基于时间纠缠光子的量子密钥分发及其密钥率前景

Lara Dolecek[1] 和 Emina Soljanin[2]

[1]加利福尼亚大学洛杉矶分校电子与计算机工程系，电子邮件：dolecek@ee.ucla.edu[2]罗格斯大学电子与计算机工程系，电子邮件：emina.soljanin@rutgers.edu

arXiv:2303.01973v1 [cs.IT] 3 Mar 2023

摘要——**为了实现安全的实用系统，量子密钥分发（量子密钥分发）必须能够在长距离传输中提供高密钥率。与其他量子密钥分发实现方案相比，基于时间纠缠的量子密钥分发有望提高密钥率并延长密钥分发距离。本文介绍量子密钥分发协议的主要步骤，重点关注基于高维时间箱纠缠光子的新兴量子密钥分发技术。我们从信息论与编码理论的角度概述该领域的最新进展。具体而言，我们讨论单光子探测器缺陷导致的密钥率损失。我们希望本文提出并讨论的开放问题能激励信息论与编码理论研究者参与其中，为初露头角的量子应用作出贡献并产生影响，同时推动未来量子通信系统的发展。**

一、引言

正如香农在其富有远见的著作中所预见的，安全性对于通信系统而言与可靠性同等重要。香农不仅凭借其 1948 年发表的开创性著作《通信的数学理论》开启了信息论这一领域，还几乎同时（于 1949 年）发表了另一篇颇具影响力的文章，探讨信息安全问题 [1]。在这篇开创性著作中，香农证明，一次一密加密方案（至少自 19 世纪末以来便已为人所知）在信息论意义上是安全的。它实现了完美保密性，即密文的后验分布与原文的先验分布完全相同。

快进数十年的数字革-命，香农最初的思想依然具有现实意义，一如既往。如今，我们正站在数据通信下一前沿的门槛上，其标志是量子技术。量子技术有望提供前所未有的数据安全和处理能力，而这在过去使用经典系统时是不可想象的。近年来，全球不仅对量子通信网络产生了浓厚兴趣并进行了投资，而且早期的实施应用在未来还将不断拓展 [2]。未来可以说属于量子，我们正迎来这个激动人心的新时代的曙光。

量子通信系统的一个关键组成部分是量子密钥分发（QKD）。为了广泛采用量子密钥分发并构建真正安全的量子网络，必须在长距离传输中实现高密钥率。本文认为，通过信息论与编码理论以及量子物理等互补领域的协同创新，基于纠缠光子的量子密钥分发有望应对这一挑战。

目前最先进的基于光纤的量子密钥分发实现，大多已达到 Mbits/s 级别[3], ，有些甚至达到 Gbps/s 级别 [4],，传输距离可达 400 km。尽管这些结果令人鼓舞，但在广域网络中扩展到端到端实现时，由于损耗和噪声等各种棘手的实现问题，实际密钥率会大幅下降 [3]。无法充分利用携带信息的光子，也无法以低延迟实现这一点，已成为实践中的瓶颈 [5]。

如今的量子密钥分发协议在“光子匮乏”的条件下运行 [5]。尽管人们持续努力，试图通过更明亮的

光源和更快的探测器来改善这些条件，但对于传统的离散变量协议而言，光子通过信道传递的信息仍不足一个比特。高维时间纠缠是一种有望打破这一瓶颈的策略。

基于时间纠缠光子的量子密钥分发方案从光子到达时间中提取密钥比特。时间-bin纠缠可追溯至二进制编码方案，这类方案只区分早到和晚到的光子。此类信息每个光子最多提供一个密钥比特。在实际系统中，由于噪声和保密性方面的考量，密钥率要低得多。与二进制方案相比，高维时间箱协议有望通过更精确地测量光子到达时间来提高光子利用率[6]。然而，实际光子探测器存在光子探测时间抖动、探测器停机时间和暗电流噪声。

人们已认识到各种探测器缺陷对量子密钥分发协议的不利影响。一篇近期综述论文 [7] 深入研究了在制备与测量协议（如 BB84）背景下，使用实际器件实现安全量子密钥分发的问题。文献 [8]–[10]讨论了采用存在定时抖动、停机时间和暗计数的探测器时，基于时间纠缠的量子密钥分发的密钥率。

这篇简短的综述性杂志文章讨论范围有限。为提供更广泛、更深入且严谨的论述，本文始终在相关部分引导读者参阅具体的技术论文及其中的参考文献。第II 节介绍量子密钥分发协议的两个基本步骤：通过量子信道生成原始密钥，以及通过经典信道进行信息协调。第III 节重点介绍采用时间分箱进行原始密钥生成的时间纠缠量子密钥分发协议，并讨论非理想光子探测器导致的速率损失。

在第IV节中，我们首先说明，单向信息协调可以自然地表述为一个带旁信息的信源编码问题，为此必须开发前向纠错（FEC）方案。随后，我们将在该节中简要综述信息协调中前向纠错领域的已知成果。

接下来，在第V节中，我们将介绍多维时间箱量子密钥分发目前面临的挑战及取得的进展，重点讨论现有的前向纠错和调制方案。

文章最后讨论了一些开放问题，这些问题对（经典）信息与编码理论学者以及量子通信从业者颇具意义，相关内容见第VI节。本文并不试图涵盖基于量子密钥分发的系统的所有方面；感兴趣的读者可参阅相关综述，例如 [3]。

II. 量子密钥分发协议

量子密钥分发指双方（通常称为Alice和Bob）通过量子信道和经典信道进行通信，从而建立密钥的协议；窃听者Eve可以访问这两个信道，如图1所示。协议结束时，Alice和Bob拥有仅他们知晓的相同均匀随机序列，否则便会中止协议。如下文所述，量子密钥分发协议需要通过量子信道和经典信道进行通信。

