arXiv:2304.03562v1 [quant-ph] 7 Apr 2023

非均匀相位随机化下量子密钥分发的密钥率界

Xoel Sixto,[1, 2, 3, *] Guillermo Curr´as-Lorenzo,[4] Kiyoshi Tamaki,[4] 和 Marcos Curty[1, 2, 3]
[1] *Vigo Quantum Communication Center, University of Vigo, Vigo E-36310, Spain*
[2] *Escuela de Ingeniería de Telecomunicación, Department of SignalTheory and Communications, University of Vigo, Vigo E-36310, Spain*[3] *atlanTTic Research Center, University of Vigo, Vigo E-36310, Spain*[4] *Faculty of Engineering, University of Toyama, Gofuku 3190, Toyama 930-8555, Japan*（日期：2023年4月10日）

诱骗态量子密钥分发（QKD）无疑是处理激光光源发射的多光子信号最高效的方案，并且能够实现与理想单光子源相同的密钥率标度。然而，该方案要求每个发射脉冲的相位都服从均匀随机分布。由于不可避免的器件不完善性，和/或为进行相位随机化而使用外部相位调制器（这会将可选相位限制在有限集合内），实际中可能难以保证这一点。本文研究了在任意连续或离散的非均匀相位随机化下，诱骗态 QKD 的安全性，并表明该技术对偏离理想均匀随机情形具有很强的鲁棒性。为此，我们将一种基于半定规划的新型参数估计技术与基不匹配事件相结合，从而精确估计决定可实现密钥率的参数。由此，我们证明，与针对限制更严格的情形的既有结果相比，我们的分析能够显著提升性能。

I. 引言

量子密钥分发（QKD）是一种在两个相距遥远的参与方（即 Alice 和 Bob）之间安全建立对称加密密钥的方法 [1–3]。其安全性基于量子力学原理，例如不可克隆定理 [4], ，该定理保证窃听者（Eve）试图获取分发密钥的信息时，必然会引入可检测的错误。重要的是，将 QKD 与一次一密加密方案 [5], 结合使用时，可提供信息论安全通信。

近年来，量子密钥分发领域在理论和实验方面都取得了长足进展，推动了城域和城际量子密钥分发网络的首次部署 [6–9]。尽管取得了这些显著成就，但要实现这项技术的广泛应用，仍有一些亟待克服的挑战。其中之一便是弥合理论与实践之间现存的安全性差距。这是因为量子密钥分发的安全性证明通常基于一些假设，而实际的实验实现并不满足这些假设。此类差异可能造成安全漏洞或所谓的侧信道，Eve 可能利用这些漏洞，在不被检测到的情况下破坏所生成密钥的安全性。

实际上，实用的 QKD发射机通常会发射由激光光源产生的相位随机化弱相干脉冲（PR-WCP）。这些脉冲可能包含多个处于同一量子态的光子。在这种情形下，Eve 不再受不可克隆定理的限制，因为多光子信号会为她提供信号光子的完美副本。因此，可以证明，采用 PR-WCP 的 BB84 协议的密钥率 [10] 会因光子数分裂（PNS）攻击 [11, 12]而随系统透射率呈二次变化。这种攻击使 Eve 能够完全获知由多光子脉冲生成的那部分密钥信息，同时不会引入任何错误。

要克服这一局限，目前最高效的解决方案无疑是诱骗态方法 [13–15], ： Alice 随机改变发送给 Bob 的 PR-弱相干脉冲的强度，从而使双方能够更准确地估计量子信道的特性。具体而言，利用与不同强度设置对应的观测测量统计数据，Alice 和 Bob 可以精确估计单光子脉冲的产额和相位错误率，而密钥正是由此提取出来的。因此，诱骗态方法实现的密钥率随量子信道透射率线性变化 [13–16], ，达到理想单光子源所能实现的标度。这项技术已在近期的多项实验中得到广泛验证 [17–23], ，包括卫星链路 [24, 25] 以及光子集成电路的应用 [26–29]。此外，多家公司目前已在商业上提供诱骗态量子密钥分发系统 [30–34], ，凸显了这项技术的重要性。

重要的是，相位随机化意味着，每个生成的弱相干脉冲的相位 θ 必须在 $[0, 2\pi)$中均匀随-机。也就是说，其概率密度函数（概率密度函数）， $g(\theta)$，必须满足 $g(\theta) = 1/2\pi$。然而，如今用于生成 PR-WCP的两种主要方法都无法完全满足这一条件。具体而言，在那些使激光源处于增益开关条件 [23, 35–40], 下的配置中，器件不完善性可能会阻止相位 θ 均匀分布。类似地，

* xsixto@com.uvigo.es

在为此目的使用外部相位调制器的那些配置中 [41–44]，仅选择有限数量的相位。两种情形都违背了诱骗态技术的一项关键假设。

离散相位随机化情形已在 [45] 中进行了分析（另见 [46]）。该工作假设 $[0, 2\pi$ 中的离散随机相位均匀分布，即，认为 $g(\theta)$ 满足

$$g(\theta) = \frac{1}{N} \sum_{k=0}^{N-1} \delta(\theta - \theta_k), \tag{1}$$

其中 $\delta(x)$ 表示狄拉克δ函数，且 $\theta_k = 2\pi k/N$，其中 N 为所选相位的总数。在这一假设下，[45] 表明，只需约 $N = 10$个随机相位，就可以逼近理想情形下可实现的密钥率；在该理想情形中，$g(\theta) = 1/2\pi$。尽管这一结果十分出色，但在实际中，相位调制器不可避免的缺陷以及电子噪声可能使相位 θ 无法做到完全均匀分布，从而使 [45] 中提出的结果无法应用于实际装置。

本文考虑一种更现实、更实用的情形：由于相位随机化过程存在缺陷，$g(\theta)$可能是任意的连续或离散概率密度函数，并为这一一般情形给出了渐近密钥率。在推导中，为简单起见，我们考虑集体攻击；但根据量子 de Finetti 定理，我们的结果对于相干攻击同样成立 [47]。本研究有两个关键要素：利用基不匹配事件（即Alice 和 Bob 选择不同基的事件），以及一种近期提出的、基于半定规划（SDP）的新型参数估计技术 [48]。值得注意的是，我们表明，这两个要素结合起来，能够紧致地估计在此处考虑的情形下评估密钥率所需的相关参数。由此我们发现，即使 $g(\theta)$为任意的连续或离散分布，诱骗态方法对于不完美相位随机化也确实非常稳健。值得注意的是，对于式（1）所述的理想离散相位随机化情形，我们的分析所得密钥率显著高于 [45]开创性分析所给出的密钥率。换言之，要达到相近的性能，所需用于选择相位的随机比特更少。

本文组织如下。在第 II，我们描述 Alice发射的量子态，当 θ 遵循任意概率密度函数，$g(\theta)$。然后，在第 III 节，我们介绍所考虑的诱骗态协议及其渐近密钥率公式。接下来，在第IV节，我们介绍基于半定规划以及基不匹配事件的使用的参数估计技术，以计算评估密钥率所需的不同参数。然后，在第 V节，我们模拟各种实际感兴趣的函数 $g(\theta)$ 对应的可实现密钥率，包括该函数已得到完全（或仅部分）刻画。第 VI节以总结结束本文。本文还包括一些附录，其中给出了额外的计算。

II. 任意 $g(\theta)$ 下的相位随机化

本节将描述 Alice 发射的量子态，其中每个量子态的相位 θ 均遵循任意的概率密度函数 $g(\theta)$。

特别地，强度为 μ 、相位为 θ 的弱相干脉冲可用福克基表示为

$$|\sqrt{\mu}e^{i\theta}\rangle = e^{-\frac{\mu}{2}} \sum_{n=0}^{\infty} \frac{\left(\sqrt{\mu}e^{i\theta}\right)^n}{\sqrt{n!}} |n\rangle, \tag{2}$$

其中，$|n\rangle$ 表示含有 n 个光子的福克态。

如果 Alice 按照 $g(\theta)$ 独立且随机地为每个生成的信号选择相位 θ ，则其状态可简单表示为

$$\rho^{\mu}_{[g(\theta)]} = \int_0^{2\pi} g(\theta) \hat{P}(|\sqrt{\mu}e^{i\theta}\rangle) d\theta, \tag{3}$$

其中 $\hat{P}(|\phi\rangle) = |\phi\rangle\langle\phi|$。

任何量子态总可以在某个标准正交基下对角化。对于由公式（3）给出的态，我们将此类基的元素记为$|\psi_{n,\mu,g(\theta)}\rangle$，因为一般而言，它们可能同时取决于强度 μ 和函数 $g(\theta)$。这里，下标 n仅用于标识基的不同元素，而这些元素不一定是福克态。也就是说，特别地，我们可以将由公式（3）给出的态改写如下

$$\rho^{\mu}_{[g(\theta)]} = \sum_{n=0}^{\infty} p_{n|\mu,g(\theta)} \hat{P}(|\psi_{n,\mu,g(\theta)}\rangle), \tag{4}$$

其中，系数 $p_{n|\mu,g(\theta)} \geq 0$满足$\sum_{n=0}^{\infty} p_{n|\mu,g(\theta)} = 1$。也就是说，在她选择强度 μ 且 θ 遵循概率密度函数$g(\theta)$的情况下，这些系数可以解释为：在某个时间点，Alice 发射状态$|\psi_{n,\mu,g(\theta)}\rangle$的概率。

