线性量子信道上的概率幅度整形离散调制连续变量量子密钥分发

Emanuele Parente、Michele N. Notarnicola、Stefano Olivares、Enrico Forestieri，*IEEE*终身会员，Luca Pot`ı，*IEEE*高级会员 和 Marco Secondini，*IEEE*高级会员

arXiv:2603.02870v1 [quant-ph] 3 Mar 2026

摘要——**GG02协议采用高斯调制所带来的实际实现困难，促使我们研究概率幅度整形技术与正交振幅调制格式相结合后，在连续变量量子密钥分发系统中的应用潜力。我们关注这一方向，是因为正交振幅调制和概率整形均可借助当前技术实现，并且已广泛应用于经典电信设备。本文假设线性量子信道场景，分析基于离散调制的协议可达到的最高安全密钥率、最远传输距离及其抗噪声能力，并与作为基准的 GG02 协议进行比较。具体而言，我们研究无限密钥长度区间，采用零差探测方案，并分析在集体攻击和反向协调情形下，不同距离对应不同输入字母表基数时的表现。我们发现，该协议不仅易于在实验室中复现，还能使性能接近 GG02 所提供的理论水平，同时保留确保无条件安全的能力。**

索引词—**连续变量量子密钥分发、无条件安全性、正交振幅调制、概率振幅整形、线性量子信道。**

I 引言

量子密钥分发（QKD）是量子密码学中最重要的应用，它能够确保两位经过认证的远程通信方 Alice 和 Bob 生成安全的一次一密密钥，即使存在强大的对手 Eve 也不例外 [1]。与经典密码学相比，QKD 的重要性在于它能够提供无条件安全性：它不对对手的能力作任何假设，其安全性仅基于量子力学定律 [2]。

Emanuele Parente 任职于意大利比萨圣安娜高等研究院电信、计算机工程与光子学（TeCIP）研究所。Enrico Forestieri 和 Marco Secondini 任职于意大利比萨圣安娜高等研究院电信、计算机工程与光子学（TeCIP）研究所，同时也任职于意大利比萨 CNIT 国家光子网络实验室。Michele N. Notarnicola 任职于捷克共和国奥洛穆茨 779 00 帕拉茨基大学光学系。Stefano Olivares 任职于意大利米兰大学“Aldo Pontremoli”物理系，地址为 I-20133 米兰，同时也任职于意大利米兰 INFN 分部，地址为 I-20133 米兰。Luca Pot`ı 任职于意大利比萨 CNIT 国家光子网络实验室。电子邮件：emanuele.parente@santannapisa.it。

量子密钥分发协议有两种等效形式：基于纠缠的（EB）版本和制备与测量（PM）版本。在这两种情况下，都需要一条用于交换光信号的量子信道，以及一条用于协调阶段的经认证的经典信道。Eve 可以篡改量子信道上的通信，但只能监听经典信道上的对话 [3]。具体而言，后一条信道必须经过认证，以便合法通信方确信彼此确实在进行通信；这可以通过信息论安全的经典算法实现，从而不会降低协议的整体安全性 [4]。经典信道被视为无误差信道，因此在后处理阶段发现的所有通信错误都完全归因于 Eve 对量子信道的干扰。事实上，利用非正交性或纠缠等量子特性，交换的量子态无法在不扰动系统的情况下被区分；根据不可克隆定理，它们也无法被完美复制 [5], [6]。这样一来，Alice 和 Bob 不仅能够检测到攻击者的存在，还能估算窃听者获取了多少有关密钥的信息；因此，只要 Eve 的干扰超过某个阈值，就可以中止协议。由于整个过程中传输的只有密钥，因此在这种情况下不会发生信息泄漏 [7], [8]。

由于光与物质的相互作用较弱且退相干时间较长，因此光是量子密钥分发领域中传输信息最常见、最实用的选择。量子密钥分发协议分为离散变量（DV-QKD）和连续变量（CV-QKD）两类，这一区别体现了可将密钥信息编码到光的不同自由度中的可能性：前者将信息编码在单光子（或弱相干态）的偏振（或时间 bin）上，后者则编码在光场的正交正交分量上。交换信号后，Alice 和 Bob 获得原始密钥，并通过多个后处理步骤对其进行提炼；在此过程中，双方交换经典辅助信息，最终达成安全共享密钥 [9]。

多个方面共同决定了通用量子密钥分发协议的性能，例如可实现距离、安全密钥的生成速率、实现的可行性（包括所用设备的成本）以及其提供的安全级别 [10]。在上述两类协议中，连续变量量子密钥分发协议近年来发展迅速 [11]，这主要是因为它们能够

避开离散变量量子密钥分发所需的单光子源和探测器所面临的技术挑战 [12]。具体而言，连续变量量子密钥分发协议非常适用于光纤系统（在城域范围内表现出高性能），并采用相干探测，即零差或外差探测（也称为相位分集或双零差探测）。这种探测方式具有探测效率更高、短距离下安全密钥率（SKR）更高、实施成本更低，以及与先进电信设备兼容性更强等优点（易于与光子芯片集成）。此外，波分复用等技术可在室温下使用标准硬件实现 [13], [14], [15], [16]。

此类协议中最著名、目前也被用作连续变量量子密钥分发基准的协议是 GG02。该协议由 Grosshans 和 Grangier 于 2002 [17], 提出，利用振幅随机取自高斯分布的相干态，并通过含噪的不可信信道发送。之所以采用高斯调制（GM），是因为在接收端进行相干探测时，它能够达到 Alice 与 Bob 之间高斯信道的香农容量 [5], [18]。尽管采用高斯调制可以简化安全性证明 [1], [13], [19], [20]，但也带来了若干实际困难：处理连续调制需要发射端的数模转换器（DAC）和接收端的模数转换器（ADC）具有无限分辨率；此外，还要求调制器具有无限消光比，并给发射端的随机数源带来极大的计算负担。此外，理论上需要无限峰值功率的信号调制才能生成高斯分布，因为该分布在相空间中的支撑范围确实是无限的 [12], [21], [22]。因此，在高信噪比和低信噪比两种极限下，缺乏高效纠错过程都会限制该协议的距离和可行性 [16]。

离散调制格式为高斯调制提供了一种实用的替代方案。这类格式通常用于数字通信，并且可以通过简单的调制方案和现成的光学器件来实现 [23]。一种有趣的选择是正交幅度调制（QAM），其星座点在相空间中排列成具有有限支撑的方形晶格。这种结构使其能够借助有限功率激光器和嵌套式马赫–曾德尔调制器实现 [24]。QAM 广泛应用于光通信，因为它能够以合理的实现复杂度提供较高的频谱效率 [25]。通过将其与概率幅度整形（PAS）结合，还可以进一步提升其性能。在概率幅度整形中，根据符号能量为星座中的发送符号分配不同的选取概率，目标是在给定平均符号能量的条件下最大化比特率 [26]。概率幅度整形正交幅度调制的主要优势包括精细的速率粒度，以及在实用的比特交织编码调制（BICM）框架内，仅使用标准二进制纠错码和逐比特软判决译码器，就能在很宽的信噪比范围内、针对加性白高斯噪声（AWGN）信道实现接近香农容量的性能 [27]。凭借这些特性及其简洁性，概率幅度整形正交幅度调制已成为一种广泛用于大容量光纤通信系统的调制方案 [28], [29] [30]。

将概率幅度整形正交幅度调制的优势引入实用的连续变量量子密钥分发系统，将是推动基于当前光网络中已部署的成熟技术大规模发展量子密钥分发系统的重要一步。例如，近期已有研究证明，可以使用二进制码和逐比特软判决译码器，为采用 QAM 调制的连续变量量子密钥分发实现高效的反向协调协议 [31]。然而，协议的此类变更必须有精确的安全性分析作为支撑。建立连续变量量子密钥分发协议时面临的挑战在于，其中涉及无限维希尔伯特空间，这阻碍了完整量子态层析的实现；因此，不可能精确获知 Alice 和 Bob 实际共享的量子态 [1]。事实上，尽管单个脉冲是高斯态，但平均量子态是非高斯的，因此，在信道评估阶段执行的协方差矩阵估计不足以对其进行完整表征。然而，2006 年，Navascues 等人 [32] 通过考虑与 Alice 和 Bob 所共享实际非高斯态具有相同协方差矩阵的高斯态，推导出了所得安全密钥率的下界，为超大 QAM 星座提供了适用的安全框架。对于研究更现实的非渐近密钥长度交换场景所需的更紧下界，可以通过凸优化问题，更确切地说是半正定规划（SDP）获得；但另一方面，这些方法在数值上计算量很大，不适用于星座规模较大的情况[33], [34]。近期，Denys 等人 [35] 解决了这一问题，并为任意量子信道上的相干态连续变量量子密钥分发协议的渐近密钥率计算引入了一个显式数值界：其方法结合了高斯最优性论证与半正定规划，所得结果表明，对于包含 64 个或更多符号的 QAM 星座图，该显式界是紧的。