概括来说，量子密钥分发主要分为两个步骤。在第一步中，Alice 和 Bob 通过量子信道生成原始密钥 比特，这对于防止未被察觉的窃听至关重要。第一步结束时，由于系统中的噪声，Alice 和 Bob 各自的原始密钥在某些位置上可能不一致，部分信息可能已被 Eve 获知，而且可能并非均匀随机。

在第二步中，Alice 和 Bob 对原始密钥进行处理，以建立共享的密钥。他们通过公开的经典信道进行通信，以协调双方原始密钥之间的差异，针对 Eve 掌握的信息增强密钥的隐私性，并压缩各自的序列，从而实现均匀随机性。最终，他们得到一个私密且难以猜测的密钥。经典后处理的目标是尽可能增加密钥中保留下来的比特数。

本文聚焦于基于时间纠缠光子的量子密钥分发协议。在基于纠缠的协议中，Alice、Bob 或

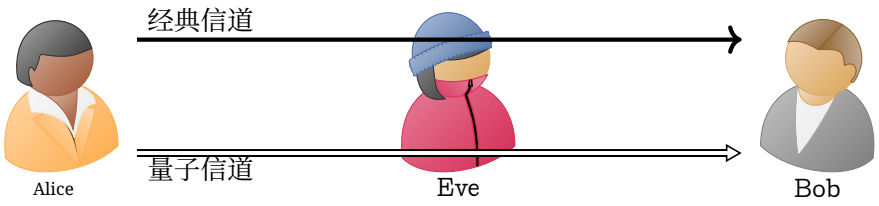

图 1. 量子密钥分发：Alice 和 Bob 通过量子信道和经典信道通信，从而建立密钥。Eve 可以访问这两个信道。

某个第三方分发纠缠光子对，使 Alice 和 Bob 各自获得每对纠缠光子中的一个光子。最初的协议由 Ekert 于 1991年提出，称为 E91量子密钥分发 [11]。假设 Alice 和 Bob 共享一组 m 处于以下状态的纠缠量子比特对

$$|\varphi\rangle = |00\rangle + |11\rangle)/\sqrt{2}, \qquad (1)$$

且 Eve 不在场。如果他们分别在计算基中测量各自的状态，就会得到相同的 m 均匀随机比特序列，每对光子对应一个比特。因此，该方案受益于共享纠缠的两个特性：随机性和相关性。

将两个光子的偏振纠缠起来，会产生一个（1）中的双量子比特态。在这类方案中，每对纠缠光子对密钥的贡献至多为一比特。将光子在时间上纠缠，有望使每个光子承载更多比特，从而提高光子利用率。

III. 时间纠缠量子密钥分发

接下来我们将介绍时间纠缠量子密钥分发方案，以及在保持其光子利用率优势方面所面临的挑战。有关更多详细信息，请参阅 [8] 。

A. 生成原始密钥比特

在常见的基于时间纠缠的量子密钥分发方案中，独立光源（或其中一位参与者）通过自发参量下转换（SPDC）随机产生纠缠光子对，如图 2 所示。当我们用激光泵浦照射非线性晶体时，可能发生自发参量下转换，从而产生两个新的纠缠光子。光子的发射在整个时间窗口内均匀

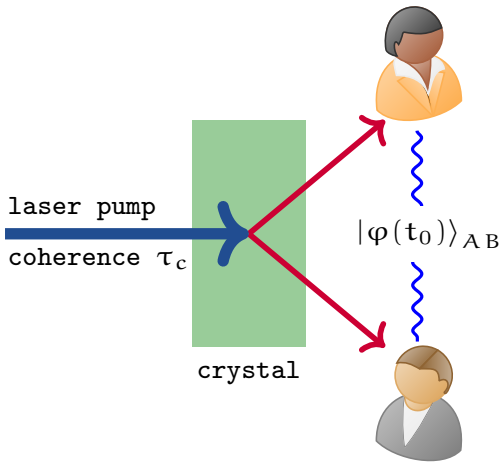

图2. 在状态 $|\varphi(t_0)\rangle_{AB} \propto \int_{t_0-\tau_c}^{t_0} dt\ |t\rangle_A |t\rangle_B$ 下生成时间纠缠光子对。理想情况下，Alice 和 Bob 会在区间 $[t_0, t_0-\tau_c,$ 内的相同且均匀随机的时间接收到各自的光子，但当他们使用实际的不完美探测器时，情况并非如此。

发生，该时间窗口等于泵浦相干时间 τ_c，且与先前的发射无关。因此，纠缠双光子态表示为

$$|\varphi(t_0)\rangle_{AB} \propto \int_{t_0-\tau_c}^{t_0} dt\ |t\rangle_A |t\rangle_B ,$$

其中一个光子发送给 Alice，另一个发送给 Bob。

纠缠光子的代际间隔时间相互独立且服从相同的指数分布，从而产生完美随机性。Alice 和 Bob 通过时间分箱，从纠缠光子的到达时间中提取原始密钥比特。双方分别将各自的时间轴离散为时间箱 ，并将其分组为时间帧。他们将光子到达记录为帧内被占用的时间箱。随后，他们使用

光子时间箱在时间帧内的位置来生成随机比特。比特提取遵循脉冲位置调制（PPM），最早在 [12]中得到研究。在理想条件下，光子到达时间间隔（即其代际间隔时间）相互独立且服从相同的指数分布。多个研究小组对这类系统进行了研究，其中最著名的是 [13]，他们构建了一个端到端的高维时间纠缠实验。