例如，在理想情形下，若 $g(\theta)$ 在 $[0, 2\pi$ 中均匀随机，则发射的信号是由福克态构成的泊松混合，其表达式为

$$\begin{aligned}\rho^{\mu}_{[\frac{1}{2\pi}]} &= \frac{1}{2\pi} \int_0^{2\pi} \hat{P}(|\sqrt{\mu}e^{i\theta}\rangle) d\theta \\ &= e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} \hat{P}(|n\rangle),\end{aligned} \tag{5}$$

即 $p_{n|\mu,\ 1/2\pi} = e^{-\mu}\mu^n/(n!\ )$ 和 $|\psi_{n,\ \mu,\ 1/2\pi}\rangle = |n\rangle$。

III. 协议描述与密钥生成率

具体而言，我们假设 Alice 和 Bob 实施一种诱骗态BB84方案，在每个基中采用三种不同的强度设置 $\{s,\nu,\omega\}$，其中 $s>\nu>\omega\geq 0$。此外，我们考虑他们仅从双方均选择 Z 基，且 Alice 选择信号强度设置 s的事件中生成密钥。这是诱骗态 BB84协议中最典型的配置。不过，我们指出，以下分析也可以直接推广到其他协议配置，或其他强度设置组合。

在协议的每一轮中，Alice 以概率 $b\in\{0,1\}$ 选择一个比特值 $p_b=1/2$，以概率 $\alpha\in\{Z,X\}$ 选择一个基 p_α，以概率$\mu\in\{s,\nu,\omega\}$ 选择一个强度值p_μ，并根据 θ给出的概率密度函数选择一个随机相位 $g(\theta)$。随后，她生成一个强度为 μ 、相位为 θ的弱相干脉冲 $|\sqrt{\mu}e^{i\theta}\rangle$，并对脉冲施加操作，将她选择的比特值 b 和α 基编码到脉冲中。从 Eve 的角度来看，由于她不知道所选相位 θ，这些状态由式（4）描述。在接收端，Bob 使用基 $\alpha\in\{Z,X\}$ 测量每个到达信号，该基由他以概率 p_α选择。本文始终假设探测效率与基无关。也就是说，Bob 获得确定测量结果的概率不取决于他选择的基。

量子通信阶段结束后，Alice和Bob 通过经认证的经典量子信道广播为每个检测到的信号所选的强度和基设置。在双方均使用Z 基以及强度设置 s的检测信号中，与之相关的结果构成筛选密钥。对于 Bob选择 X 基的检测轮次，Alice 公布她的比特值 b ，而 Bob 宣布相应的测量结果。这些数据用于参数估计，即确定评估密钥率公式所需的相关量。最后，Alice 和Bob 按照QKD [1–3]中的标准后处理流程，对筛选密钥进行纠错和隐私放大，以获得最终的秘密密钥。关于诱骗态 BB84 方案协议步骤的更详细描述，读者可参见例如 [16]。

在理想情形下，当 $g(\theta)=1/2\pi$时，Alice 的态制备过程等价于发射福克态$|n\rangle$ ，其服从均值等于所选强度设置 μ的泊松分布，如式（5）所示。在这种情况下，具有该强度设置 s 的单光子脉冲和真空脉冲都对秘密比特[49]有贡献。多光子信号由于 PNS 攻击而不安全。类似地，当 θ 服从任意概率密度函数 $g(\theta)$，且 Alice 选择强度设置 μ时，由式（4）可知，她的态制备过程等价于以概率 $p_{n|\mu,g(\theta)}$生成纯态$|\psi_{n,\mu,g(\theta)}\rangle$ 。

函数越接近均匀分布， $g(\theta)$越接近均匀分布，信号（概率）$|\psi_{n,\ \mu,\ g(\theta)}\rangle$ （$p_{n|\mu,\ g(\theta)}$）越接近福克态 $|n\rangle$（概率 $e^{-\mu}\mu^n/n!$ ）。在这种情形下，Alice 和 Bob 原则上可以从任意$|\psi_{n,\ \mu,\ g(\theta)}\rangle$ 中蒸馏出秘密比特，只要 $\mu=s$，不过主要贡献主要来自索引为$n=0$，1的项，它们更接近真空和单光子脉冲。这些是我们将在下文考察的贡献。事实上，对于第V节中研究的示例，我们观察到，在考虑 $n>1$ 时所能获得的密钥率提升基本上可以忽略不计。

这意味着，特别是，所考虑的诱骗态BB84协议的渐近密钥率公式可以写成 [15, 49, 50]

$$\begin{aligned}R&\geq p_Z^2 p_s\Bigg\{\sum_{n=0}^{\infty}p_{n|s,g(\theta)}Y^Z_{n,s,g(\theta)}\left[1-h\left(e_{n,s,g(\theta)}\right)\right]\\&\quad-fQ^Z_{s,g(\theta)}h\left(E^Z_{s,g(\theta)}\right)\Bigg\}\\&\geq p_Z^2 p_s\Bigg\{\sum_{n=0}^{1}p^{\mathrm{L}}_{n|s,g(\theta)}Y^{Z,\mathrm{L}}_{n,s,g(\theta)}\left[1-h\left(e^{\mathrm{U}}_{n,s,g(\theta)}\right)\right]\\&\quad-fQ^Z_{s,g(\theta)}h\left(E^Z_{s,g(\theta)}\right)\Bigg\},\end{aligned}\tag{6}$$

其中，$Y^Z_{n,s,g(\theta)}$ 表示与状态$|\psi_{n,s,g(\theta)}\rangle$ 相关的产额，该状态在 Z 基中编码（并测量）；也就是说，在 Alice 和 Bob 选择 Z 基且 Alice 制备状态$|\psi_{n,s,g(\theta)}\rangle$的条件下，Bob 的测量装置中出现探测点击的概率；参数$e_{n,s,g(\theta)}$ 表示这些信号的相位错误率； $h(x)=-x\log_2(x)-(1-x)\log_2(1-x)$是二元香农熵函数；量 f 是纠错协议的效率；$Q^Z_{s,g(\theta)}$ 是 Alice 选择强度 s 且 Alice 和 Bob 选择 Z 基的条件下所发射信号的总增益，即 Alice 向 Bob 发送此类信号时，Bob 出现探测点击的概率；而$E^Z_{s,g(\theta)}$ 是与这些信号相关的总量子比特错误率（QBER）。此外，在式（6）中，上标 L（U）表示下界（上界）。

这些量$Q^Z_{s,\ g(\theta)}$ 和 $E^Z_{s,\ g(\theta)}$ 可直接在实验中观测到。原则上，概率 $p_{n|s,\ g(\theta)}$也可以获知，并且取决于态制备过程。然而，在实践中，可能很难通过解析方法求出它们的值。相反，在下一节中，我们将介绍一种简单的方法来获得下界$p^{\mathrm{L}}_{n|s,\ g(\theta)}$，即这些量的下界。在那里，我们还将解释如何估计参数 $Y^{Z,\ \mathrm{L}}_{n,\ s,\ g(\theta)}$ 和 $e^{\mathrm{U}}_{n,\ s,\ g(\theta)}$，以及$n=0$，1，它们是计算公式（6）所必需的。

IV. 参数估计

该分析采用了 [48] 近期在增益开关激光器相位相关性的研究背景下提出的技术。为简洁起见，下面我们介绍主要结果，详细推导请参阅附录A和B 。

A. 产额下界 $Y^{Z}_{n\,s,,g(\ \ \ \ \ \theta)}$

在附录A 中证明了，可以通过求解以下半定规划得到产额$Y^{Z}_{n\,,s,g(\theta)}$ 的下界：

$$\begin{aligned}\min_{J_Z}\quad & \mathrm{Tr}\left[\hat{P}(|\psi_{n,s,g(\theta)}\rangle)J_Z\right]\\ \text{s.t.}\quad & \mathrm{Tr}\left[\rho^{\mu}_{[g(\theta)]}J_Z\right]=Q^{Z}_{\mu,g(\theta)},\quad \forall\mu\in\{s,\nu,\omega\}\\ & 0\le J_Z\le\mathbb{I}.\end{aligned}\tag{7}$$

原则上，状态$|\psi_{n,s,g(\theta)}\rangle$ 和$\rho^{\mu}_{[g\ (\theta)]}$ 是已知的，但无法直接获取；它们取决于 Alice 选择的强度设置以及函数 $g(\theta$。此外，正如前文所述，在协议的一次实际执行中，增益 $Q^{Z}_{\mu,g(\theta)}$ 可通过实验直接观测。因此，式（7）中唯一未知的是进行最小化所针对的半正定算子J_Z 。令 J^{*}_{Z} 表示式（7）所给半定规划的解。那么，我们得到

$$Y^{Z}_{n,s,g(\theta)}\ge\mathrm{Tr}\left[\hat{P}(|\psi_{n,s,g(\theta)}\rangle)J^{*}_{Z}\right]:=Y^{Z,\mathrm{L}}_{n,s,g(\theta)}.\tag{8}$$