在本研究中，我们提出一种基于 QAM 调制的连续变量量子密钥分发协议，该协议通过线性量子信道实现，可很好地模拟常见光纤中的传输；并在集体攻击、反向协调方案、无限密钥长度、零差探测以及距离范围为 0.5–300 km 的条件下，研究其可达速率、可实现距离和最大可容忍噪声。我们考虑不同的星座大小，并比较以下性能指标：输入符号按均匀分布（U-）或通过概率幅度整形技术（PAS-）以非均匀分布抽取时的情形，以及相应的 GG02 指标。随后，我们将这种无条件安全方法下得到的安全密钥率与 [36], 中所述假定窃听信道的情形进行比较；在该情形下，假设 Eve 实施分束攻击。我们还着重指出，在采用 QAM 调制和相干态的连续变量量子密钥分发协议中使用 PAS 技术所带来的性能优势。

II. 方法

A. 所提出的协议

参见图（1），下面我们介绍离散调制（DM）协议的 PM 版本，并考虑传输了无限多个符号时的渐近极限。

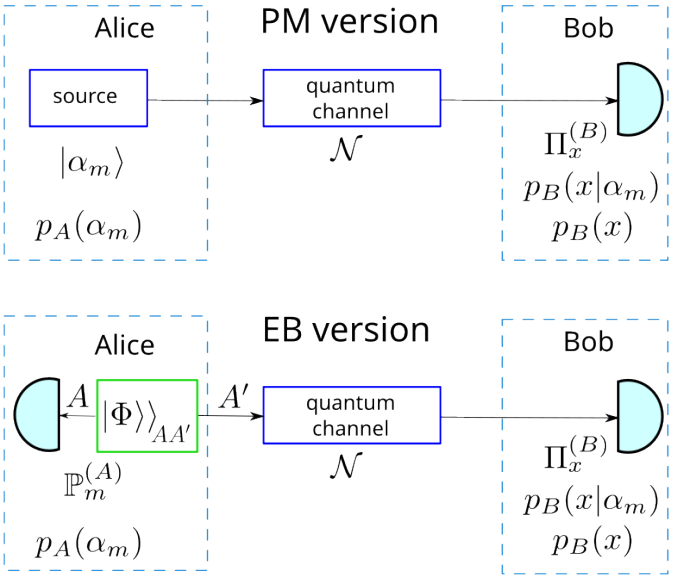

图 1. 我们离散调制协议的制备与测量版本（上）和基于纠缠的版本（下）。

Alice (A) 在一组位移单模相干态 $|x_A + iy_A\rangle$ 中编码一对经典变量 $(x_A,\ y_A)$，其中 $x_A,\ y_A \in \mathbb{R}$ 根据离散值概率分布生成。随后，Alice 通过由 Eve (E) 控制的量子信道将这些状态发送给 Bob (B)。在接收端，Bob 执行量子零差探测，随机测量两个正交正交分量 q 或 p之一，它们满足对易关系$[q,p] = 2i\sigma_0^2$，其中 σ_0^2 为散粒噪声方差。下文中，我们采用散粒噪声单位（SNU），即令 $\sigma_0^2 = 1$；此外，在不失一般性的前提下，我们假设 Bob 通过投影算符$\Pi_x^B = |x\rangle\langle x|$测量正交分量 q 。

在本工作中，我们关注通过光纤链路传输信号；该介质由透射率参数 T表征，该参数反映了光在其中传播时因随机散射造成的损耗，并且根据通信链路的长度呈指数变化d ，其关系为 $T = 10^{-\eta d/10}$，其中 $\eta = 0.2\text{dB/km}$ 是光波长为 1550nm [3]时的衰减系数。除损耗外，噪声也会影响通信的可靠性，其影响由过量噪声参数 ξ量化。在我们的分析中，我们假设量子信号的传输和检测可能受到噪声影响，并且量子信道是线性的。线性量子信道代表一类信道，其中也包括高斯信道 [1], [5]。事实上，该信道由以下内容表征：

海森堡绘景下正交分量算符的输入输出关系 [11], [20]

$$q_B = \sqrt{T}\, q_{A'} + q_b \quad \text{and} \quad p_B = \sqrt{T}\, p_{A'} + p_b, \tag{1}$$

其中， q_b 和 p_b 表示某些额外噪声模式的正交分量算符。假设这些算符与输入正交分量 $q_{A'}$ 和 $p_{A'}$ （即输入信号）不相关，其特征由前两阶矩给出

$$\begin{cases} \langle q_b \rangle = \langle p_b \rangle = 0\ , \\ \langle q_b^2 \rangle = \langle p_b^2 \rangle = 1 - T + \xi T\ . \end{cases} \tag{2}$$

信号交换后，Alice 和 Bob 进行后处理，通过经典认证信道共享辅助信息，以协商出共享密钥。具体而言，他们首先执行参数估计操作，估计描述信道的实验参数 T 和 ξ，以及 Eve 迄今可能获取的信息量；然后进行纠错协调，这一步可以采用直接协调（DR）或反向协调（RR），具体取决于密钥比特的信息分别由 Alice 还是 Bob 共享；最后执行隐私放大，从原始密钥中提取出更短的密钥，以消除窃听者 [9], [10]可能获取的任何信息。这里我们采用 RR 方案，因为它能够克服 DR 方案的 3 dB 极限问题。 [4], [10], [13]。

最后，为了确保我们的协议具有更高的安全性，我们考虑不可信设备场景——在此场景中，Eve 可以访问信道和 Bob 的装置——以及集体攻击的情形；在无限长密钥的渐近极限下，集体攻击是最强大的攻击。在集体攻击图景中，Eve 通过使所有信号与一组可分辅助态相互作用，对所有信号实施独立同分布（i.i.d.）攻击，将每个辅助态存储在量子存储器中，并在后处理结束时对它们进行联合测量。这样，Eve 就能利用信号传输，以及 Alice 和 Bob 在后处理过程中通过经典信道共享的公开信息。

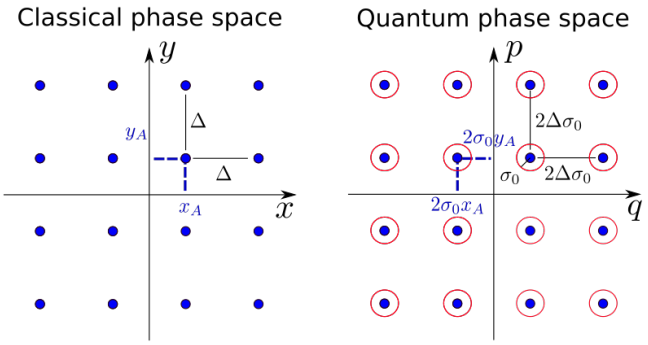

图 2. 经典（左）与量子相空间（右）中的 16QAM 星座图：前一种情况下，符号间距为 Δ，中心位于 (x_A, y_A)；后一种情况下，间距为 2Δ，位于 $(2\sigma_0 x_A, 2\sigma_0 y_A)$。

B. Alice 的调制

在调制阶段，Alice 生成一对对正交分量值 (x_A, y_A)，表示经典相空间中均匀方形 M 元 QAM 星座的坐标：这些值属于有限字母表 $\mathcal{A} = \Lambda \times \Lambda$，其中 $\Lambda = \{n\Delta \mid n = -(N-1)/2, \ldots, (N-1)/2\}$ 包含$N = 2^k$ 个点，$k = \mathbb{N}$ 和 $\Delta \in \mathbb{R}$，后者称为缩放因子或符号间距。随后，Alice 将 $\mathcal{A}$ 的 $M = N^2$ 个星座点映射到量子相空间[37]，方法是将每一对 (x_A, y_A) 编码为相应的相干态 $|x_A + iy_A\rangle$。具体而言，经典相空间中相邻点之间的距离等于Δ；相应地，根据任意相干态上的正交分量算符期望值 $|\alpha\rangle$ [13]

$$\langle q\rangle_\alpha = 2\sigma_0 Re(\alpha) \quad \text{and} \quad \langle p\rangle_\alpha = 2\sigma_0 Im(\alpha), \tag{3}$$

我们发现，在量子相空间中，QAM 符号仍排列成方形晶格，但其中心位于$(2\sigma_0 x_A，2\sigma_0 y_A)$，间距为 $2\sigma_0\Delta$，见图（2）。