在脉冲位置调制（PPM）中，Alice 和 Bob 同步时钟，并将时间轴划分为固定的时间帧，每帧包含 n 个时间箱。在 PPM 中，Alice 和 Bob 约定只保留恰好有一个时间箱被占用的时间帧，并丢弃所有其他帧。因此，PPM 解码从每个保留帧中最多可提取的原始密钥比特数为 $\log_2 n$。图 3 展示了一个包含八个时间箱的帧，并标示了探测缺陷，我们将在后文讨论这些缺陷。如果 Alice

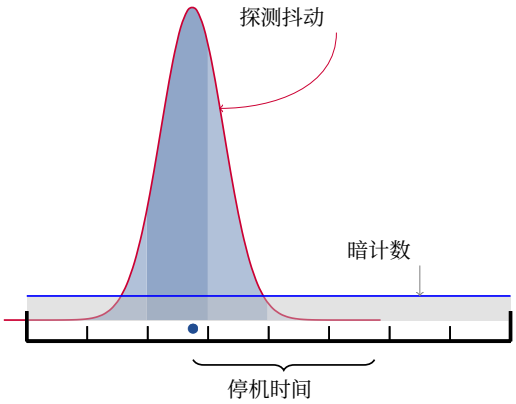

图 3. 一个包含八个时间箱且仅有一个时间箱被占用的帧。每个时间箱由三比特标识。探测器缺陷包括抖动、停机时间和暗计数。高斯曲线示意了探测器抖动的概率密度函数。多个时间箱都可能受到影响，每个时间箱受到影响的可能性与其上方曲线下的面积成正比。暗计数在整个帧内均匀发生，此处用均匀分布表示。

Alice 和 Bob 增加每帧的时间箱数量n，就能获得更多原始密钥比特。不过，由于探测缺陷，他们的密钥可能会有更多差异。

B. 示例说明

图 4给出了 Alice 和 Bob 所持二进制序列的示例，展示了他们如何达成一致，以及他们可能出现的差异。我们假设 Alice 和 Bob 已分别将时间轴离散化为帧，并将每帧划分为四个大小相同的时间箱。每帧有四个时间箱，因此，只要该帧中只有一个时间箱被占用，这个时间箱就能贡献两比特信息。没有时间箱被占用或有多个时间箱被占用的帧都会被丢弃；前者是由光子损耗造成的，后者则是由暗计数造成的。

在此示例中，我们展示四个具有代表性的帧。将每帧中的四个时间箱按从左到右的顺序排列，并依次赋予比特对 ’00’、’01’、’10’ 和 ’11’。

- 在最左侧的帧中，Alice 和 Bob 都将结果映射为 ’00’（两人的最左侧时间箱均被占用）。尽管存在轻微的到达抖动，比特提取仍然成功。
- 在第二帧中，Alice 检测到两次到达事件，其中一次是由暗计数造成的伪事件。虽然 Bob 最初可以将第二帧的结果映射为 ’01’，但在收到 Alice 告知该帧无效的信息后，他也将其丢弃。
- 在第三帧中，Alice 和 Bob 都观测到一次到达事件。然而，由于定时抖动，这两次到达事件落入了相邻时间箱。Alice 将结果映射为 ’01’，而 Bob 将结果映射为 ’10’，因此产生了 2 比特的差异。
- 在最右侧的帧中，Alice 和 Bob 又各自检测到一次到达事件。在此示例中，两次到达事件均由暗计数造成，彼此不相关（此时 Alice 和 Bob 并不知情）。Alice 将结果映射为 ’01’，而 Bob 将结果映射为 ’11’。

如示例所示，定时抖动、光子损耗和暗计数对最终密钥率的影响取决于分箱宽度和帧的大小。

C. 探测器缺陷

最常见的单光子探测器是超导纳米线单光子

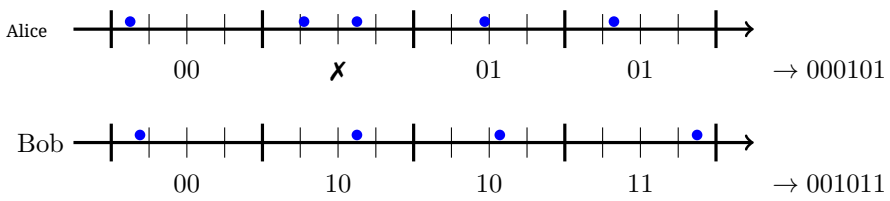

图4. Alice（A）和 Bob（B）的到达序列示例。右侧的二进制序列是双方提交用于信息协调的序列。

探测器（超导纳米线单光子探测器）。实际探测器会受到抖动、暗计数和停机时间的影响。

抖动误差源于时间标记不精确，导致 Alice 和 Bob 的原始密钥出现差异。原始密钥差异会增加 Alice 和 Bob 为密钥协调而进行的公开信息交换量，从而降低密钥率。探测器停机时间是指光子探测后无法进行其他探测的这段时间。在他们的实验中，Zhong 等人 [13] 使用 50:50 分束器，将光子到达事件分配到每个站点的两个探测器，以克服停机时间造成的光子损失。然而，探测器停机时间会导致探测遗漏，进而在系统中引入记忆，改变观测到的到达事件，使其不再相互独立。仅这种依赖性就会降低密钥率。暗计数是指并非来自纠缠光子源的光子，主要由漏光进入探测器的光线路所致。暗计数均匀且独立地到达任一探测器。由于它们与自发参量下转换光子无法区分，如果暗计数占探测光子的比例过大，就可能导致显著误差。