B. 相位错误率上界 $e_{n,s,g(\theta)}$

相位错误率$e_{n,s,g(\theta)}$由虚拟协议 [51]定义。为此，我们考虑一个标准假设，即 Bob 的测量效率与其所选基无关。于是，在 Alice 和 Bob 均选择Z 基，且 Alice 生成第 n个本征态$|\psi_{n,s,g(\theta)}\rangle$的那些轮次中，我们可以用以下等价方式描述 Alice 的制备过程。首先，她制备以下双体纠缠态

$$|\Psi^{Z}_{n,s,g(\theta)}\rangle=\frac{1}{\sqrt{2}}\left(|0_Z\rangle_A\hat{V}_{0_Z}+|1_Z\rangle_A\hat{V}_{1_Z}\right)|\psi_{n,s,g(\theta)}\rangle,\tag{9}$$

其中，$\hat{}\,V_{b_\alpha}$（$b=0,\ 1$ 和 $\alpha\in\{Z,X\}$）表示与 α 基和$\hat{}$比特值 b 相对应的编码操作。尽管我们的分析适用于任意 $\{V_{b_\alpha}\}$，但为简便起见，在模拟中，我们假设这些算子是理想的 BB84 编码算子，定义为

$$\hat{}V_{0_Z}|n\rangle=|n\rangle|0\rangle,\ \hat{}V_{1_Z}|n\rangle=|0\rangle|n\rangle,$$

$$\begin{aligned}\hat{V}_{0_X}|n\rangle&=\sum_k\frac{1}{\sqrt{2^n}}\sqrt{\binom{n}{k}}|k\rangle|n-k\rangle,\\ \hat{V}_{1_X}|n\rangle&=\sum_k(-1)^k\frac{1}{\sqrt{2^n}}\sqrt{\binom{n}{k}}|k\rangle|n-k\rangle.\end{aligned}\tag{10}$$

接下来，她在 A 方程（9）中的标准正交基 $\{|0_Z\rangle,\ |1_Z\rangle\}$ 以了解所编码的比特值，并将另一个系统发送给 Bob，Bob在 Z 基中对其进行测量。

在这种情况下，相位错误率 $e_{n,s,g(\theta)}$ 对应于 Alice和 Bob 在 Alice（Bob）改为对辅助系统 A （到达信号）执行 X 基测-量时所观测到的比特错误率。如果Alice 对她的系统 A执行 X 基测量，这等价于发射以下状态

$$\begin{aligned}|\lambda^{\mathrm{virtual}}_{\Delta,n,s,g(\theta)}\rangle\propto|\bar{\lambda}^{\mathrm{virtual}}_{\Delta,n,s,g(\theta)}\rangle&={}_A\langle\Delta_X|\Psi^{Z}_{n,s,g(\theta)}\rangle\\ &=\frac{1}{2}\left[\hat{V}_{0_Z}+(-1)^{\Delta}\hat{V}_{1_Z}\right]|\psi_{n,s,g(\theta)}\rangle,\end{aligned}\tag{11}$$

概率为$p^{\mathrm{virtual}}_{\Delta\ n\ s\ ,\ \ ,\ \ ,\ g(\theta)}=\||\bar{\lambda}^{\mathrm{virtual}}_{\Delta\ n\ s\ ,\ \ ,\ \ ,\ g(\theta)}\rangle\|^2$，其中 $\Delta\in\{0,1\}$ 和 $|\Delta_X\rangle=\left[|0_Z\rangle+(-1)^{\Delta}|1_Z\rangle\right]/\sqrt{2}$。$^{-}$令 $Y^{(\Delta\oplus1)_X,\ \text{虚拟}\,\Delta,\ n,\ s,\ g(\theta)}$ 表示在 Alice 发射状态$|\lambda^{\mathrm{virtual}}_{\Delta\ n\ s\ ,\ \ ,\ \ ,\ g(\theta)}\rangle$的条件下，Bob 对到达信号执行 X 基测量时获得测量结果 $(\Delta\oplus1)_X$ 的概率。也就是说，该事件对应于相位错误。于是，相位错误率 $e_{n,\ s,\ g(\theta)}$ 可写为

$$e_{n,s,g(\theta)}=\frac{1}{Y^{Z}_{n,s,g(\theta)}}\sum_{\Delta=0}^{1}p^{\mathrm{virtual}}_{\Delta,n,s,g(\theta)}Y^{(\Delta\oplus1)_X,\mathrm{virtual}}_{\Delta,n,s,g(\theta)}.\tag{12}$$

在附录 A 中，通过求解以下半定规划，可以得到量$p^{\mathrm{virtual}}_{\Delta\ n\ s\ ,,,g(\theta)}Y^{(\Delta\oplus1)_X}_{\Delta\ n\ s\ g\ ,\text{虚拟}\ ,,,(\theta)}$ 的一个上界：

$$\begin{aligned}\max_{L_{(\Delta\oplus1)_X}}\quad & \mathrm{Tr}\left[\hat{P}(|\bar{\lambda}^{\mathrm{virtual}}_{\Delta,n,s,g(\theta)}\rangle)L_{(\Delta\oplus1)_X}\right]\\ \text{s.t.}\quad & \mathrm{Tr}\left[\hat{V}_{b_\alpha}\rho^{\mu}_{[g(\theta)]}\hat{V}^{\dagger}_{b_\alpha}L_{(\Delta\oplus1)_X}\right]=Q^{(\Delta\oplus1)_X}_{\mu,g(\theta),b_\alpha},\\ & \forall\mu\in\{s,\nu,\omega\},\forall b\in\{0,1\},\forall\alpha\in\{Z,X\}\\ & 0\le L_{(\Delta\oplus1)_X}\le\mathbb{I},\end{aligned}\tag{13}$$

其中 $\rho^{\mu}_{[g\ (\theta)]}$ 由式（4）给出，而 $Q^{(\Delta\oplus1)_X}_{\mu\ g\ \theta\ ,\ ()\ b_\alpha}$ 表示在 Alice 选择强度设置 μ、基 α、比特值 b，且相位 θ 服从概率密度函数 $g(\theta)$的条件下，Bob 通过 X 基测量观察到结果 $(\Delta\oplus1)_X$的概率。我们注意到，式（13）包含了基不匹配事件 [52] 所提供的约束：在这些事件中，Alice 在 Z 基中制备信号，而 Bob 在 X 基中测量信号，这可能会得到更紧的估计。这是因为一般而言，$|\lambda^{\mathrm{virtual}}_{\Delta\ n\ s\ ,,,}$ $_{g(\theta)}\rangle\neq\hat{}V_{\Delta_X}|\psi_{n,s,g(\theta)}\rangle$以及 $\hat{}P(|\lambda^{\mathrm{virtual}}_{\Delta\ n\ s\ ,,,g(\theta)}$)

可以用同时包含 Z 编码态和 X 编码态的算子形式线性组合来更好地近似，而不只是用后者。

值得注意的是，态 $|\bar{\lambda}^{\text{virtual}}_{\Delta\ n\ s}\text{、}\text{、}\text{、}_{g(\theta)}\rangle$ 以及 $\rho^{\mu}_{[g\ (\theta)]}$，，还有算子 V_{b_α}，都是已知的，并取决于 Alice 的态制备过程。增益 $Q^{(\Delta\oplus 1)x}_{\mu\ g\ \theta}$ ，() b_α 可在协议的一次实际运行中直接观测得到。也就是说，式（13）中唯一未知的是进行最大化的正半定算子 L 。

令 $L^{*}_{(\Delta\oplus 1)_X}$ 表示式（13）所给出的半定规划的解。于是有

$$p^{\text{virtual}}_{\Delta,n,s,g(\theta)} Y^{(\Delta\oplus 1)x,\text{virtual}}_{\Delta,n,s,g(\theta)} \le \text{Tr}\left[\hat{P}(|\bar{\lambda}^{\text{virtual}}_{\Delta,n,s,g(\theta)}\rangle) L^{*}_{(\Delta\oplus 1)_X}\right]. \tag{14}$$

也就是说，

$$\begin{aligned} e_{n,s,g(\theta)} &\le \frac{1}{Y^{Z,\text{L}}_{n,s,g(\theta)}} \sum_{\Delta=0}^{1} \text{Tr}\left[\hat{P}(|\bar{\lambda}^{\text{virtual}}_{\Delta,n,s,g(\theta)}\rangle) L^{*}_{(\Delta\oplus 1)_X}\right] \\ &:= e^{\text{U}}_{n,s,g(\theta)}. \end{aligned} \tag{15}$$

C. 数值求解方程（7）-（13）

对上述半定规划进行数值求解有两个主要难点。首先，由于态 $\rho^{\mu}_{[g(\theta)]}$ 是无限维的，因此它们也是无限维的。其次，这也使得计算式（4）给出的 $\rho^{\mu}_{[g\ (\theta)]}$ 的特征分解变得困难。为了克服这两个限制，我们采用近期在 [48, 53] 中提出的一种技术（另见[54]），将态 $\rho^{\mu}_{[g(\theta)]}$ 投影到一个至多包含 M 个光子的有限维子空间。我们将投影后的态记为

$$\rho^{\mu}_{[g(\theta)],M} = \frac{\Pi_M \rho^{\mu}_{[g(\theta)]} \Pi_M}{\text{Tr}\left[\Pi_M \rho^{\mu}_{[g(\theta)]} \Pi_M\right]}, \tag{16}$$

其中 $\Pi_M = \sum_{n=0}^{M} |n\rangle\langle n|$ 表示投影到M-光子子空间上的投影算符，其中 $|n\rangle$ 为一个福克态。在此过程中，现在可以很容易地通过数值方法获得$\rho^{\mu}_{[g\ (\theta)]\text{的特征分解，}\ M}$ 为方便后续讨论，我们将式（16）右端分子的特征分解记为

$$\Pi_M \rho^{\mu}_{[g(\theta)]} \Pi_M = \sum_{n=0}^{M} q_{n|\mu,g(\theta)} \hat{P}(|\varphi_{n,\mu,g(\theta)}\rangle). \tag{17}$$

重要的是，这种技术还可以将由方程（7）-（13）给出的无限维半定规划转换为可进行数值求解的有限维半定规划。所得半定规划及其推导见附录 B。

D. 概率的下界 $p_{n|s,g(\theta)}$

如上一小节所述，由于这些状态 $\rho^{\mu}_{[g\ (\theta)]}$ 是无限维的，因此可能难以计算它们的特征分解，从而难以计算概率 $p_{n|s,\ g(\theta)}$。相反，本文基于方程（17）给出的特征分解，为这些概率提供一个下界。具体而言，附录 B证明了

$$p_{n|s,g(\theta)} \ge q_{n|s,g(\theta)} - \epsilon_s := p^{\text{L}}_{n|s,g(\theta)} \tag{18}$$

with $\epsilon_s = 2\sqrt{1 - \text{Tr}\left[\Pi_M \rho^{s}_{[g(\theta)]} \Pi_M\right]}$.

