、G. I. Shamir 和 G. Zémor，《几何整形：类高斯星座的低密度编码》，IEEE 信息论研讨会，ITW 2018，中国广州，2018年11月。[18] S. Yang、M. C. Sarihan、K. Chang、C. W. Wong 和 L. Dolecek，《能量-时间纠缠量子密钥分发的高效信息协调》，载于第53届阿西洛马会议：信号、系统与计算机，ACSCC 2019，美国加利福尼亚州太平洋丛林，第1364–1368页，2019年11月。[19] H. Zhou、L. Wang 和 G. W.Wornell，《大字母表密钥分发的分层方案》，载于2013年信息论与应用研讨会，ITA 2013，美国加利福尼亚州圣迭戈，第1–10页，2013年2月。