我们对这些误差进行如下数学建模；另请参见图 3。令 U 为描述纠缠光子到达时间的随机变量。理想情况下，U 在区间 $[t_0 - \tau_c, t_0]$上均匀分布，其中时间点 t_0可任意选取，并且 τ_c是我们所说的泵浦相干时间。然而，探测器停机时间会引入记忆效应，使 U 不再均匀分布。由于探测器抖动，Alice 的探测器记录到达事件的时间可用随机变量 T_A建模，而 Bob 的探测器记录到达事件的时间可用随机变量 T_B 建模，其中

$$T_A = U + \eta_A \text{ and } T_B = U + \eta_B. \quad (2)$$

这里，η_A 和 η_B 是均值为零的独立高斯随机变量。

在时间分箱密钥提取中，Alice 和 Bob 会观测到离散相关随机变量，用以标识帧内被占用的时间箱。当每帧的时间箱数量为 n 时，Alice 观测到 X_n，Bob 观测到 Y_n，其定义如下：

$$X_n = U_n + J_{A,n} \text{ and } Y_n = U_n + J_{B,n} \quad (3)$$

其中，U_n 在 $\{0, 1, \ldots, n-1\}$ 上服从均匀分布，而 $J_{A,\,n}$ 和 $J_{B,\,n}$ 的取值为整数，可取值 k、$0 \le k \le n-1$，其概率取决于噪声统计特性和时间箱大小。

D. 窃听模型

由于量子信道上不可能发生被动窃听，Alice 和 Bob 总能检测到截获重发攻击：Eve 测量 Alice 的量子态（光子），然后向 Bob 发送以她测得的状态制备的替代态。他们通常会让一部分光子通过特殊干涉仪，从而产生处于最大纠缠态 $|\varphi_{AB}\rangle \propto |0_A 0_B\rangle + |1_A 1_B\rangle$的纠缠光子。Alice 和 Bob 可以通过进行 CHSH 博弈的一种变体，量化 Eve 基于这类光子所获得的信息增益。我们假设，如果检测到窃听者导致的结果超出 CHSH 博弈的非经典界限，他们就会停止密钥分发。因此，Alice 和 Bob 获得的原始密钥可确保免受量子信道上的窃听。实验系统

实现这类量子密钥分发协议的系统近期已被证明，光子信息效率最高可达每光子 4.082 个安全密钥比特，安全密钥率最高可达 237 kbit/s，从而能够抵御集体攻击 [14]。

截获重发攻击是可能攻击中最简单的一种，而这类攻击超出了这篇科普杂志文章的讨论范围。相反，我们将关注 Eve 在接下来描述的协调阶段，仅通过观察公共信道上的通信所获取的信息。

E. 密钥率

密钥率是“在使 Eve 获取信息的速率任意小的同时，Alice 和 Bob 能够达成密钥的最大速率”，[15]。对于基于时间纠缠的量子密钥分发，Alice 和 Bob 根据测量结果获得相关比特流（原始密钥），如第III-B节所示。然而，他们必须进行通信以达成密钥，也就是说，协调彼此的差异。此过程中所需的所有通信都必须视为公开的，因此常用的级联协议 [16] 效率低下；另见第II节。

这里，我们考虑单向信息协调方案：Alice 将有关其序列的信息发送给 Bob，后者据此修正自己与 Alice 的原始密钥之间的差异，如图5所示。



图5. Alice 通过公共信道向 Bob 发送比特。Bob 使用这些比特将自己的原始密钥与 Alice 的原始密钥进行协调。

经过单向信息协调（将在下一节讨论）后，Alice 和 Bob 共享 Alice 最初的原始密钥。然而，由于他们通过公共信道进行通信，共享密钥并不保密。为了解决这一问题，Alice 和 Bob 执行隐私放大。他们压缩共享密钥，从而确保密钥的保密性，但也使密钥变短。

F. 非理想探测器导致的速率损失

1) 探测器抖动导致的速率损失：当分箱方案的时间箱数量等于 n 时，其保密容量为 $I(X_n;Y_n)$，其中 X_n 和 Y_n 由 (3) 给出。我们称 $I(X,Y) = \lim_{n\to\infty} I(X_n;Y_n)$ 为最终可实现的密钥率（参见例如 [17, 第 567] 页）。

我们考虑以下示例。假设 Alice 的探测器没有噪声，并在时间箱起始处探测到光子。Bob 的光子到达时间（相对于 Alice 的光子）在时间Δ内均匀分布。将持续时间为 T_f 的一帧划分为 n 个时间箱时，每个时间箱的大小为 T_f/n。在这些假设下，我们看到，如果 $n \le T_f/\Delta$（或等价地 $\Delta \le T_f/n$），Alice 和 Bob 的原始密钥比特完全相同，因此密钥率为

$$I(X_n;Y_n) = \log n.$$

另一方面，当 $n > T_f/\Delta$ 时，我们有

$$\begin{aligned} I(X_n;Y_n) &= H(X_n) - H(X_n|Y_n) \\ &= \log n - \log \Delta/(T_f/n) = \log \frac{\Delta}{T_f}. \end{aligned}$$

因此，增加 n 会提高密钥率，但前提是 $n \le T_f/\Delta$。

2) 探测器停机时间导致的速率损失：非零的停机时间不会引入错误，而是会使 Alice 和 Bob 的原始密钥比特产生记忆。因此，Alice 和 Bob 必须压缩协调后的原始密钥，以获得均匀随机性。压缩率取决于探测器停机时间、光子产生率以及每帧的时间箱数。

为描述探测器停机时间对系统的影响，我们必须用马尔可夫链（MC）对探测器与时间分箱操作的组合进行建模。系统的 MC 的熵率决定了保证密钥具有均匀随机性的最低压缩率。图6展示了一个简单示例。这些 MC 可能会变得非常复杂