V. 仿真结果

在本节中，我们现在评估各种函数 $g(\theta)$ 所能获得的密钥率。为便于说明，我们考虑三种主要情形，具体取决于函数 $g(\theta)$ 是否已被完全表征。此外，对于模拟，我们考虑一个简单的量子信道模型，其传输效率由$10^{-\frac{\gamma}{10}}$ 给出，其中 γ（以dB 为单位测量）表示系统总损耗，即，它还包括 Bob的探测器有限探测效率的影响。此外，为简单起见，我们忽略任何失配效应，并假设唯一的误差源是 Bob 的探测器暗计数，其速率设为 $p_d = 10^{-8}$。另外，如前所述，我们认为BB84 编码算子是理想的，尽管本文所述的分析在不满足这一条件时仍然适用，并取纠错效率 $f = 1.16$。

为获得界 $Y^{Z,\ \text{L}}_{n\ s\ ,\ ,\ g(\theta)}$ 以及$e^{\text{U}}_{n,\ s,\ g(\theta)}$，我们使用上述半定规划的有限维版本，相关内容见附录B。请注意，由此得到的密钥率是 M的递增函数。然而，数值求解此类半定规划所需的时间会随着该参数增大而迅速增长。因此，我们设置了足够大的 M，以确保数值测试表明，继续增大该参数对密钥率的提升可以忽略不计。

A. 完全表征的 $g(\theta)$

这里，我们考虑函数g（θ）已被完全刻画的情形，并评估两个具有实际意义的具体示例。第一个示例对应于式（1）所给出的情形，该情形已在 [45], 中被考虑；而第二个示例可以解释为第一个示例的含噪版本。

1. *Ideal discrete phase randomization*

结果如图所示。1图中展示了 Alice 选择不同随机相位总数 N 时的结果。具体而言，图中的实线是基于第 IV 节所述的参数估计流程，使用半定规划和基不匹配事件得到的。若舍弃这些后者事件，可获得的密钥率会降低，如点划线所示。最后，虚线对应于 [45] 中的分析。为完整起见，附录D总结了这一方法。前两种情况下，为简单起见，我们将强度设置设为可能并非最优的值 $\omega = 0, \nu = s/5$，并将 s 作为系统总损耗 γ 的函数进行优化；而在后一种情况下，我们设定 $\omega = 0$，并将 ν 和 s 都作为 γ 的函数进行优化（这为该方法提供了最优解）。重要的是，尽管如此，图1表明，与 [45] 中的结果相比，使用半定规划和基不匹配事件可显著提高密钥率。此外，我们发现，当 N 较小时，使用基不匹配事件带来的改进更为显著。事实上，当 $N \geq 5$ 时，这种性能提升几乎可以忽略不计。这是意料之中的，因为在理想的连续相位随机化情况下，即 *i.e.*，当 $N \to \infty$ 时，基不匹配事件并不能改善估计。另一方面，当 N 较小时，特征态 $|\psi_{n,s,g(\theta)}\rangle$ 对于 $n = 0,1$ 会偏离完美的福克态，这意味着虚拟态 $|\lambda^{\text{virtual}}_{\Delta\, n\, s\, ,,,g(\theta)}\rangle$ 会更偏离 X-ˆ 编码态 $V_{\Delta_X}|\psi_{n,s,g(\theta)}\rangle$，因此基不匹配事件能够提供更紧的估计。

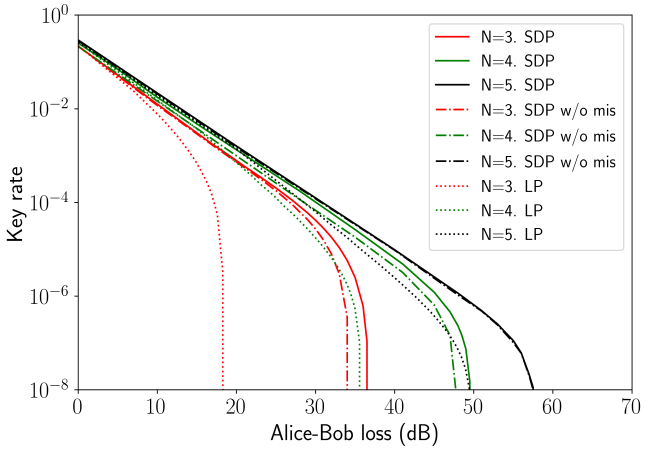


图 1. 对于式（1所给出的理想离散相位随机化情形，密钥率的对数值随总系统损耗的变化关系，其中密钥率是总随机相位数的函数 N，这些随机相位由 Alice 选取。实线对应于本文所考虑的、基于半定规划和基不匹配事件的参数估计过程；点划线表示忽略基不匹配事件时采用的相同过程。最后，点线对应于 [45] 中使用线性规划进行的分析。

值得注意的是，如图2所示，当 $N = 8$ 时，我们的方法所得到的密钥率已经相当接近理想情形；在该情形中，θ 在$[0, 2\pi$中均匀随机分布。需要注意的是，这种配置每个脉冲仅需三个随机比特来选择随机相位，因此不会显著增加随机数的消耗。

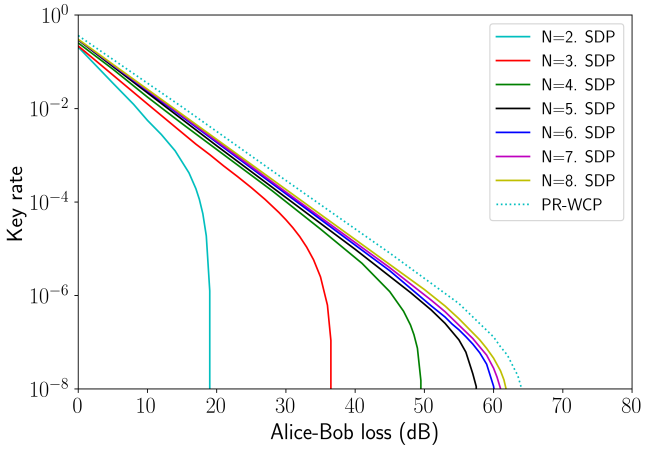


图 2. 对于式（1所给出的理想离散相位随机化情形，密钥率的对数值随总系统损耗的变化关系，其中密钥率是总随机相位数的函数 N，这些随机相位由 Alice 选取；Alice 和 Bob 采用本文所考虑的、基于半定规划和基不匹配事件的参数估计过程。值得注意的是，如图所示，仅需八个随机相位，就足以实现已相当接近理想 PR-WCP 情形的密钥率；在该理想情形中，每个脉冲的相位在 $[0, 2\pi$中均匀随机分布。

2. *Noisy discrete phase randomization*

这里我们考虑这样一种情况：Alice 在每个发射脉冲中编码的实际相位，会围绕所选离散值 $\theta_k = 2\pi k/N$ 按照某个概率密度函数分布。这可能是由相位调制器或控制它的电子设备存在器件不完善性所导致的。为便于具体说明，我们假设该概率密度函数服从截断高斯分布，不过需要指出，我们的分析适用于任意给定的分布。截断高斯分布的形式为

$$f\left(\theta;\theta_k,\sigma_k,\lambda_k,\Lambda_k\right) = \frac{\phi\left(\theta;\theta_k,\sigma_k^2\right)}{\Phi\left(\Lambda_k;\theta_k,\sigma_k^2\right) - \Phi\left(\lambda_k;\theta_k,\sigma_k^2\right)}, \tag{19}$$

当相位 θ 位于区间 $\lambda_k < \theta < \Lambda_k$内时，否则为零。这些函数 $\phi\left(x;\ \gamma,\ \sigma^2\right)$ 和 $\Phi\left(x;\ \gamma,\ \sigma^2\right)$ 在方程（19）中分别定义为

$$\begin{aligned}\phi\left(x;y,z\right) &= \frac{1}{\sqrt{2\pi z}} e^{-\frac{(x-y)^2}{2z}},\\ \Phi\left(x;y,z\right) &= \int_{-\infty}^{x} \frac{1}{\sqrt{2\pi z}} e^{-\frac{(t-y)^2}{2z}} dt.\end{aligned} \tag{20}$$