Δ 的值与星座的平均能量有关，此处用平均光子数表示

$$\frac{\bar{n}}{2} = \sum_{z=-(M-1)/2}^{(M-1)/2} p_A(z)\,|z|^2, \tag{4}$$

其中，$p_A(z)$ 是控制正交分量 $z = (x_A, y_A)$提取的输入概率质量函数。对于 $p_A(z)$而言，一个简单的选择是均匀分布；不过，与相移键控（PSK）等仍需要相干检测的其他调制格式相比，基于 QAM 的系统可以通过采用 PAS 技术得到增强。QAM 与 PAS 的结合能够在固定发射功率下提高通信的比特率。具体而言，利用最大熵原理 [38] 或变分法 [39] 可以发现，对于离散星座的固定平均能量（因此对应于特定的功率使用），Maxwell-Boltzmann（MB）分布能够使香农熵最大化，并可提供终极整形增益 1。53dB [40]。MB 分布可写为

$$\mathcal{M}_\beta(z) = \frac{e^{-\beta z^2}}{\sum_z e^{-\beta z^2}} \quad , \tag{5}$$

其中，β 是整形参数：当 $\beta \to 0$ 时，我们得到均匀分布；而对于 $\beta \gg 1$，一般的 M-QAM会退化为QPSK 格式，因为星座外层点的提取被排除在外 [26]。

在本工作中，我们比较了我们的协议在量子态采用均匀信号传输与非均匀信号传输（即使用 MB 分布的概率幅度整形）时的性能。在均匀情形下，即 $p_A(z) = 1/N$，星座由单一参数表征，即间距 Δ（符号之间），其完全由所选的平均光子数 $\bar{n}$ 所确定：给定后者，Δ 可通过求逆（4）轻易求得。相反，当前验概率遵循 MB 分布（5）时，调制由两个参数表征，即间距 Δ与整形参数 β。这两个自由度受到所需平均光子数 $\bar{n}$ 的约束：对于任意固定的 β，Δ 的相应值可通过（4）求得。β 的最优值随后通过最大化安全密钥率（见下一节）来确定，依据 [27]中所述的数值过程。

C. 秘密密钥率计算

渐近秘密密钥率是评估连续变量量子密钥分发协议性能和安全性的基本指标。尽管无限长信号交换这一假设并不现实，但它为可实现的安全密钥率提供了上界，并简化了理论安全性分析 [22]。

对于采用反向协调方案的集体攻击，安全密钥率的下界由Devetak-Winter公式给出 [9]

$$SKR \geq \zeta I_{AB} - \chi_{BE}, \tag{6}$$

其中，I_{AB} 是Alice和Bob共享的互信息，χ_{BE} 是Bob与Eve之间的Holevo信息（HI），而 $\zeta \in [0,1]$ 是协调效率。具体而言，该参数考虑了Alice和Bob执行的不完美纠错，并由此限制他们能够提取的经典信息量；另一方面，HI 项不受 ζ 影响，因为假设Eve的能力不受当前技术水平的限制[16]。从现在起，我们将 ζ 设为现实值 0.95 [35]。

1）互信息：互信息 I_{AB} 衡量 Alice 与 Bob 之间交换的平均信息量 [2]。为计算这一项，我们考虑 II-A中描述的相位调制方案。每次使用信道时，Alice 制备相干态 $|x_A + iy_A\rangle$ 并通过量子信道发送；在输出端，Bob 测量正交分量 q 并获得测量结果 x_B。鉴于信道的线性，这等价于加性高斯白噪声图景，随机变量可由一般的输入输出关系描述 $x_B = 2\sigma_0\sqrt{T}x_A + n$，其中噪声 n 服从正态分布 $\mathcal{N}(0, \sigma_\xi^2)$；在我们的情形下，$x_A$，$n$因此 x_B均为实数。对于一般的 M元调制符号集，互信息可表示为 [41]

$$I_{AB} = \sum_{x_A} \int dx_B\; p_A(x_A) p_{B|A}(x_B|x_A) \times \log_2 \frac{p_{B|A}(x_B|x_A)}{\sum_{x'_A} p_A(x'_A) p_{B|A}(x_B|x'_A)}, \tag{7}$$

其中 $p_A(x_A)$ 是经典符号 x_A 的先验概率，而 $p(x_B|x_A)$ 是连接加性高斯白噪声信道输入与输出的转移概率

$$p_{B|A}(x_B|x_A) = \frac{1}{\sqrt{2\pi\sigma_\xi^2}} \exp\left(-\frac{(x_B - 2\sigma_0\sqrt{T}x_A)^2}{2\sigma_\xi^2}\right), \tag{8}$$

其中，方差值 $\sigma_\xi^2 = \sigma_0^2(1 + T\xi)$ 在 (8) 中量化了噪声对信道输出处接收信号的影响。

2) Holevo 信息：Holevo 信息项 χ_{BE}量化了在反向协调场景下，Eve 能够获取的有关 Bob的测量结果的最大信息量 [11]。准确确定这一数量对于连续变量量子密钥分发协议的安全性分析至关重要。

为便于分析，我们利用量子密钥分发协议的相位调制方案与纠缠基础描述之间的等价性 [13]，并重点讨论后者，因为它提供了一个更易处理的理论框架。在相位调制方案中，Alice 制备相干态 $\{|\alpha_k\rangle, p_A(\alpha_k)\}$，其中 $k = (x_A,\ y_A) \in \mathcal{A}$ 和 $\mathcal{A}$ 是 QAM 星座的符号集，后者由密度算符 $\rho = \sum_k p_A(\alpha_k)|\alpha_k\rangle\langle\alpha_k|$ 描述；而在纠缠基础描述中，Alice 实际上在两个模式 A 和 A' [20]中制备一组双体纠缠态$|\Phi\rangle\rangle_{AA'}$， [34]

$$|\Phi\rangle\rangle_{AA'} = \sum_{k\in\mathcal{A}} \sqrt{p_A(\alpha_k)}\ |\varphi_k\rangle_A|\alpha_k\rangle_{A'}, \tag{9}$$

其中 $\{|\varphi_k\rangle_A\}_{k\in\mathcal{A}}$ 构成模式 A中的正交归一基。为了确定向 Bob 发送哪个状态，Alice 对其进行局域测量，该测量由 POVM$\{\Pi_k^A = |\varphi_k\rangle_A\langle\varphi_k|\}_{k\in\mathcal{A}}$描述。这使得另一模式 A' 上的状态 $|\alpha_k\rangle_{A'}$ 投影为相干态，投影概率为 $p_A(\alpha_k)$。

随后，她通过量子信道将状态 $|\alpha_k\rangle_{A'}$ 发送给 Bob，该信道由完全正（CP）量子映射 $\mathcal{N}_{A'\to B}$描述；Alice 和 Bob 共享的二部态 ρ_{AB} 为

$$\rho_{AB} = (\mathbb{I}_A \otimes \mathcal{N}_{A'\to B})\left[\ |\Phi\rangle\rangle_{AA'}\langle\langle\Phi|\ \right], \tag{10}$$

其中，$\mathbb{I}_A$ 是作用于 Alice 一侧收集到的状态上的恒等信道，而 $(\mathbb{I}_A\otimes\mathcal{N}_{A'\to B})$ 是完全正且保迹（CPTP）映射。Alice 进行投影测量后 Bob 接收到的条件态为：

$$\rho_{B|\alpha_k} = \frac{1}{p_A(\alpha_k)}\,\mathrm{Tr}_A\left[\rho_{AB}\ (\Pi_k^A \otimes \mathbb{I}_B)\right]. \tag{11}$$

如果 Alice 发送了状态 $|\alpha_k\rangle = |x_A + iy_A\rangle$，Bob 进行零差探测并使用 POVM $\Pi_x^B = |x\rangle\langle x|$测量正交分量 q，那么 Bob 的测量结果 x_B 的条件分布为

$$p_{B|A}(x_B|x_A) = \mathrm{Tr}_A\left[\rho_{AB}\ |\varphi_k\rangle\langle\varphi_k|_A \otimes \Pi_x^B\right], \tag{12}$$

Bob 的测量结果所对应的边缘分布为：

$$p_B(x_B) = \sum_m p_{B|A}(x_B|x_A)p_A(x_A). \tag{13}$$

遗憾的是，这些可用统计量——即 $p_A(x_A)$、$p_{B|A}(x_B|x_A)$ 和 $p_B(x_B)$——不足以让相关各方唯一刻画底层的不可信量子信道，而这种信息不完整的情况有利于 Eve。事实上，窃听者可以利用产生相同输入—输出统计量的噪声映射 $\mathcal{N}$ 并不唯一这一点，选择并实施能使其可获取信息最大化的量子信道幺正扩张，同时确保其与 Alice 和 Bob 观测到的统计量相符，因此不会被察觉。为实现无条件安全，我们考虑 Eve 实施纯化攻击；此时，Devetak-Winter公式可改写为 [33]

$$\mathrm{SKR} = \zeta I_{AB} - \sup_{\mathcal{U}_{A'\to BE}\in S} \chi_{BE}, \tag{14}$$