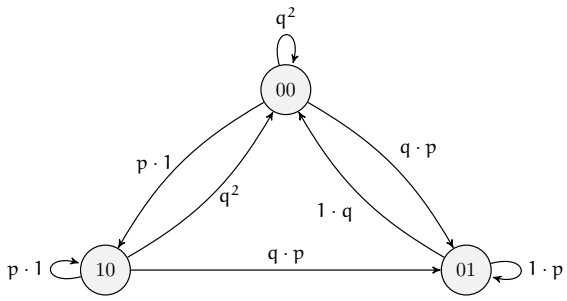

图 6. 用马尔可夫链对具有双时隙帧（链的状态）且探测器停机时间为一个时间箱的系统进行建模。一个时间箱内发生光子到达的概率分别为 p 和 $q = 1 - p$。由于停机时间的存在，不会有任何一帧包含两个被占用的时间箱。



图 7. 原则上，抛掷多面硬币的系统每次抛掷可提供超过一比特的信息。然而，如果二十面体抛掷系统中的噪声使我们只能区分个位数和两位数，那么该系统的表现就如同抛硬币系统。

随着系统参数的变化。文中介绍了一种可针对不同参数值生成这些 MC 的算法，并在 [8] 中实现为一个在线工具，可通过以下网址访问：https://cc1539.github.io/qkd-binning-demo-2。

G. 时间纠缠速率优势

时间纠缠量子密钥分发有望实现每个光子提供超过一比特的信息，而偏振纠缠量子密钥分发中，每对纠缠光子对至多为密钥贡献一比特。为了结合系统描述来考察这一优势，不妨考虑抛掷（多面）硬币，如图7所示。

我们通过偏振纠缠所能获得的最大密钥率对应于公平抛硬币实验中的信息率，即一个比特。采用时间纠缠的脉冲位置调制后，我们的硬币变成了多面体，其面数等于 n，即帧中的时间箱数量。因此，例如，使用四面体硬币时，原始密钥比特数为log4，而使用八面体硬币时则为log8。然而，增加硬币的面数也会放大系统缺陷的影响。例如，如果 Alice 抛掷八面体硬币得到四（即测得她的光子在八时间箱帧中的到达时间），Bob 由于探测器抖动，可能在自己这边得到四、三或五。在抛硬币的类比中，探测器停机时间会使我们无法在观测到较大的数值后观测到较小的数值。

对于给定的脉冲位置调制帧时长（通常由泵浦相干时间决定）以及探测器噪声参数（抖动方差和停机时间），$I(X_n; Y_n)$ 可通过选择每帧的时间箱数量来最大化n；更多详情见 [8] 。原则上，通过基于适当纠错编码的协调方案可以实现任意速率 $I(X_n; Y_n)$，我们将在接下来的章节中讨论这些方案。

若要进一步提高光子利用率，就需要更好的设备（纠缠光子源和单光子探测器）[18]。为提高光子利用率，人们提出了自适应脉冲位置调制方案，见 [19] 及其中的参考文献。

IV. 用于量子密钥分发的前向纠错

A. 信息论视角

由于 Alice 和 Bob 从相关随机变量中提取密钥，单向信息协调相当于 Slepian-Wolf 编码，这是一个经过深入研究的、带有旁信息的信源编码问题。其一般原理如下：Alice 记录自己的比特序列，并将该序列的伴随式发送给 Bob。伴随式根据所选码的奇偶校验计算得出，并通过公共经典信道传输。Bob 使用自己的比特序列以及从 Alice 收到的伴随式来

解码（协调）Alice 的序列。在图5中，协调比特正是由 Alice 端所选码生成的伴随式比特。

主要挑战在于以数学方式构建高性能、实用的纠错方案，使其兼容能够生成携带信息的光子的实际物理系统，同时最大限度地减少向 Eve 泄露的信息。要使这类编码方案在实践中取得成功，它们需要高性能且快速的译码算法。

第 II 节所述的时间纠缠量子密钥分发代表了一种多维（多比特）离散变量（DV）量子密钥分发实例，因为信息由离散时间箱中的一个箱的索引表示。Alice 也可以调制相干态，而 Bob 则测量电磁光场的振幅和相位正交分量。这种设置称为连续变量（CV）量子密钥分发。由于前向纠错方面的研究成果对于二进制离散变量量子密钥分发而言可以说是最为成熟的，并且这些成果为高维时间纠缠量子密钥分发中的前向纠错研究提供了必要背景，因此我们将在下一小节讨论相关文献。

B. 典型离散变量量子密钥分发模型的前向纠错

前向纠错方法已成功应用于许多数据传输和存储应用。基于图的码（例如低密度奇偶校验码（LDPC））是其中最常用的方法之一。LDPC 编码同样是量子密钥分发信息协调中的主要数学技术，可用于克服不完美探测器和传输噪声的影响。

对于二进制离散变量量子密钥分发，早期研究最初受到将信息编码到光子的偏振或相位上的启发。开创性研究 [20] 敏锐地认识到，通过恰当设计信道码，可以克服级联协议带来的延迟问题； [20] 的重点是开发适用于二进制表示的低密度奇偶校验码。在这种情形下，Alice 记录一个二进制序列 X，Bob 记录一个二进制序列 Y。序列 X 和 Y 长度相同。