也就是说，在这种情形下，函数 $g(\theta)$具有以下形式

$$g(\theta) = \frac{1}{N}\sum_{k=0}^{N-1} f\left(\theta;\theta_k,\sigma_k,\lambda_k,\Lambda_k\right) \tag{21}$$

对于某些参数 θ_k、 σ_k、 λ_k 和 Λ_k。

当标准差 $\sigma_k \to 0\ \forall k$趋于极限时，式（21）收敛于式（1所给出的概率密度函数，因为在该情形下，每个截断高斯分布都趋近于狄拉克δ函数。另一方面，当 $\sigma_k \to \infty$时，并且鉴于由 λ_k 和 Λ_k 定义的截断区间的连接允许相位在 $[0,2\pi)$ 的范围内取任意值，但这些区间彼此不重叠，式（21）收敛于 $[0,2\pi)$ 中的均匀分布的概率密度函数。重要的是，这意味着在 σ_k取更高值时，可实现密钥率将提高；换句话说，在 g（θ）已被完全刻画的情况下，Alice在其制备的每个信号上实际施加的相位的不确定性增加时，可实现密钥率将提高。

仿真结果如图 3所示，该图比较了两个不同标准差值下的可实现密钥率σ_k。为简单起见，假设这些标准差对所有k都相等。正如预期， σ_k 的值越大，所得密钥率就越高，而与 N所选择的随机相位数量无关，尽管当 N 较小时，这种改善更加明显。为简单起见，并且由于缺乏实验数据，图 3 假设 $\lambda_k = \theta_k - 3\sigma_k$ 和 $\Lambda_k = \theta_k + 3\sigma_k$。此外，与前一个示例一样，我们令 $\omega = 0$， $\nu = s/5$ 并将 s 优化为系统总损耗的函数。

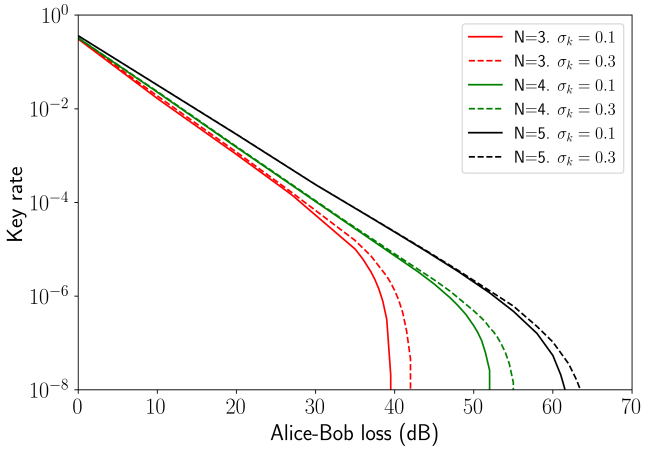


图 3. 当 g（θ）遵循由公式（21给出的概率密度函数时，密钥率的对数值与系统总损耗的关系，作为 Alice 选取的随机相位总数 N 的函数，并针对标准差 σ_k的两种不同取值，其中假设所有 k均相等。

B. 部分表征 $g(\theta)$

这里，我们现在考虑仅已知关于函数 $g(\theta)$的部分信息的情形。特别地，作为说明，我们将假设 Alice 在每个发射脉冲中编码的实际相位可以是所选离散值 $\theta_k = 2\pi k/N$附近某个区间内的任意相位，但其精确的概率密度函数 $g(\theta)$ 未知。具体而言，令$\delta_{\max}$ 表示实际选定相位 θ_k 与实际印加的ˆ相位之间的最大可能偏差，我们将该相位记为 θ_k。也就是说，我们假设实际印加的相位位于区间 $\hat{}\theta_k \in [\theta_k - \delta_{\max}, \theta_k + \delta_{\max}]$内，并保守地取使得按照附录 C中所述分析得到的密钥率最小的值组合 θ_k ，对于所有 k 均如此。

结果如图4所示，其为总相位数 N （由 Alice 选取）和最大偏差 $\delta_{\max}$的函数。与前面的示例一样，为简单起见，我们固定 $\omega = 0$， $\nu = s/5$ 并针对系统总损耗对 s 进行优化。正如预期， $\delta_{\max}$ 的值越大，所得密钥率越低。

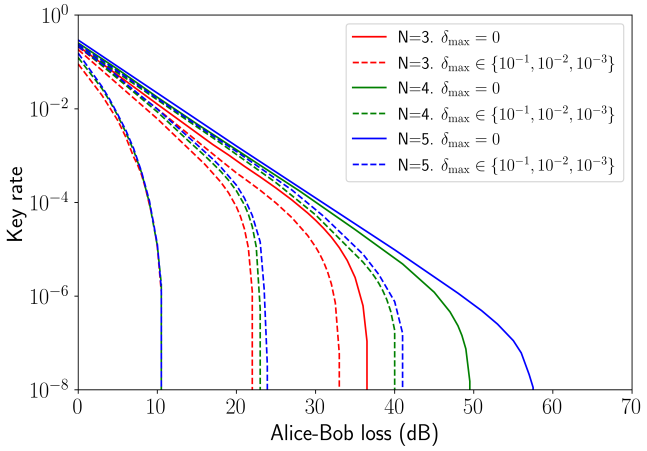


图4. 对数尺度下的密钥率与系统总损耗的关系，其中相位位于区间 $\theta_k \pm \delta_{\max}$内，且函数 $g(\theta)$ 未知；该关系以随机相位总数 N （由 Alice 选取）和 $\delta_{\max}$的值为函数。

此外，从图 4 可以看出，当 $\delta_{\max}$取值较高时，密钥率对参数 N的敏感度会降低。事实上，当 $\delta_{\max} = 10^{-1}$ 时， $N = 3$、4、5 这几种情况的可实现密钥率曲线基本重合，形成最左侧的曲线。这似乎是因为显著增大 $\delta_{\max}$ ，原则上会使某些相位彼此接近；当该参数足够大时，它们甚至可能变得相同。在这种情况下，增大 N 并不能改善性能，因为有效随机性几乎保持不变。

VI. 结论

在本文中，我们考察了诱骗态量子密钥分发（QKD）的安全性，其中每个生成信号的相位并非如理论所要求的那样服从均匀随机分布，而是遵循任意的、连续或离散的概率密度函数（概率密度函数）。这可能是由于相位随机化过程中存在设备缺陷，和/或由于使用外部相位调制器将随机相位施加到生成的脉冲上所导致的；后者将可选相位限制为有限集合。

我们的分析将一种基于半定规划的新颖参数估计技术与基不匹配事件的使用相结合，从而精确估计评估可实现密钥率所需的相关参数。在此过程中，我们表明，诱骗态 QKD 对有缺陷的相位随机化具有相当强的稳健性，尤其是在支配随机相位的概率密度函数得到良好表征时。此外，我们的结果在显著优于以往研究结果的同时，也更加一般，因为它们能够处理更现实、更实用的情形。

这项工作可能也与 QKD 之外使用激光光源和诱骗态的其他量子通信协议相关。

VII. 致谢

本研究获得了思科系统公司、加利西亚自治区政府（研究单位整合：AtlantTIC）、西班牙经济与竞争力部（MINECO）、通过编号为 PID2020-118178RB-C21的资助项目提供支持的欧洲区域发展基金（FEDER）、由欧盟下一代欧盟计划（PRTR-C17.I1）资助的MICIN，以及加利西亚自治区政府通过“量子通信领域与各自治区签订的 I+D+I补充计划”提供的自有资金支持；同时还获得了欧盟“地平线欧洲”框架计划下的Marie Sk·lodowska-Curie 资助项目（编号 101072637，项目 QSI）以及“量子安全网络合作伙伴关系”项目（QSNP，资助协议编号 101114043）的支持。X.S. 感谢西班牙大学部授予的FPI 博士前奖学金所提供的支持。G.C.-L. 感谢日本学术振兴会赴日本开展研究的博士后奖学金所提供的支持。K.T. 感谢日本学术振兴会科学研究资助金（JSPSKAKENHI）项目（编号 JP18H05237）所提供的支持。

附录A：给出式（7）-（13）的半定规划推导

在本附录中，我们遵循 [48], 中的方法，在集体攻击的假设下，推导正文公式（7）至（13）中给出的半定规划。

设 Ω 表示一个量子信道（或 Eve 的操作），它独立地作用于 Alice 发射的每个光脉冲。此外，假设在某一轮中，Bob 使用一个包含元素 Π 的正算子值测量（POVM）测量入射信号。在这种情形下，给定 Alice 向 Bob 发送量子态 σ，Bob 获得与元素 Π 相关联的测量结果的概率可表示为

$$\begin{aligned}\mathrm{Tr}[\Omega(\sigma)\Pi] &= \mathrm{Tr}\left(\sum_k A_k\sigma A_k^\dagger\Pi\right) = \mathrm{Tr}\left(\sigma\sum_k A_k^\dagger\Pi A_k\right)\\ &= \mathrm{Tr}(\sigma H),\end{aligned} \tag{A1}$$

其中 Ω(σ) 表示 Ω 对 σ的作用，$\{A_k\}$ 表示对应于量子信道 Ω 的算子和表示的 Kraus 算符集合，并且

$$0 \le H = \sum_k A_k^\dagger\Pi A_k \le \sum_k A_k^\dagger A_k = \mathbb{I}. \tag{A2}$$