其中，上确界取遍由 Eve 控制、且属于集合 S 的所有等距量子信道；该集合与 Alice 和 Bob 在 PM版本协议的参数估计阶段获得的信道统计相符。在此处考虑的纯化攻击中，Eve 持有一个三方隔离系统 ABE，该系统由纯态 $|\psi\rangle_{ABE}$ 描述，而 Eve 控制含噪完全正映射 $\mathcal{N}$的幺正扩张附加模式。密度矩阵 ρ_{AB} 和 ρ_E 可通过分别对 $|\psi\rangle_{ABE}$ 的模式 E 和 AB求迹得到。

现在，HI 项对应于 [9]

$$\chi_{BE} = S(E) - S(E|B), \tag{15}$$

其中 $S(E)$ 是 Eve 可通过集体测量获取的状态 ρ_E的冯·诺依曼熵，而 $S(E|B)$ 是 Bob 测量后（在本例中为零差投影）的同一状态的条件冯·诺依曼熵。然而，在纯化攻击情形下，状态 ρ_{AB}提供了与 ρ_E相同的熵计算结果，即 $S(E)$ $=S(AB)$，且 $S(E|B) = S(A|B)$，因此

$$\chi_{BE} = S(E) - S(E|B) = S(AB) - S(A|B). \tag{16}$$

这意味着可以直接根据 Alice 和 Bob 共享的二部态 ρ_{AB} [1], [9],[13]计算 χ_{BE}。

基于这一考虑，我们通过调用“高斯攻击的最优性”定理进行安全性分析 [20],[32], [42], [43], [44], 16 χ_{BE} <，该定理对式 () $\chi_{BE}^{(G)}$ 中的 HI 进行了界定：，其中 是与高斯态相关联的 HI $\rho_{AB}^{(G)}$，该高斯态具有相同的协方差矩阵 Γ_{AB}，与 ρ_{AB}。经过局部操作，Γ_{AB} 可表示为

$$\Gamma_{AB} = \begin{pmatrix} V\mathbb{I}_2 & Z\sigma_z \\ Z\sigma_z & W\mathbb{I}_2 \end{pmatrix} = \begin{pmatrix} \gamma_A & \gamma_C \\ \gamma_C & \gamma_B \end{pmatrix}, \tag{17}$$

其中，$\mathbb{I}_2$ = diag(1，1) 是单位矩阵，σ_z =diag(1，−1) 是泡利矩阵；V 是 Alice 端（模式 A）的方差，W 是 Bob 端的方差，而 Z 是关联项。此时，联合态 $\rho_{AB}^{(\mathrm{G})}$ 的冯·诺依曼熵可表示为 [33], [37]

$$S(\rho_{AB}) = g\left(\frac{d_1-1}{2}\right) + g\left(\frac{d_2-1}{2}\right), \tag{18}$$

其中，$d_{1,\ 2}$ 是 Γ_{AB} 的辛特征值，满足约束条件 $d_{1,\ 2} \geq 1$，即：

$$d_{1,2} = \sqrt{(\Delta \pm \sqrt{\Delta^2 - 4I_4})/2}, \tag{19}$$

and

$$g(x) = (x+1)\log_2(x+1) - x\log_2 x, \tag{20}$$

当 $\Delta = I_1 + I_2 + 2I_3$ 时，以及

$$I_1 = \det(\gamma_A)\ ,\ I_2 = \det(\gamma_B)\ ,$$
$$I_3 = \det(\gamma_C)\ ,\ I_4 = \det(\Gamma_{AB}). \tag{21}$$

条件熵 $S(\rho_{A|B}^{(\mathrm{G})})$则可计算为 $S(\rho_{A|B}^{(\mathrm{G})}) = g(d_3)$ [20] 其中

$$d_3 = \det(\gamma_A - \gamma_C(\gamma_B + \gamma_M)^{-1}\gamma_C^T), \tag{22}$$

且 γ_M 是与零差探测 [45]相关的 2×2 协方差矩阵:

$$\gamma_M = \lim_{\lambda\to 0}\begin{pmatrix}\lambda & 0\\ 0 & \frac{1}{\lambda}\end{pmatrix}. \tag{23}$$

在连续变量量子密钥分发的实际实现中，虽然调制阶段已知 Alice 的方差 $V = 1+2\bar{n}$，但 Bob 的方差 W 是通过测量确定的（透射率和过量噪声的数值在参数估计阶段后即可获得），因此唯一未知的量是交叉项Z，需要通过非局域双体测量直接评估 [11]。

在这方面，线性量子信道的假设解决了这一问题，并能精确计算 Z，进而得到纯化攻击下的协方差矩阵。信道的线性 Γ_{AB}确保 Alice 和 Bob 共享的态的协方差矩阵 $\Gamma_{AA'}$ 可以表示为 Alice 生成的二部态$|\Phi\rangle\rangle_{AA'}$ 的协方差矩阵的函数，其表达式为

$$\Gamma_{AA'} = \begin{pmatrix} V\mathbb{I}_2 & Z_{AA'}\,\sigma_z \\ Z_{AA'}\,\sigma_z & V\mathbb{I}_2\end{pmatrix}, \tag{24}$$

其中

$$Z_{AA'} = \frac{1}{2}\,{}_{AA'}\langle\langle\Phi|\,(q_A q_{A'} - p_A p_{A'})\,|\Phi\rangle\rangle_{AA'}. \tag{25}$$

为求得 Z，我们对二部纠缠态 $|\Phi\rangle\rangle_{AA'}$ [35]使用施密特分解:

$$|\Phi\rangle\rangle_{AA'} = \left((\rho_A^*)^{1/2}\otimes\mathbb{I}\right)|EPR\rangle\rangle_{AA'}\,, \tag{26}$$

其中，$|EPR\rangle\rangle = \sum_{n=0}^{\infty}|n_A\rangle|n_{A'}\rangle$ 为无限压缩下的双模压缩真空态，$\{|n\rangle_A\}_{n=0}^{\infty}$和 $\{|n\rangle_{A'}\}_{n=0}^{\infty}$为模式 A 和 A'的福克基。经过直接计算可得:

$$Z_{AA'} = \sum_{mn}\left\langle mm\middle|[\rho_A^{1/2}\otimes\mathbb{I}_2](a_A a_{A'})[(\rho_A^*)^{1/2}\otimes\mathbb{I}_2]\middle|nn\right\rangle + h.c. = \tag{27}$$

$$= \sum_{mn}\left\langle m\middle|\rho_A^{1/2}a_A(\rho_A^*)^{1/2}\middle|n\right\rangle\langle m|a_{A'}|n\rangle + h.c., \tag{28}$$

其中 $\langle m|a_{A'}|n\rangle = \sqrt{n}\,\delta_{m,\ n-1}$，因此

$$Z_{AA'} = \sqrt{n}\sum_n\left\langle n-1\middle|\ \rho_A^{1/2}a_A(\rho_A^*)^{1/2}\middle|n\right\rangle + h.c. = \tag{29}$$

$$= \left\langle n\middle|a_A^\dagger\ \rho_A^{1/2}\ a_A\ (\rho_A^*)^{1/2}\middle|n\right\rangle + h.c., \tag{30}$$

and

$$Z_{AA'} = 2\,\mathrm{Tr}[\rho_A^{1/2}\,a\,\rho_A^{1/2}\,a^\dagger]. \tag{31}$$

最终，协方差矩阵为 [20]

$$\Gamma_{AB} = \begin{pmatrix} V\mathbb{I}_2 & \sqrt{T}\ Z_{AA'}\sigma_z \\ \sqrt{T}\ Z_{AA'}\sigma_z & TV_B\mathbb{I}_2\end{pmatrix}, \tag{32}$$

其中

$$V_B = V + \chi \quad , \quad \chi = \frac{1-T}{T} + \xi. \tag{33}$$

III. 结果

通过与两个基准方案进行比较，评估所提出的连续变量量子密钥分发协议的性能。该协议采用结合了概率幅度整形的 QAM 调制。两个基准方案分别为：(i) 采用均匀分布的 QAM；(ii) 使用高斯调制的基准 GG02 协议。具体而言，我们将分析并比较这些方案可实现的最大密钥生成率、最大传输距离以及可容忍的最大过量噪声。此外，对于相同的协议，我们还将研究最优发射功率，以及能够实现正安全密钥率的功率范围；两者均以 Alice 端的每符号光子数表示。