Alice 使用所选低密度奇偶校验码的奇偶校验矩阵计算 X 的伴随式，并通过公共信道将该伴随式发送给 Bob。由于纠缠光子传输过程中出现的物理缺陷， X 和Y 不一定相同。将 X 与 Y 通过交叉概率为 p的二进制对称信道（BSC）建立统计关系较为方便，其中假定所有参与方都知道 p 。根据收到的伴随式和自己的旁信息 Y，Bob 的任务是推断 X 。研究 [20] 指出，要使低密度奇偶校验码有效，就需要针对接近容量运行的相应二元对称信道进行优化。为此，研究者利用离散密度演化工具优化低密度奇偶校验码的度分布，并在不同运行点构造相应的奇偶校验矩阵（每个运行点对应一种不同码率的编码）。所得编码通常长达数百万比特，以实现高性能。尽管这些编码都经过了高度优化，但它们在设计上彼此完全独立。这种方法会带来极高的实现复杂度，因为原则上，每个译码器都需要针对极长的码长单独实现。

随后，一系列研究致力于开发性能权衡优于完全交互式级联协议以及基准单轮 LDPC 编码的 LDPC 编码。二进制速率兼容低密度奇偶校验码此前已在 [21] 中针对分布式信源编码提出，因此也适用于量子密钥分发问题。节点打孔和码缩短是传统技术，已成功用于 [22] 中调整二进制 LDPC 码的码率，以适用于离散变量量子密钥分发（二元对称信道下）。

非二进制速率兼容低密度奇偶校验码在 [23]中被提出。这类速率兼容码的优势在于，Alice 可以逐步公开越来越多的综合校验比特，Bob 则结合自己的旁信息来解码 Alice 的序列。 [23] 中的码构造以一个“母码”为基础，使得

整个过程中都使用同一个二部图，从而至少在一定程度上缓解了原始低密度奇偶校验码方案所带来的实现挑战。

与其他（经典）应用一样，另一种很有前景的信道编码技术是基于极化码的。为实现高效率，人们同样研究了非常长的码（长度约为一百万比特）。研究表明，得益于递归译码，基于极化码的译码时延低于相当的低密度奇偶校验码；而且极化码在离散变量和连续变量场景中均有效 [24]。

我们在此指出，尽管大量相关工作致力于构造兼具高效率、速率兼容性和低复杂度的编码，但它们都一致地假设采用典型且经过充分研究的信道模型，即离散变量场景下的二进制对称信道，以及连续变量场景下的加性高斯白噪声信道，例如[23]–[26]。

显然，尽管这些假设能够利用传统通信应用中针对二进制对称信道和加性高斯白噪声信道编码的大量研究成果，但它们未能充分刻画我们先前在第III节讨论过的复杂时隙探测器特性和信道损伤。

在下一节中，我们将讨论专为高维时间纠缠量子密钥分发量身打造的数学工具的最新进展，并展示这些工具如何优于基于传统假设的现有方法，从而缩小与预期密钥率之间的差距。

V. 信息论与物理学力挽狂澜

要充分释放量子密钥分发系统的全部潜力，必须结合量子光子学在生成光子纠缠方面的新思路，以及信息论在如何充分利用这些携带信息的光子方面的新思路。回顾时隙协议中原始密钥比特的生成过程，参见第III-A节：光子的到达时间会在帧内标记为一个时隙索引。在基线脉冲位置调制中，Alice 和 Bob 仅保留包含单个光子的帧以供后续处理，所有其他帧（包括空帧以及标记了多个光子到达事件的帧）均予以丢弃。

如第 III-A 节所述，虽然可以轻松地使用基线脉冲位置调制来表示比特，但设计良好的自适应调制方案能够带来更好的性能。文献[27]研究了自适应调制方案的性能，这些方案不一定会丢弃检测到多个光子的帧。该论文基于一种更贴近现实的模型，分析并评估了固定和自适应脉冲位置调制方案的性能；该模型考虑了光子传输损耗、探测损耗和多对事件。数值结果证实了自适应方案的显著优势。

在一项近期研究中， [19], 对光子到达事件进行了更精细的建模，并据此首次分析了基线脉冲位置调制。该研究[19] 表明，与理论上可能达到的水平相比，这种基线方案产生的信息率显著偏低。研究者提出了三种新颖的自适应方案，以增加每个光子产生的原始比特数，并比较了它们所能达到的信息率。与 [12], [27], 不同的是，这项研究利用单占用时间箱和单空时隙生成秘密比特。

与更具信息量的调制方式类似，高维量子密钥分发系统也受益于能够利用时间表征的编码方案。回顾第 III节，我们描述了抖动误差、探测器停机时间和暗计数。因此，成功的信道编码设计应明确考虑局部和全局信道特性。

在 [28], 中提出了一种分层方案，将大字母表符号划分为各个独立的层。其核心思想是使用各自的低密度奇偶校验码对每个比特层进行编码，编码可以联合进行，也可以逐层进行。根据互信息链式法则，将联合信道拆分为逐层信道。 [28] 中的研究考虑了不同的信道模型，包含

均匀误差和局部误差。中考虑的低密度奇偶校验码是基于随机构造的正则（无结构）码。

在多维设置下， [13] 展示了多层方法在单光子探测器相关的光子匮乏条件以及长距离传播损耗下的实际可行性； [6], 则展示了该方法在实验室环境和已部署光纤上均成功实施。

设计的码应充分考虑信道特性，并具备足够的结构以实现快速译码。近期的研究方法 [29],[30] 精心构造了针对诱导信道局部—全局特性进行优化的低密度奇偶校验码。 [29] 中的工作首次考虑了该应用的有限长度码构造；它提出了一种平衡调制方案，并采用新的方法构造结构化低密度奇偶校验码。与此前关于量子密钥分发低密度奇偶校验码的文献不同，这种构造明确在码的Tanner图中纳入了全局纠错和局部纠错。具体而言，该码的 Tanner图具有一项特殊性质：校验节点分为两种互不相交的类型。第一种（全局）校验节点在组级别与变量节点相连；第二种（局部）校验节点则仅与各组内部的变量节点相连。