Bob在以下任一 Z或 X 基中测量输入信号。我们将分别用$\{\Pi_{0_Z},\Pi_{1_Z},\Pi_f\}$和 $\{\Pi_{0_X},\Pi_{1_X},\Pi_f\}$表示与这两种测量相对应的 POVM 元素。也就是说，Π_{b_α} 表示与 b 基中的测量结果 α相关联的 POVM 元素，其中 $\alpha\in\{Z,X\}$，而 Π_f 表示与不确定性结果相关联的 POVM 元素。注意，这里我们隐含地考虑了基无关探测效率假设，这意味着 POVM 元素 Π_f 对于两个基均相同。令$\Pi_d = \mathbb{I}-\Pi_f = \Pi_{0_Z}+\Pi_{1_Z} = \Pi_{0_X}+\Pi_{1_X}$ 表示 Bob 一侧与确定性结果相关联的算子。然后，在将式（A1）中的状态 σ替换为 Alice选择 Z 基时发射的发射态后，

$$\rho^{\mu,Z}_{[g(\theta)]} = \frac{1}{2}\hat{V}_{0_Z}\rho^{\mu}_{[g(\theta)]}\hat{V}_{0_Z}^\dagger + \frac{1}{2}\hat{V}_{1_Z}\rho^{\mu}_{[g(\theta)]}\hat{V}_{1_Z}^\dagger, \tag{A3}$$

以及满足 Π 的算子 Π_d，我们得到

$$\begin{aligned}Q^Z_{\mu,g(\theta)} &= \mathrm{Tr}[\Omega(\rho^{\mu,Z}_{[g(\theta)]})\Pi_d] = \mathrm{Tr}[\rho^{\mu,Z}_{[g(\theta)]}H]\\ &= \mathrm{Tr}[\rho^{\mu}_{[g(\theta)]}J_Z],\end{aligned} \tag{A4}$$

其中 $H=\sum_k A_k^\dagger\Pi_d A_k$，以及满足条件的算子 J_Z

$$0 \le J_Z = \frac{1}{2}\left(\hat{V}_{0_Z}^\dagger H\hat{V}_{0_Z} + \hat{V}_{1_Z}^\dagger H\hat{V}_{1_Z}\right) \le \mathbb{I}. \tag{A5}$$

最后，考虑到在 Z 基中编码的状态$|\psi_{n、s、g(\theta)}\rangle$ 所对应的产额为

$$\begin{aligned}Y^Z_{n,s,g(\theta)} &= \mathrm{Tr}\{\Omega[\hat{P}(|\psi^Z_{n,s,g(\theta)}\rangle)]\Pi_d\}\\ &= \mathrm{Tr}[\hat{P}(|\psi_{n,s,g(\theta)}\rangle)J_Z],\end{aligned} \tag{A6}$$

with

$$\begin{aligned}\hat{P}(|\psi^Z_{n,s,g(\theta)}\rangle) &= \frac{1}{2}\hat{V}_{0_Z}\hat{P}(|\psi_{n,s,g(\theta)}\rangle)\hat{V}_{0_Z}^\dagger\\ &+ \frac{1}{2}\hat{V}_{1_Z}\hat{P}(|\psi_{n,s,g(\theta)}\rangle)\hat{V}_{1_Z}^\dagger,\end{aligned} \tag{A7}$$

我们得到式（7）中给出的半定规划。

关于式（13）给出的半定规划以估计相位错误率，我们注意到式（12）的分子可以表示为

$$\begin{aligned} & p^{\text{virtual}}_{\Delta,n,s,g(\theta)} Y^{(\Delta\oplus 1)_X,\text{virtual}}_{\Delta,n,s,g(\theta)} \\ &= p^{\text{virtual}}_{\Delta,n,s,g(\theta)} \operatorname{Tr}\left\{\Omega[\hat{P}(|\lambda^{\text{virtual}}_{\Delta,n,s,g(\theta)}\rangle)]\Pi_{(\Delta\oplus 1)_X}\right\} \\ &= \operatorname{Tr}\left[\hat{P}(|\bar{\lambda}^{\text{virtual}}_{\Delta,n,s,g(\theta)}\rangle) L_{(\Delta\oplus 1)_X}\right], \end{aligned} \tag{A8}$$

其中 $0 \le L_{(\Delta\oplus 1)_X} = \sum_k A_k^\dagger \Pi_{(\Delta\oplus 1)_X} A_k \le \mathbb{I}$ 根据式（A1），以及 $|\bar{\lambda}^{\text{virtual}}_{\Delta\ n\ s\ ,,,g(\theta)}\rangle = \sqrt{p^{\text{virtual}}_{\Delta\ n\ s\ ,,,g(\theta)}}|\lambda^{\text{virtual}}_{\Delta\ n\ s\ ,,,g(\theta)}\rangle$。

再次使用公式(A1)，可知增益 $Q^{(\Delta\oplus 1)_X}_{\mu\ g\ \theta\ ,()\ b_\alpha}$ 可表示为

$$Q^{(\Delta\oplus 1)_X}_{\mu,g(\theta),b_\alpha} = \operatorname{Tr}\left[\hat{V}_{b_\alpha}\rho^\mu_{[g(\theta)]}\hat{V}^\dagger_{b_\alpha} L_{(\Delta\oplus 1)_X}\right]. \tag{A9}$$

综上，我们发现，正文中式(13)所给出的半定规划，为 $p^{\text{virtual}}_{\Delta\ n\ s\ ,,,g(\theta)} Y^{(\Delta\oplus 1)_X}_{\Delta\ n\ s\ g\ ,\text{虚拟}\ ,,,(\theta)}$ 提供了上界。

附录 B：当 $g(\theta)$ 得到充分刻画时的有限维半定规划

1. 产额的下界 $Y^Z_{n\ s,,g(\theta)}$

在本附录中，我们展示如何对式（7）给出的半定规划进行有限维松弛，以求得产额 $Y^Z_{n\ 、s、\ g(\theta)}$的下界。为此，我们再次采用 [48, 53]中提出的方法。其核心思想相当简单：我们不考虑无限维状态 $\rho^\mu_{[g\ (\theta)\ ]}$（由式（4给出），而是将该状态投影 $\rho^\mu_{[g\ (\theta)\ ],\ M}$ 到一个最多包含 M 个光子的有限维子空间（见式（16）），然后相应地放松半定规划的原始约束。

我们首先简要介绍一些有助于实现这一目的的结果。第一个结果可直接由希尔伯特空间中的柯西-施瓦茨不等式推出，该不等式允许我们通过状态 σ 和 ρ之间的保真度，将量 $\mathrm{Tr}[\sigma H]$ 和 $\mathrm{Tr}[\rho H]$与 $0 \le H \le \mathbb{I}$联系起来，作为.....的函数，

$$F(\rho,\sigma) = \operatorname{Tr}\left[\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}\right]^2. \tag{B1}$$

特别地，它指出

$$\begin{aligned} & G_-\left(\operatorname{Tr}\left[\rho H\right], F\left(\sigma,\rho\right)\right) \le \operatorname{Tr}[\sigma H] \\ & \le G_+\left(\operatorname{Tr}\left[\rho H\right], F\left(\sigma,\rho\right)\right), \end{aligned} \tag{B2}$$

其中函数 $G_\pm(y,z)$ 定义为

$$G_-(y,z) = \begin{cases} g_-(y,z) & \text{if } y > 1-z \\ 0 & \text{otherwise}, \end{cases} \tag{B3}$$

and

$$G_+(y,z) = \begin{cases} g_+(y,z) & \text{if } y < z \\ 1 & \text{otherwise}, \end{cases} \tag{B4}$$

其中 $g_\pm(y,z) = y+(1-z)(1-2y) \pm 2\sqrt{z(1-z)y(1-y)}$。

我们使用的其余结果，即式（B5）-（B6）-（B7）-（B8），已在 [48, 53, 57]中推导得出。特别地，我们有

$$\begin{aligned} & F\left(\rho^\mu_{[g(\theta)]}, \rho^\mu_{[g(\theta)],M}\right) = \operatorname{Tr}\left[\Pi_M \rho^\mu_{[g(\theta)]}\Pi_M\right] \\ &= \sum_{n=0}^{M} q_{n|s,g(\theta)} := F^{\text{proj}}_{\mu,g(\theta)}, \end{aligned} \tag{B5}$$

其中，系数 $q_{n|s,\ g(\theta)}$ 由式（17）给出。此外，量 $|p_{n|\mu,\ g(\theta)} - q_{n|\mu,\ g(\theta)}|$ 的上界为

$$\begin{aligned} |p_{n|\mu,g(\theta)} - q_{n|\mu,g(\theta)}| &\le 2\sqrt{1 - \operatorname{Tr}\left[\Pi_M \rho^\mu_{[g(\theta)]}\Pi_M\right]} \\ &= 2\sqrt{1 - F^{\text{proj}}_{\mu,g(\theta)}} =: \epsilon_\mu. \end{aligned} \tag{B6}$$