A. 可实现的最大*SKR*

我们首先讨论无噪声情形（$\xi = 0$）。图（3）（左）展示了在固定距离为100km时，GG02以及采用均匀（U）分布或概率幅度整形（PAS）的4、16和64QAM方案的SKR随Alice端平均光子数 $\bar{n}$ 变化的情况。正如预期，不同星座图的SKR性能各不相同。4QAM等同于正交相移键控，其SKR峰值最低，且出现在极低的 $\bar{n}$处，之后SKR迅速衰减至零。增大星座的基数可以提高SKR峰值，并扩大SKR曲线在光子数域上的支撑范围。然而，均匀信号传输带来的改进相当有限，U-64QAM相较于U-16QAM增益甚微，且与GG02可实现的SKR峰值相差甚远；另一方面，PAS显著提升了性能，并能更充分地利用基数较大的符号集。PAS-16QAM的性能远优于U-16QAM和U-64QAM，而PAS-64QAM则进一步提升性能，缩小了与GG02之间的差距。

探究最大安全密钥率如何随传输距离变化，并验证各种协议之间的相对表现是否会发生变化，尤其值得关注。对于每个距离，我们将安全密钥率$_{max}$ 定义为安全密钥率曲线在不同发射功率下的峰值，并引入无量纲参数 R:

$$\mathrm{R} = \frac{\mathrm{SKR}_{\max}}{\mathrm{SKR}_{\max}^{\mathrm{GM}}} \tag{34}$$

其定义为给定协议所得的安全密钥率$_{\max}$ 与 GG02协议所得的安全密钥率之比。这可以衡量给定协议相较于GG02协议的效率。

图（3）右侧展示了这一效率参数。与均匀信号传输相比，概率幅度整形显著提高了协议的效率，并减缓了 R 在长距离下的衰减，此时信道损耗占主导地位。对于基数更高的 QAM 星座图，由于输入分布整形的灵活性更大，性能提升也更为显著。例如，传输距离超过 40% km 时，PAS-64QAM 的性能可达到 GG02 的；而在相同距离下，PAS-16QAM 已足以达到近乎 70% 的性能，优于 U-16QAM 和 U-64QAM，后两者的效率始终不超过 50%。总之，概率幅度整形不仅提高了基于 QAM 的协议的安全密钥率，还使 64QAM 这类高基数星座能够更接近

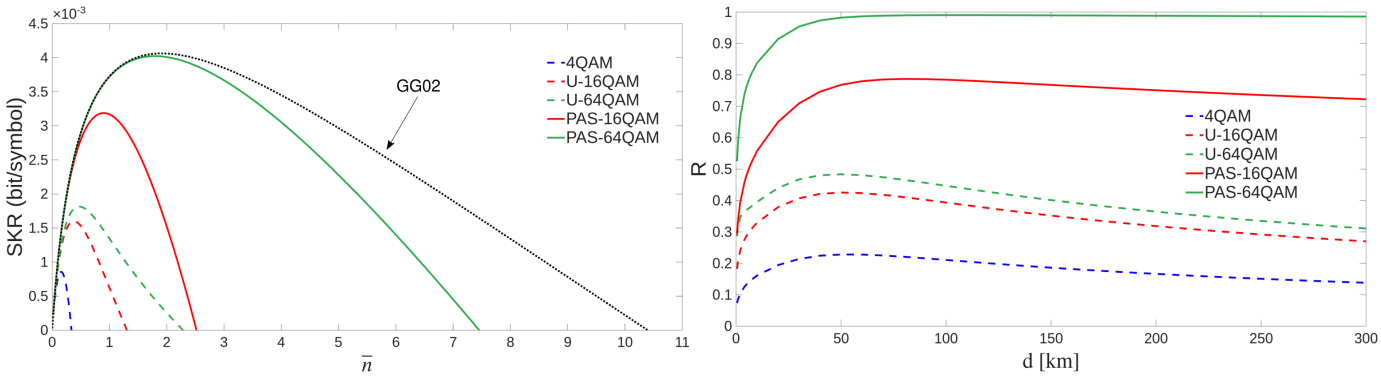

图 3. 在集体攻击、零差探测、反向协调且无过量噪声的情况下，100千米处 GG02 以及采用均匀和非均匀输入信号传输的 4QAM、16QAM、64QAM 的安全密钥率与 Alice 端光子数的关系（左）；R 在 0.5–300 千米范围内的对应值（右）。

GG02 的性能，使基于离散调制的实用协议在可实现的最大安全密钥率方面更具竞争力。

现在，我们来关注过量噪声的作用。过量噪声与损耗共同影响实际场景中的性能。我们固定星座基数（64QAM），并研究安全密钥率$_{\max}$ 随距离的变化，以及过量噪声水平 $\xi \in \{0.01, 0.03, 0.05\}$（以散粒噪声单位 SNU 计）逐渐增加时的情况。

如图（4）（左）所示，安全密钥率$_{\max}$ 会随着距离增加而更快衰减， ξ 增大时，安全密钥率会在越来越短的距离处降至零。然而，概率幅度整形仍然是一种有效的解决方案，与均匀信号传输相比，它显著减缓了衰减速度，并延长了最大传输距离。

这种韧性也体现在相对效率R的变化趋势中，如图（4）（右）所示。在短距离下，R 受星座基数 M的限制，这使得信源的熵上限为$\log_2 M$。有趣的是，在这一范围内，过量噪声水平 ξ 的增加会缩小离散调制与 GG02 之间的差距。这体现为：对于均匀信号传输，R 随 ξ 适度上升；而对于 PAS，上升幅度略大。

总体而言，在所有噪声水平下，PAS 相较于均匀信号传输都能带来显著增益。尽管整形信号调制受前述熵限制影响，无法在短距离下完全弥合与 GG02 之间的差距，但在中距离范围内表现越来越好，此时 R 接近 1。在这一范围内，过量噪声通常会降低离散调制相对于 GG02 的效率。然而，随着过量噪声水平升高，PAS 相较于均匀信号传输的优势愈发明显，效率参数 R 在很宽的距离和噪声水平范围内都保持接近 1。事实上，PAS-64QAM 达到的距离极限几乎与 GG02 相同，且其相对于 GG02 的效率直到距离极限前几公里才开始下降。

B. 发射功率

量子密钥分发系统中的一个关键设计参数是发射功率——通常表示为每个符号 $\bar{n}$在 Alice 一侧的平均光子数——必须进行优化，以确保在给定距离和噪声水平下安全运行。图（5）给出了最优发射功率随距离的变化$\bar{n}_{\max}$ （实线），该功率可使安全密钥率达到最大值，同时还给出了工作功率范围（阴影区域），其定义为安全密钥率保持为正时的最小和最大 $\bar{n}$值（虚线）。左、右面板分别对应 16QAM 和 64QAM 格式，所有图中均显示了 GG02参考。顶部、中部和底部面板表示不同水平的过量噪声。对于每个距离，Bob 一侧对应的功率值等于 $T(\bar{n} + \xi/2)$。

GG02协议在短距离下（信道损耗可忽略）起初具有较高的最优发射功率（超过每符号100个光子）和较宽的工作功率范围。随着距离增加，最优发射功率先迅速下降，随后稳定在近乎恒定的数值。同时，工作功率范围逐渐围绕最优功率收窄，并最终在协议达到最大传输距离时收缩为零，而最大传输距离取决于过量噪声水平。离散调制呈现出定性上相似的趋势，但也存在一些显著差异。首先，由于有限尺寸星座的熵限制，其最优发射功率在零距离时便从低得多的数值起步。此外，与GG02相比，其工作功率范围和最大可达距离通常都更小。均匀信号传输下这些限制尤为明显，从16QAM升级到64QAM带来的改善也微乎其微。相比之下，概率幅度整形的效率更高，因而相较于均匀信号传输，具有更高的最优发射功率和更宽的工作范围。值得注意的是，除最初的70km外——此时星座的熵约束仍会限制性能——PAS-64QAM的表现与GG02十分接近，其最优发射功率、工作功率范围和最大距离实际上都相同。