在 [30]中，进一步改进了针对组合高斯（量化）信道和均匀信道的码设计。在该方案中，空间耦合（SC）不规则重复累积（IRA）码将高性能SC码与IRA码策略性地结合起来，克服了原始多层方案 [28]中连续比特解码之间的依赖关系（以及由此产生的错误传播），同时与诱导信道良好匹配。与多层方案相比，密钥率至少提高了20%。

[31] 对存在探测器抖动的系统进行了严格分析。该研究计算了存在探测器抖动误差时可实现的密钥率，并构造了用于信息协调的编码，以逼近这些密钥率。

具体而言，论文表明，即使是标准的Reed-Solomon、BCH 和低密度奇偶校验码，也能实现远高于偏振纠缠QKD 所能达到的最大密钥率。

VI. 讨论与开放问题

在前文各节中，我们概述了量子密钥分发的基础知识，详细介绍了基于时间纠缠的量子密钥分发，并讨论了已知的离散变量量子密钥分发信道编码方法。除了基于 [19], [27]–[30]目前的研究结果，进一步探索信息论与编码理论中的相关思路，以处理更现实的时间-bin纠缠之外，我们认为，迄今总结的结果可作为研究和开发以下新兴量子技术适用数学模型（目前这类模型大多尚不可用）的起点。

•频率梳。得益于其频率标度和长期相干性，频率梳为纠缠光子生成提供了一个更新颖、更稳健的平台 [32]。

- 基于超纠缠的量子密钥分发。在超纠缠中 [18], , 信息表示在多个基上。例如，时间纠缠量子密钥分发中的单一时间-bin基可扩展为包含偏振或角动量。

•混合量子密钥分发方案。近期研究 [33]探讨了一种同时使用连续变量和离散变量量子密钥分发的混合量子密钥分发协议。

- 量子网络与会议密钥协商。量子网络 [34] 将实现安全多方通信，前提是存在高效的会议密钥协商多方协议。

以下技术都将分别从以下方面受益：

- 对恰当的信道模型进行仔细的数学刻画；

•建立容量型界，并对所研究的数学模型进行严格分析；

- 针对量子密钥分发信道的具体特性设计编码；

•低时延译码算法的设计与实现；

• 研究低密度奇偶校验码以外的其他类型编码；以及
•研究实用的联合调制与编码方案。

此外，确定相关攻击模型并为其提供安全性证明，是高维时间-bin量子密钥分发的另一个富有成果的研究方向。通过将未决问题与经典场景中的现有研究成果联系起来，我们希望表明，进入量子领域的门槛并不像看起来那么高，而且信息论与编码理论界能够在设计和开发未来的量子信息系统方面发挥重要作用。

致谢

本研究部分由美国国家科学基金会通过 FET 2007203 和 FET 2008728 项目资助。我们感谢以下同事：Murat Can Sarıhan 提供并解释实验数据，Esmaeil Karimi 和 Phil Whiting 就非理想探测器展开一般性讨论。

参考文献

[1] C. Shannon，《保密系统的通信理论》，贝尔系统技术期刊，第 28 卷，第 656–714 页，1949年4月。[2] 埃森哲，《厘清量子通信的未来》，白皮书，2022年12月。[3] E. Diamanti、H.-K. Lo、B. Qi 和 Z. Yuan，《量子密钥分发的实际挑战》，*npj Quantum Information*，第 2 卷，16025 页，2016年11月。[4] Z. Zhang、C. Chen、Q. Zhuang、F. N. Wong 和 J. H. Shapiro，《在 10 dB 损耗信道上以每秒 1.3 吉比特密钥率进行量子密钥分发的实验》，《量子科学与技术》，第 3 卷，025007 页，2018年4月。[5] S. Wehner、D. Elkouss 和 R. Hanson，《量子互联网：未来发展蓝图》，《科学》，第 362 卷，eaam9288 页，2018年10月。[6] 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，《用于提升量子密钥分发速率的大字母表编码》，《光学快报》，第 27 卷，第 17539–17549 页，2019年6月。[7] F. Xu、X. Ma、Q. Zhang、H.-K. Lo 和 J.-W. Pan，《使用实际器件实现安全量子密钥分发》，《现代物理评论》，025002 页，2020年5月。