最后，保真度 $F\left(\hat{}P(|\varphi_{n,\ \mu,\ g(\theta)}\rangle), \hat{}P(|\psi_{n,\ \mu,\ g(\theta)}\rangle)\right) = |\langle\varphi_{n,\mu,g(\theta)}|\psi_{n,\mu,g(\theta)}\rangle|^2$ 满足

$$\begin{aligned} F\left(\hat{P}(|\varphi_{n,\mu,g(\theta)}\rangle), \hat{P}(|\psi_{n,\mu,g(\theta)}\rangle)\right) &\ge 1 - \left(\frac{\epsilon_\mu}{\delta_{n,\mu}}\right)^2 \\ &:= F^{\text{vec}}_{n,\mu,g(\theta)}, \end{aligned} \tag{B7}$$

with

$$\begin{aligned} \delta_{0,\mu} &= q_{0|\mu,g(\theta)} - q_{1|\mu,g(\theta)} - \epsilon_\mu \\ \delta_{n,\mu} &= \min\left\{q_{n-1|\mu,g(\theta)} - q_{n|\mu,g(\theta)} - \epsilon_\mu, q_{n|\mu,g(\theta)}\right. \\ &\quad \left. - q_{n+1|\mu,g(\theta)} - \epsilon_\mu\right\}. \end{aligned} \tag{B8}$$

然后，由式（8）-（B2）-（B7）可得

$$\begin{aligned} Y^{Z,\text{L}}_{n,s,g(\theta)} &= \operatorname{Tr}\left[\hat{P}(|\psi_{n,s,g(\theta)}\rangle) J^*_Z\right] \\ &\ge G_-\left(\operatorname{Tr}\left[\hat{P}(|\varphi_{n,s,g(\theta)}\rangle) J^*_Z\right], F^{\text{vec}}_{n,s,g(\theta)}\right), \end{aligned} \tag{B9}$$

其中 J^*_Z 是式（7）中所给出的半定规划的解，并且我们利用了 G_- 关于其第二个自变量递增这一事实。由于 $G_-(y,\ z)$ 关于其第一个自变量递减，因此可以通过求其第一个自变量的下界来得到式（B9）的下界。

由式（B2），我们有

$$\begin{aligned} G_-\left(Q^Z_{\mu,g(\theta)}, F^{\text{proj}}_{\mu,g(\theta)}\right) &\le \operatorname{Tr}\left[\rho^\mu_{[g(\theta)],M} J_Z\right] \\ &\le G_+\left(Q^Z_{\mu,g(\theta)}, F^{\text{proj}}_{\mu,g(\theta)}\right), \end{aligned} \tag{B10}$$

其中算子 J_Z 定义于式（7）中。这里，由于状态 $\rho^\mu_{[g\ (\theta)],\ M}$ 是有限维的，因此计算

$\mathrm{Tr}\left[\rho^{\mu}_{[g(\theta)],M} J_Z\right]$ 可限定在作用于其有限子空间的算子 J_Z 上。综上，通过求解以下有限维半定规划，可以得到 $Y^{Z}_{n,s,g(\theta)}$ 的下界

$$\begin{aligned}\min_{J_Z}\quad & \mathrm{Tr}\left[\hat{P}(|\varphi_{n,s,g(\theta)}\rangle) J_Z\right] \\ \text{s.t.}\quad & G_-\left(Q^{Z}_{\mu,g(\theta)}, F^{\mathrm{proj}}_{\mu,g(\theta)}\right) \le \mathrm{Tr}\left[\rho^{\mu}_{[g(\theta)],M} J_Z\right] \\ & \le G_+\left(Q^{Z}_{\mu,g(\theta)}, F^{\mathrm{proj}}_{\mu,g(\theta)}\right), \quad \forall \mu \in \{s,\nu,\omega\} \\ & 0 \le J_Z \le \mathbb{I}.\end{aligned} \tag{B11}$$

也就是说，我们有

$$\mathrm{Tr}\left[\hat{P}(|\varphi_{n,s,g(\theta)}\rangle) J^{*}_{Z}\right] \ge \mathrm{Tr}\left[\hat{P}(|\varphi_{n,s,g(\theta)}\rangle) J^{**}_{Z}\right], \tag{B12}$$

其中 J^{**}_Z 是式（B11）中半定规划的解，J^{*}_Z 是式（7）的解。这是因为式（B11）中的约束比式（7）中的约束更宽松。

最后，通过将公式（B9）与公式（B12）相结合，我们得到

$$\begin{aligned}Y^{Z,\mathrm{L}}_{n,s,g(\theta)} &\ge G_-\left(\mathrm{Tr}\left[\hat{P}(|\varphi_{n,s,g(\theta)}\rangle) J^{**}_{Z}\right], F^{\mathrm{vec}}_{n,s,g(\theta)}\right) \\ &:= \tilde{Y}^{Z,\mathrm{L}}_{n,s,g(\theta)}.\end{aligned} \tag{B13}$$

下界 $\tilde{Y}^{Z,\mathrm{L}}_{n,s,g(\theta)}$ 是我们在第 VA 节的模拟中所使用的结果。

2. 相位错误率的上界 $e_{n,s,g(\theta)}$

在本附录中，我们展示如何通过使用有限维半定半无限规划来估计 $e_{n,s,g(\theta)}$ 的上界。为此，我们还定义算子

$$M_{\mathrm{ph}} := |0_X\rangle\langle 0_X| \otimes L^{*}_{1_X} + |1_X\rangle\langle 1_X| \otimes L^{*}_{0_X}, \tag{B14}$$

其中 $L^{*}_{(\Delta\oplus 1)_X}$ 表示由式（13）给出的半定规划（SDP）的解，因此

$$\begin{aligned}&\sum_{\Delta=0}^{1} p^{\mathrm{virtual}}_{\Delta,n,s,g(\theta)} Y^{(\Delta\oplus 1)_X,\mathrm{virtual}}_{\Delta,n,s,g(\theta)} \le \sum_{\Delta=0}^{1} \mathrm{Tr}\left[\hat{P}(|\bar{\lambda}^{\mathrm{virtual}}_{\Delta,n,s,g(\theta)}\rangle)\right. \\ &\left.\times L^{*}_{(\Delta\oplus 1)_X}\right] = \mathrm{Tr}\left[\hat{P}(|\Psi^{Z}_{n,s,g(\theta)}\rangle) M_{\mathrm{ph}}\right].\end{aligned} \tag{B15}$$

现在，让我们定义有限维态

$$|\Psi^{Z,M}_{n,s,g(\theta)}\rangle = \frac{1}{\sqrt{2}}\left(|0_Z\rangle_A \hat{V}_{0_Z} + |1_Z\rangle_A \hat{V}_{1_Z}\right)|\varphi_{n,s,g(\theta)}\rangle, \tag{B16}$$

以及未归一化态 $|\bar{\lambda}^{\mathrm{virtual},M}_{\Delta,n,s,g(\theta)}\rangle$ 作为

$$\begin{aligned}|\bar{\lambda}^{\mathrm{virtual},M}_{\Delta,n,s,g(\theta)}\rangle &= {}_A\langle \Delta_X|\Psi^{Z,M}_{n,s,g(\theta)}\rangle \\ &= \frac{1}{2}\left[\hat{V}_{0_Z} + (-1)^{\Delta}\hat{V}_{1_Z}\right]|\varphi_{n,s,g(\theta)}\rangle.\end{aligned} \tag{B17}$$

于是，我们有

$$\begin{aligned}\left|\langle\Psi^{Z,M}_{n,s,g(\theta)}|\Psi^{Z}_{n,s,g(\theta)}\rangle\right|^2 &= \left|\langle\varphi_{n,s,g(\theta)}|\psi_{n,s,g(\theta)}\rangle\right|^2 \\ &\ge F^{\mathrm{vec}}_{n,s,g(\theta)},\end{aligned} \tag{B18}$$

这里我们使用了式（B7）以及事实 $\hat{V}^{\dagger}_{0_Z}\hat{V}_{0_Z} + \hat{V}^{\dagger}_{1_Z}\hat{V}_{1_Z} = \mathbb{I}$。现在，应用式（B2）给出的柯西-施瓦茨约束，并考虑到 $G_+(y,z)$ 关于其第二个自变量是递减函数，我们得到

$$\begin{aligned}&\mathrm{Tr}\left[\hat{P}(|\Psi^{Z}_{n,s,g(\theta)}\rangle) M_{\mathrm{ph}}\right] \le \\ &G_+\left(\mathrm{Tr}\left[\hat{P}(|\Psi^{Z,M}_{n,s,g(\theta)}\rangle) M_{\mathrm{ph}}\right], F^{\mathrm{vec}}_{n,s,g(\theta)}\right).\end{aligned} \tag{B19}$$

重要的是，由于 $G_+(y,z)$ 关于其第一个自变量是递增函数，因此可以通过求其第一个自变量的上界，得到前一个方程的上界。此外，由于状态 $|\Psi^{Z,M}_{n,s,g(\theta)}\rangle$ 是有限维的，因此可以将优化搜索限制在作用于相应有限维子空间的算子 L 上。特别地，我们有

$$\begin{aligned}&\mathrm{Tr}\left[\hat{P}(|\Psi^{Z,M}_{n,s,g(\theta)}\rangle) M_{\mathrm{ph}}\right] = \sum_{\Delta=0}^{1}\mathrm{Tr}\left[\hat{P}(|\bar{\lambda}^{\mathrm{virtual},M}_{\Delta,n,s,g(\theta)}\rangle)\right. \\ &\left.\times L^{*}_{(\Delta\oplus 1)_X}\right] \le \sum_{\Delta=0}^{1}\mathrm{Tr}\left[\hat{P}(|\bar{\lambda}^{\mathrm{virtual},M}_{\Delta,n,s,g(\theta)}\rangle) L^{**}_{(\Delta\oplus 1)_X}\right].\end{aligned} \tag{B20}$$