C. 最大可容忍过量噪声

现在，我们通过分析能够容忍的最大过量噪声，来评估所提出协议的抗噪性。

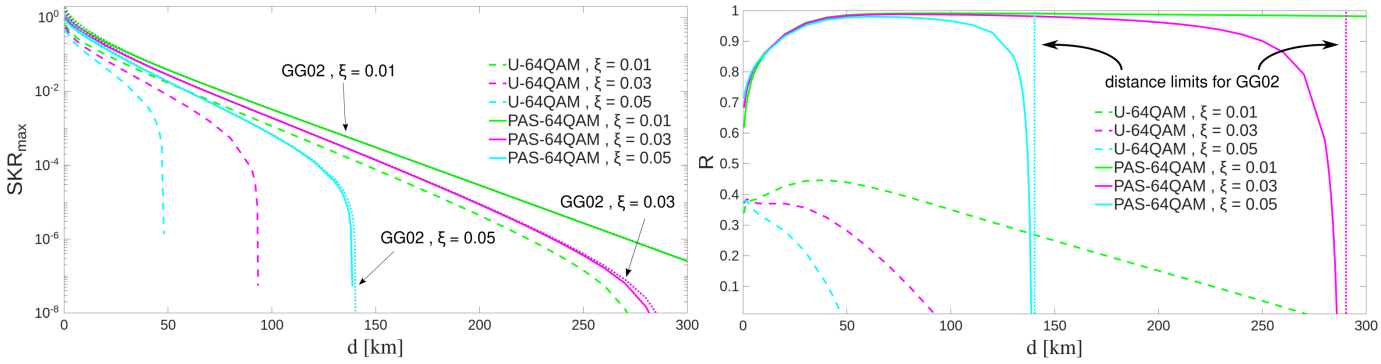

图 4。（左）在 0.5–300 km 范围内，对于不同过量噪声值 ξ，采用均匀和非均匀输入信号传输的 64QAM 的 SKR 最大值。GG02 曲线以点线表示，几乎无法区分，因为它们几乎完全与相应的 PAS 曲线重合。（右）在相同距离和过量噪声值范围内对应的 R 值；点线表示 GG02 在 $\xi = 0.03$（洋红色）和 $\xi = 0.05$（浅蓝色）下的最大可达距离。

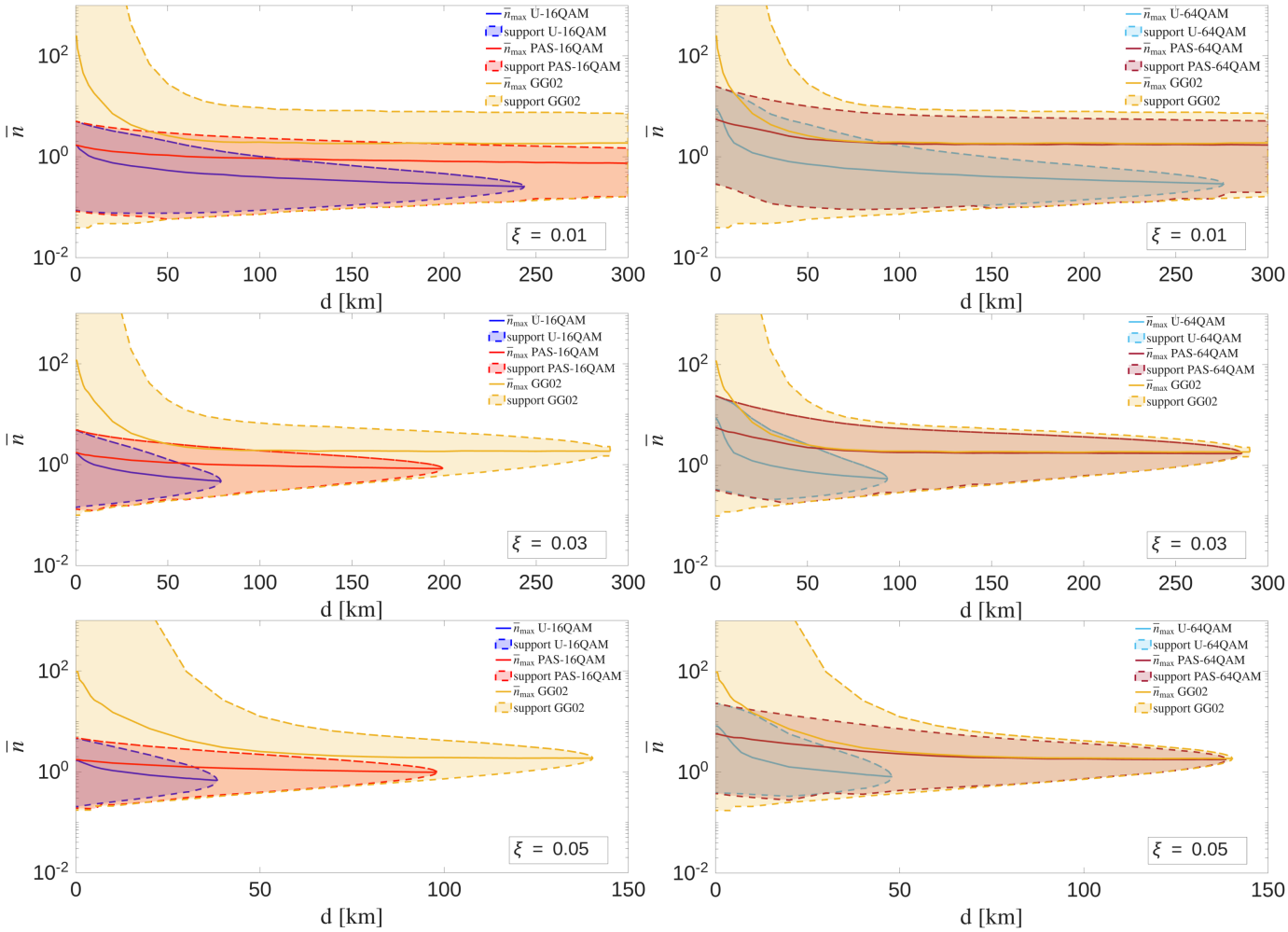

图 5。 $\bar{n}_{\max}$ 和平均光子数 在 Alice 端，16QAM（左）和 64QAM（右）的 SKR 曲线支撑范围，以及均匀和非均匀信号传输，并与不同过量噪声值下的 GG02 情况 c 况进行比较（从上到下 $\xi = 0.01$，0.03，0.05）。

作为传输距离的函数。我们将最大可容忍过量噪声定义为 ξ 的最高值，在该值下安全密钥率仍保持为正。图（6）比较了 GG02协议以及采用均匀或整形输入分布的基于 QAM 的协议的这一量。

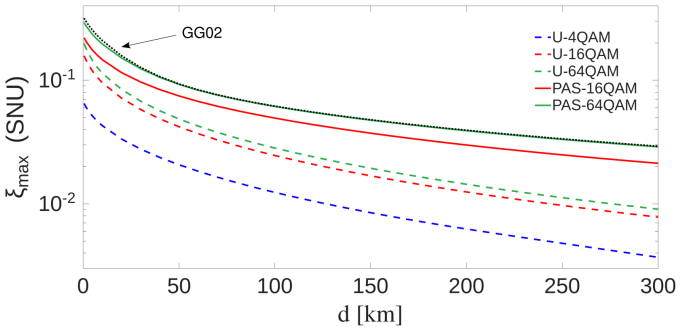

图6. 针对集体攻击、零差探测和反向协调，在0.5–300km范围内，采用均匀和非均匀信号传输的4QAM、16QAM、64QAM以及GG02协议的可容忍过量噪声 ξ_{max}。

与前几节中观察到的趋势一致，我们发现最大可容忍过量噪声随星座的基数 M 增大而增大，并随传输距离减小。这一行为反映了安全密钥率表达式（14）中两项相反的变化趋势：HI 项随噪声增大而增大，而 MI 项随噪声和距离的增大而减小。正如预期，均匀 QAM 对过量噪声的耐受能力明显低于 GG02。然而，概率幅度整形显著提高了基于 QAM 的协议的稳健性。值得注意的是，在长距离下，PAS-16QAM 的噪声容限相比均匀 16QAM 和 64QAM 均提高了一倍以上。此外，在所有超过40km的距离上，PAS-64QAM 所能容忍的过量噪声水平几乎与 GG02 相同。

D. 窃听信道安全性与无条件安全

要有效评估一种通用协议，必须考虑它所保证的安全性级别、所提供的性能以及实施的可行性。关于后两者，我们在上文讨论过，我们的协议如何轻松兼容目前采用的经典电信技术，以及它能达到怎样的可达速率、距离和抗噪性。至于其安全性，则体现在对 HI 项的估计中；在估计时，我们假设 Eve 能够纯化该系统，并引入由她控制的额外模式。