[8] D. Birnie 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率”，*arXiv: 2207 04146 . [ ],* 2023 *cs.IT IEEE Trans. Commun.* 即将发表，.[9] D. Birnie IV，《时间纠缠量子密钥分发中探测器抖动的代价》，硕士论文，罗格斯大学新泽西州立大学研究生院，2021年。[10] C. Cheng，《探测器恢复时间对时间纠缠量子密钥分发密钥率的影响及其在线计算工具》，硕士论文，罗格斯大学新泽西州立大学研究生院，2022年。[11] A. K. Ekert，“基于贝尔定理的量子密码学”，《物理评论快报》，第67卷，第6期，第661–663页，1991年。[12] Y. Kochman 和 G. W. Wornell，“关于高效率光通信与密钥分发”，载于*2012*年信息论与应用会议（*ITA*）论文集，第172–179页，2012年2月。[13] 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，“利用时间-能量纠缠和高维编码实现光子高效量子密钥分发”，《新物理学杂志》，第17卷，022002页，2015年2月。[14] X. Cheng、M. C. Sarihan、K.-C. Chang、C. Chen、F. N. C. Wong 和 C. W. Wong，“基于波长复用时隙编码的安全高维量子密钥分发”，载于*2021*年激光与电光会议（*CLEO*），第1–2页，2021年5月。[15] U. Maurer，“通过公开讨论进行密钥协商”，*IEEE*信息论汇刊，第39卷，第733–742页，1993年3月。[16] G. Brassard 和 L. Salvail，“通过公开讨论进行密钥协调”，计算机科学讲义，第765卷，第410–423页，1994年。[17] A. E. Gamal 和 Y. Kim，网络信息论。剑桥大学出版社，2011年。[18] K.-C. Chang、X. Cheng、M. C. Sarihan、A. K. Vinod、Y. S. Lee、T. Zhong、Y.-X. Gong、Z. Xie、J. H. Shapiro、F. N. Wong 和 C. W. Wong，“双光子频率梳中的648维希尔伯特空间：形成纠缠与施密特模式分解”，*npj Quantum Information*，第7卷，48页，2021年3月。[19] 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率”，载于*IEEE*阿西洛马会议：信号、系统与计算论文集，2020年11月。[20] D. Elkouss、A. Leverrier、R. Alléaume 和 J. Boutros，“离散变量量子密钥分发的高效协调协议”，载于*IEEE*国际信息论研讨会（*ISIT*）论文集，2009年6月。[21]D. Varodayan、A. Aaron 和 B. Girod，“速率

自适应分布式信源编码”，信号处理，第86卷，第3123–3130页，2006年11月。[22] D. Elkouss、J. Martínez Mateo 和 V. Martin，“量子密钥分发的信息协调”，量子信息与计算，第11卷，第226–238页，2011年3月。[23] K. Kasai、R. Matsumoto 和 K. Sakaniwa，“采用速率兼容非二元低密度奇偶校验码的量子密钥分发信息协调”，载于*2010*年国际信息论及其应用研讨会，第922–927页，2010年10月。[24] P. Jouguet 和 S. Kunz-Jacques，“使用极化码实现量子密钥分发的高性能纠错”，量子信息与计算，第14卷，第329–338页，2012年4月。[25] S. Jeong、H. Jung 和 J. Ha，“用于连续变量量子密钥分发系统的速率兼容多边类型低密度奇偶校验码组”，*npj Quantum Information*，第1卷，6页，2022年1月。[26] M. Milicevic、C. Feng、L. Zhang 和 P. Gulak，“用于长距离量子密码学的准循环多边低密度奇偶校验码”，*npj Quantum Information*，第4卷，21页，2018年12月。[27] H. Zhou 和 G. Wornell，“面向高维量子密钥分发的自适应脉冲位置调制”，载于*IEEE*国际信息论研讨会（*ISIT*）论文集，2013年7月。[28] H. Zhou、L. Wang 和 G. 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*）论文集，2013年2月。[29] S. Yang、M. C. Sarihan、K.-C. 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*IEEE*阿西洛马会议：信号、系统与计算论文集，2019年11月。[30] S. Yang，应用驱动的编码技术：从云存储到量子通信。博士论文，加利福尼亚大学洛杉矶分校（UCLA），2021年。[31] J. J. Boutros 和 E. Soljanin，“时间纠缠量子密钥分发：密钥率与信息协调编码”，*arXiv*预印本 *arXiv:2301.00486*，2023年。[32] S. K. Lee、N. S. Han、T. H. Yoon 和 M. Cho，“频率梳单光子干涉测量”，*Communications Physics*，第1卷，51页，2018年9月。[33] I. B. Djordjevic，“性能优于离散变量和连续变量量子密钥分发协议的混合量子密钥分发协议”，*IEEE*光子学期刊，第12卷，第1–8页，2020年2月。[34] M. Proietti、J. Ho、F. Grasselli、P. Barrow、M. Malik 和 A. Fedrizzi，“实验量子会议密钥协商”，*Science Advances*，第7卷，eabe0395页，2021年6月。



Lara Dolecek 是加州大学洛杉矶分校（UCLA）电气与计算机工程教授，并兼任数学教授。Dolecek教授获得了加利福尼亚大学伯克利分校电气工程与计算机科学学士、硕士和博士学位，以及统计学硕士学位，她曾担任《IEEE信息论汇刊》《IEEE通信汇刊》和《IEEE通信快报》的副编辑。她曾任IEEE信息论学会秘书，现为该学会杰出演讲人。Dolecek教授曾获IBM教师奖（2014年）、诺斯罗普·格鲁曼卓越教学奖（2013年）、英特尔早期职业教师奖（2013年）、加利福尼亚大学教师发展奖（2013年）、大川研究资助（2013年）、NSF CAREER奖（2012年）和赫尔曼研究奖学金（2011年）。她与研究团队及合作者共同获得了十余项最佳论文奖。她的研究兴趣涵盖编码与信息论、图模型、统计方法和算法，并应用于数据存储与计算领域的新兴系统。



Emina Soljanin 是罗格斯大学教授。2016年转至罗格斯大学之前，她曾在贝尔实验室数学科学研究部门担任技术人员（杰出级），长达21年。她的研究兴趣和专长十分广泛。在过去的四分之一个世纪里，她参与了众多研究和商业项目，领域涵盖电力系统优化、磁记录、色彩空间量化、混合自动重传请求、网络编码、数据与网络安全、分布式系统性能分析以及量子信息论。她曾担任《IEEE信息论汇刊》编码技术领域的副编辑，曾是信息论学会理事会成员，并在其他期刊编委会和会议程序委员会担任过各种职务。Soljanin教授是IEEE会士、德州农工大学工程学院杰出校友、2011年帕多瓦尼讲师、2016/17年杰出演讲人，以及2019年IEEE信息论学会主席。