在下文中，我们将此处得到的结果与我们先前工作的结果进行比较 [36]，。在先前的工作中，我们研究了基于 QAM 的连续变量量子密钥分发方案，但采用的是不同的场景，即窃听量子信道，其中 Eve 仅限于实施分束攻击。尽管窃听信道所代表的窃听限制严格得多，但比较这两种信道模型有助于阐明概率整形技术在采用输入符号 QAM 调制的通用连续变量量子密钥分发系统中的作用。因此，了解窃听信道（w）和线性量子信道（ℓ）这两种假设如何影响同一连续变量量子密钥分发协议的性能，以及概率整形技术在这些不同情境中如何发挥资源作用，很有意义。这两种假设对应不同的安全级别。特别是，由于我们关注通信速率（安全密钥率，SKR）方面的优势，因此仅在无噪声框架下探讨这些特性。

在有损（无噪声）窃听信道场景中，Eve 无法改变量子信号的性质：事实上，她只能收集传播过程中丢失的那部分信号。因此，Eve 控制下的信道可以用一个分束器来描述，其输出端口分别将比例为 T 的信号传送给 Bob，并将被窃取的比例为 $1-T$ 的信号传送给 Eve [46]，[47]。在线性无噪声量子信道框架中，散粒噪声仍是 Eve 唯一可利用来掩饰其与系统交互的资源；但 Eve 的行动只需满足不改变 Alice 和 Bob 的统计特性这一约束，不受高斯攻击的限制，因此攻击者在选择扩张映射时拥有更大自由度，从而能够最大限度地获取有关系统的信息。

如前所述，用于评估相较于 GG02 协议的可达速率的一个良好指标是参数 R；在图（7）中，我们比较了各模型下该量的取值，以及 16QAM（左图）和 64QAM（右图）的结果。总体而言，就最大速率而言，线性量子框架（ℓ）的结果不如窃听信道框架。事实上，我们可以看到，（w）中的均匀信号传输曲线与（ℓ）中对输入概率进行麦克斯韦–玻尔兹曼整形所得的曲线非常接近：例如，U-16QAM（w）（蓝色虚线）的表现优于（ℓ）中得到的 PAS-16QAM（红色实线）。然而，这一特点在 64QAM 情形下并未出现：与前述情况不同，在此情形下，较大的统计集合使 PAS 技术对密钥分发可达速率的提升效果更为显著。

因此，我们可以说，在通常情况下，在假设线性量子信道的条件下，要提高针对 Eve 的策略和攻击的安全性，就需要以降低性能为代价。不过，即使均匀信号传输时，(ℓ) 中的 R 值明显低于 (w) 中的值，整形仍能在长距离范围内提升系统性能，缩小与 GG02 之间的差距。值得注意的是，与 (w) 相比，(ℓ) 中速率的百分比增幅按比例而言甚至更大；特别是可以很容易看出，经过 40千米的距离后，PAS-64QAM (ℓ) 的性能几乎与 PAS-64QAM (w) 相同。

IV. 结论

本研究在零差探测框架及无限密钥长度的渐近范围内，研究了采用均匀信号传输和非均匀信号传输（使用麦克斯韦–玻尔兹曼分布的概率幅度整形技术）的基于 QAM 的连续变量量子密钥分发系统。我们重点研究了集体攻击——这是渐近极限下最强大的一类攻击，并采用反向协调方案，因为该方案能够延长合法双方之间的通信距离。具体而言，我们基于线性量子信道模型研究了该系统；该模型能够简洁地描述量子信号在光纤链路中的传播，并且

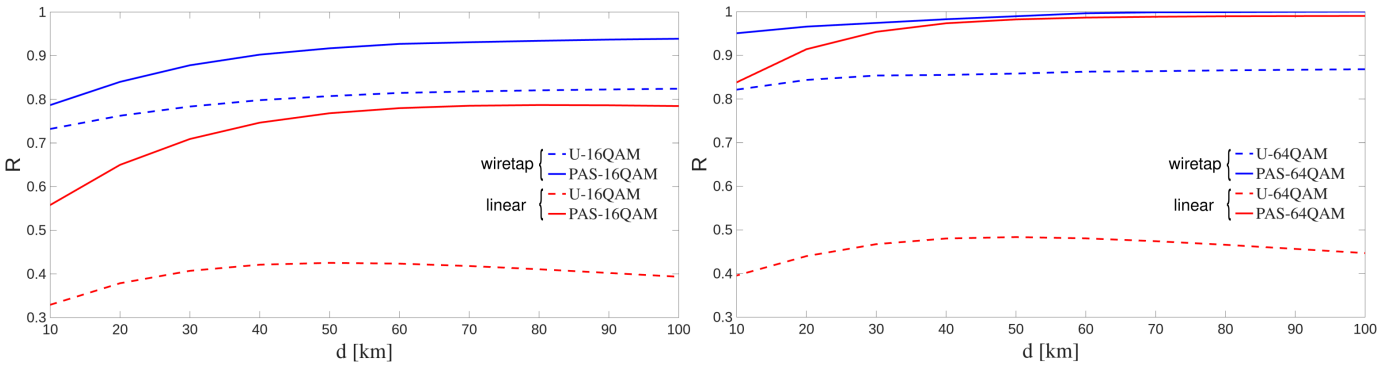

图 7. 集体攻击下的参数 R 对于窃听量子信道和线性 对于 16QAM（左）和 64QAM（右），在 10–100 千米范围内采用零差探测和反向协调时 量子信道，且无过量噪声。)

分析了该系统在纯化攻击下的表现。纯化攻击代表了 Eve 从系统中提取信息时可采用的最强策略。我们以 GG02协议为基准，评估了系统在不同过量噪声水平下可实现的安全密钥率和最大传输距离，并评估了其抗噪声能力。

我们发现，在本研究考虑的所有距离和过量噪声取值下，结合 QAM 调制与基于麦克斯韦-玻尔兹曼分布的概率幅度整形，始终优于相应的均匀分布协议。具体而言，PAS-64QAM 被证明是一种有效且实用的方案，能够使性能接近 GG02 协议，尤其是在长距离范围内。事实上，当距离超过约 40 千米时，PAS-64QAM 可实现几乎相同的安全密钥率，且其对过量噪声的容忍度与理想的 GG02 协议相同。此外，概率幅度整形在任何距离下都能显著提升基于正交振幅调制的方案的性能；更简单的 PAS-16QAM 优于复杂度更高的均匀 64QAM，并表现出更强的过量噪声鲁棒性。

此外，我们还分析了在对 Eve 的能力采用不同假设时，概率幅度整形（PAS）的影响。为此，我们比较了无噪声线性量子信道模型下的结果与有损窃听信道场景下的结果；在后一场景中，Eve 只能访问光纤链路缺陷所引入的那部分损耗。总体而言，我们发现，与有损窃听信道模型相比，在无噪声线性量子信道中，采用均匀输入符号概率的离散调制所能达到的密钥率较低。然而，在无噪声线性量子信道框架下，概率幅度整形（PAS）不仅能有效缓解这种性能下降，而且与有损窃听信道模型相比，还能带来更高比例的安全密钥率增益。在长距离范围内，PAS-64QAM 在两种信道模型下得到的最大安全密钥率相当吻合，这尤其体现了上述特点。

需要强调的是，对于非高斯协议例如本文研究的协议，Eve 的最优攻击策略仍是一个尚未解决的问题，这为未来研究非高斯攻击在离散调制连续变量量子密钥分发协议安全性分析中的作用铺平了道路。然而，一方面，线性信道假设相比有损窃听信道模型，为 Eve 提供了限制更少的操作框架；另一方面，它仍然限制了 Eve 的能力。为了进一步加强离散调制连续变量量子密钥分发的安全性评估，未来的工作将研究非线性量子信道这一最一般的情形，其特征是正交分量算符之间具有非线性输入输出关系。

致谢

本研究部分由 PNRR MUR 项目 PE0000023-NQSTI 以及 2014—2020年国家研究与创新运营计划——FSE REACT EU“行动 IV.5：绿色主题博士项目”资助。

参考文献

[1] C. Weedbrook、S. Pirandola、R. Garc´ıa-Patr´on、N. J. Cerf、T. C. Ralph、J. H. Shapiro和S. Lloyd，“高斯量子信息”，《现代物理评论》，卷 84， 2， 621 669, 2012 2 期页–。I、[2] II-A、II-C U. Maurer，“信息论密码学”，载于年度国际密码学会议。施普林格， 1999， 47 65 1 页–。I、[3] II-C V. Scarani、H. Bechmann-Pasquinucci、N. J. Cerf、M. Du˘sek、N. L¨utkenhaus和M. Peev，“实用量子密钥分发的安全性”，《现代物理评论》，第81卷，第3期，第1301页，2009。I、II-A [4] V. Martin、J. Martinez-Mateo和M. Peev，“量子密钥分发导论”，《威利电气与电子工程百科全书》，第1卷，第1–17页，2017。I、II-A [5] G. Cariolaro和G. Cariolaro，“量子通信系统”，《量子通信》，第281–359页，2015。I、II-A [6] S. L. Braunstein和P. Van Loock，“基于连续变量的量子信息”，《现代物理评论》，第77卷，577，2005 2，513期页–。I[7] N. Gisin、G. Ribordy、W. Tittel和H. Zbinden，“量子密码学”，《现代物理评论》，第74卷，第1期，第145页，2002。I [8] M. Du˘sek、N. L¨utkenhaus和M. Hendrych，“量子密码学”，《光学进展》，第49卷，第381–454页，2006。I [9] S. Pirandola、U. L. Andersen、L. Banchi、M. Berta、D. Bunandar、R. Colbeck、D. Englund、T. Gehring、C. Lupo、C. Ottaviani等，“量子密码学进展”，《光学与光子学进展》，卷 12， 4， 1012 1236, 2020 2， 2 期页–。I、[10] II-A、II-C、II-C II-C R. Wolf，《量子密钥分发》。施普林格，。I、II-A、II-A 2021

[11] Y. Zhang、Y. Bian、Z. Li、S. Yu和H. Guo，“连续变量量子密钥分发系统：过去、现在与未来”，Applied Physics Reviews，卷 11， 1, 2024 2， 2 期。I、II-A、II-C II-C E. Kaur、S. Guha和M. M. Wilde，“面向连续变量量子密钥分发的离散调制协议的渐近安全性”，Physical Review A，第103卷，第1期，第012412页，2021。I [12] F. Laudenbach、C. Pacher、C.-H. F. Fung、A. Poppe、M. Peev、B. Schrenk、M. Hentschel、P. Walther和H. H¨ubel，“采用高斯调制的连续变量量子密钥分发——实用实现理论”，Advanced Quantum Technologies，第1卷，第1期，第1800011, 2018 2， 2 页。I、II-A、II-B、II-C II-C [13] A. A. Abushgra，“基于传统系统测量的量子密钥分发协议变体：文献综述”，Cryptography，第6卷，第1期，第12页，2022。I [14] C. Lupo和Y. Ouyang，“非理想外差探测下的量子密钥分发：离散调制连续变量协议的可组合安全性”，PRX Quantum，第3卷，010341，2022 1，期页。I [15] A. Leverrier和P. Grangier，“采用离散调制的长距离连续变量量子密钥分发的无条件安全性证明”，Physical Review Letters，第102卷，第18期，第180504页，2009。I、II-C [16] F. Grosshans和P. Grangier，“使用相干态的连续变量量子密码学”，Physical Review Letters，第88卷，第5期，第057902页，2002。I [17] A. S. Holevo和V. Giovannetti，“量子信道及其熵特征”，Reports on Progress in Physics，第75卷，046001，2012 4，期页。I [18] N. J. Cerf、G. Leuchs和E. S. Polzik，《原子与光的连续变量量子信息》。World Scientific，2007。I [19] M. N. Notarnicola等，“连续变量系统中的量子通信”， 2024 2， 2， 2， 2 。I、II-A、II-C II-C II-C [20] P. Jouguet、S. Kunz-Jacques、E. Diamanti和A. Leverrier，“实用连续变量量子密钥分发中的缺陷分析”，Physical Review A——原子、分子与光物理，第86卷，第3期，第032309页，2012。I [21] E. Diamanti和A. Leverrier，“利用量子连续变量分发密钥：原理、安全性与实现”，Entropy，第17卷，第9期，第6072–6092页，2015。I、II-C [22] I. B. Djordjevic，“论基于离散化高斯调制（DGM）的连续变量量子密钥分发”，IEEE Access，第7卷，第65 342–65 346页，2019。I [23] J. Proakis和M. Salehi，“数字通信第4版，McGraw-Hill”，纽约，2001。I [24] P. J. Winzer，“高频谱效率光调制格式”，Journal of Lightwave Technology，第30卷，第24期，第3824–3835页，2012。I [25] F. R. Kschischang和S. Pasupathy，“高斯信道的最优非均匀信号传输”，IEEE Transactions on Information Theory，第39卷，第3期，第913–929页，1993。I、II-B [26] G. B¨ocherer、F. Steiner和P. Schulte，“带宽高效且速率匹配的低密度奇偶校验编码调制”，《IEEE通信汇刊》，第63卷，第12期，第4651–4665页，2015。I、II-B [27] F. Buchali、F. Steiner、G. B¨ocherer、L. Schmalen、P. Schulte和W. Idler，“通过概率整形64QAM实现速率自适应与传输距离提升：实验演示”，Journal of Lightwave Technology，第34卷，第7期，第1599–1609页，2015。I [28] T. Fehenberger，“采用64QAM的多跨段光纤通信系统中概率整形编码调制的信息速率”，Optics Communications，第409卷，第2–6页，2018。I [29] T. Fehenberger、A. Alvarado、G. B¨ocherer和N. Hanik，“论非线性光纤信道中正交振幅调制的概率整形”，Journal of Lightwave Technology，第34卷，第21期，第5063–5073页，2016。I [30] M. Origlia和M. Secondini，“离散调制的软反向协调”，载于2025年第14届国际ITG系统、通信与编码会议（SCC）。IEEE，2025，第1–6页。I [31] M. Navascu´es、F. Grosshans和A. Acin，“连续变量量子密码学中高斯攻击的最优性”，Physical Review Letters，卷 97， 19， 190502, 2006 2 期页。I、II-C S. Ghorai、P. Grangier、E. Diamanti和A. Leverrier，“采用离散调制的连续变量量子密钥分发的渐近安全性”，Physical Review X，第9卷，第2期，第021059页，2019。I、II-C2、II-C2 [33] J. Lin、T. Upadhyaya和N. L¨utkenhaus，“离散调制连续变量量子密钥分发的渐近安全性分析”，Physical Review X，第9卷，第4期，第041064页，2019。I、II-C2 [34] A. Denys、P. Brown 与 A. Leverrier，“任意调制下连续变量量子密钥分发的显式渐近密钥率”，Quantum，第 5， 540, 2021 2 卷，第 页。I、II-C、II-C M. N. Notarnicola、S. Olivares、E. Forestieri、E. Parente、L. Pot`i 与 M. Secondini，“窃听信道上离散调制连续变量量子密钥分发的概率幅度整形”，IEEE Transactions on Communications，2023。I、III-D [36] S. Olivares，“相空间中的量子光学：高斯态教程”，The European Physical Journal Special Topics，第203卷，第1期，第 3 24, 2012 2 –页。II-B、II-C T. M. Cover，《信息论基础》。John Wiley & Sons，1999。II-B [38] G. D. Forney 与 L.-F. Wei，“多维星座。一、引言、性能指标与广义交叉星座”，IEEE Journal on Selected Areas in Communications，第7卷，892，1989 6，877，第 期，第–页。II-B [39] G. Forney、R. Gallager、G. Lang、F. Longstaff 与 S. Qureshi，“带限信道的高效调制”，IEEE Journal on Selected Areas in Communications，第2卷，第5期，第632–647页，1984。II-B [40] M. Secondini，“光信道的信息容量”，载于 Optical Fiber Telecommunications VII。Elsevier， 2020， 867 920 1 第–页。II-C [41] R. Garcıa-Patron 与 N. J. Cerf，“高斯攻击对连续变量量子密钥分发的无条件最优性”，Physical Review Letters，第 97， 19， 190503, 2006 2 卷，第 期，第 页。II-C M. N. Notarnicola 与 S. Olivares，“采用可行物理无噪声线性放大器的长距离连续变量量子密钥分发”，Physical Review A，第 108， 2， 022404, 2023 2 卷，第 期，第 页。II-C A. Leverrier，“连续变量量子密钥分发的理论研究”，博士学位论文，T 2009 2 elecom ParisTech，。II-C A. Ferraro、S. Olivares 与 M. G. Paris，“连续变量量子信息中的高斯态”，arXiv 预印本 quant-ph/0503237，2005。II-C2 [46] D. Sych 与 G. Leuchs，“采用多字母相移键控的相干态量子密钥分发”，New Journal of Physics，第12卷，第5期，第053019页，2010。III-D [47] Z. Pan、K. P. Seshadreesan、W. Clark、M. R. Adcock、I. B. Djordjevic、J. H. Shapiro 与 S. Guha，“受限窃听下跨量子窃听信道的密钥蒸馏”，Physical Review Applied，第14卷，第2期，第024044页，2020。III-D