其中，$L^{**}_{(\Delta\oplus 1)_X}$ 是下文所述有限维半定半无限规划的解。

同样，式（13）中的约束也可以采用附录 B1 中讨论的基本相同的方法予以放宽。由此，我们发现，可以通过求解以下半定规划，得到 $\mathrm{Tr}\left[\hat{P}(|\bar{\lambda}^{\mathrm{virtual},M}_{\Delta,n,s,g(\theta)}\rangle) L_{(\Delta\oplus 1)_X}\right]$ 的一个上界

$$\begin{aligned}\max_{L_{(\Delta\oplus 1)_X}}\quad & \mathrm{Tr}\left[\hat{P}(|\bar{\lambda}^{\mathrm{virtual},M}_{\Delta,n,s,g(\theta)}\rangle) L_{(\Delta\oplus 1)_X}\right] \\ \text{s.t.}\quad & G_-\left(Q^{(\Delta\oplus 1)_X}_{\mu,g(\theta),b_\alpha}, F^{\mathrm{proj}}_{\mu,g(\theta)}\right) \le \mathrm{Tr}\left[\hat{V}_{b_\alpha}\rho^{\mu}_{[g(\theta)],\mathrm{M}}\hat{V}^{\dagger}_{b_\alpha} L_{(\Delta\oplus 1)_X}\right] \le G_+\left(Q^{(\Delta\oplus 1)_X}_{\mu,g(\theta),b_\alpha}, F^{\mathrm{proj}}_{\mu,g(\theta)}\right), \\ & \forall \mu \in \{s,\nu,\omega\}, \forall b \in \{0,1\}, \forall \alpha \in \{Z,X\} \\ & 0 \le L_{(\Delta\oplus 1)_X} \le \mathbb{I},\end{aligned} \tag{B21}$$

其中 $F^{\mathrm{proj}}_{\mu\, g\, \theta,\ ()}$ 由公式（B5）给出。令 $L^{**}_{(\Delta\oplus 1)_X,}$ 表示使该值最大化的算子

由式（B21）给出的半定规划，然后

$$e_{n,s,g(\theta)} \leq \frac{1}{\tilde{Y}^{Z,\mathrm{L}}_{n,s,g(\theta)}} G_{+}\left(\sum_{\Delta=0}^{1}\mathrm{Tr}\left[\hat{P}(|\bar{\lambda}^{\mathrm{virtual},M}_{\Delta,n,s,g(\theta)}\rangle)L^{**}_{(\Delta\oplus 1)_X}\right], F^{\mathrm{vec}}_{n,s,g(\theta)}\right) := \tilde{e}^{\mathrm{U}}_{n,s,g(\theta)}.$$

这是我们在第 VA 节的模拟中所使用的上界。

附录 C：当 $g\ (\theta)$ 被部分刻画时的有限维半定规划

这里，我们考虑第 VB 节研究的情形，即，实际的印刻相位位于某些区间 $\hat{}\theta_k \in [\theta_k - \delta_{\max}, \theta_k + \delta_{\max}]$，其中 $\theta_k = 2\pi k/N$，而 $g\ (\theta)$ 的确切形式未知。

可以如下直接求解这一情形。首先，在每个区间内定义一个包含 p 个离散值的稠密网格，然后针对来自不同区间的这些离散相位的每一种可能组合，基本按照第 VA1 节中的方法进行处理。密钥率将对应于最坏情况，即在所有可能的组合中使其最小的那一种情况。然而，这种方法的主要缺点是，需要求解的半定规划数量会极快增长，即 $\propto p^N$。

相反，我们在此介绍一种更简单的方法，该方法基于对式（B11）-（B21）中所给半定规划的修改版本。具体而言，令 $f(\theta)$ 表示与式（1）给出的理想离散相位随机化情形相关联的概率密度函数，并令 $\rho^{\mu}_{[f\ (\theta)],M}$ 表示将 $\rho^{\mu}_{[f\ (\theta)]}$ 投影到包含至多 M 个光子的子空间后得到的有限维状态。另外，令 $\rho^{\mu}_{[g\ (\theta)]}$表示 Alice 在上述情形中实际发射的状态，即*i.e.*，当 $g(\theta)$被部分表征时。然后，我们可以借助布雷斯距离来界定 $\rho^{\mu}_{[g\ (\theta)]}$ 与$\rho^{\mu}_{[f\ (\theta)],M}$ 之间的保真度，其中布雷斯距离定义为 [58]

$$d_B(\rho,\sigma)^2 = 2[1-\sqrt{F(\rho,\sigma)}], \tag{C1}$$

对于任意状态 ρ 和 σ。该距离满足三角不等式 [58], ，这意味着

$$\begin{aligned}\sqrt{F(\rho^{\mu}_{[g(\theta)]},\rho^{\mu}_{[f(\theta)],M})} &= 1-\frac{1}{2}d_B(\rho^{\mu}_{[g(\theta)]},\rho^{\mu}_{[f(\theta)],M})^2\\ &\geq 1-\frac{1}{2}\Big[d_B(\rho^{\mu}_{[f(\theta)]},\rho^{\mu}_{[f(\theta)],M})\\ &\quad + d_B(\rho^{\mu}_{[g(\theta)]},\rho^{\mu}_{[f(\theta)]})\Big]^2. \end{aligned}\tag{C2}$$

现在我们计算与布雷斯距离 $d_B(\rho^{\mu}_{[f(\theta)]},\rho^{\mu}_{[f(\theta)],M})$ 相对应的保真度，并且

$d_B(\rho^{\mu}_{[g\ (\theta)]},\rho^{\mu}_{[f\ (\theta)]})$ 从而，通过公式 (C1)，我们可以利用公式 (C2) 获得必要的保真度界限。

特别地，根据公式 (B5)，我们有$F(\rho^{\mu}_{[f(\theta)]},\rho^{\mu}_{[f(\theta)],M}) = F\mathrm{proj}_{\mu,f(\theta)}$。另一方面，保真度$F(\rho^{\mu}_{g\ (\theta)}\ \rho^{\mu}_{[f(\theta)]})$可以通过考虑状态 $\rho^{\mu}_{[f\ (\theta)]}$ 和 $\rho^{\mu}_{[g\ (\theta)]}$各自的以下纯化态来计算，

$$\begin{aligned}|\psi^{\mu,N}_{[f(\theta)]}\rangle &= \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}|k\rangle\left|\sqrt{\mu}e^{2\pi ki/N}\right\rangle,\\ |\psi^{\mu,N}_{[g(\theta)]}\rangle &= \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}e^{i\phi_k}|k\rangle\left|\sqrt{\mu}e^{i(2\pi k/N+\delta_k)}\right\rangle.\end{aligned}\tag{C3}$$

因此，我们发现，

$$\begin{aligned}F(\rho^{\mu}_{[g(\theta)]},\rho^{\mu}_{[f(\theta)]}) &\geq |\langle\psi^{\mu,N}_{[f(\theta)]}|\psi^{\mu,N}_{[g(\theta)]}\rangle|^2\\ &= \Big|\sum_{k=0}^{N-1}\frac{1}{N}\langle\sqrt{\mu}e^{2\pi ki/N}|\sqrt{\mu}e^{i(2\pi k/N+\delta_k)}\rangle\Big|^2\\ &\geq \Big|\sum_{k=0}^{N-1}\frac{1}{N}\langle\sqrt{\mu}e^{2\pi ki/N}|\sqrt{\mu}e^{i(2\pi k/N+\delta_{\max})}\rangle\Big|^2\\ &= |\langle\sqrt{\mu}|\sqrt{\mu}e^{i\delta_{\max}}\rangle|^2,\end{aligned}\tag{C4}$$

其中，在第一个不等式中，我们利用了右端的态是左端态的纯化这一事实；在第一个等式中，我们考虑到相位 ϕ_k 在式（C3）中可以选取，使其抵消内积的相位；在第二个不等式中，我们利用了以下事实：$|\delta_k| \leq \delta_{\max}\forall k$。

由于函数 $g(\theta)$ 未知，我们无法获得特征向量$|\varphi_{n,s,[g(\theta)]}\rangle$的$\rho^{s}_{[g(\theta)],M}$ 的精确形式，而这些特征向量是求解相关有限维半定规划所必需的；不过，我们可以利用式（B2）中给出的柯西-施瓦茨约束，得到迹[$\hat{}P(|\varphi_{n,s,[g(\theta)]}\rangle)J_Z$]的下界，其中 $0 \leq J_Z \leq \mathbb{I}$。具体而言，我们有

$$\begin{aligned}&\mathrm{Tr}\left[\hat{P}(|\varphi_{n,s,[g(\theta)]}\rangle)J_Z\right] \geq\\ &G_{-}\left(\mathrm{Tr}\left[\hat{P}(|\varphi_{n,s,[f(\theta)]}\rangle)J_Z\right], F(|\varphi_{n,s,[g(\theta)]}\rangle, |\varphi_{n,s,[f(\theta)]}\rangle)\right),\end{aligned}\tag{C5}$$

其中$|\varphi_{n,s,[f(\theta)]}\rangle$ 是 $\rho^{s}_{[f(\theta)],M}$ 的特征向量，而 $F(|\varphi_{n,s,[g(\theta)]}\rangle, |\varphi_{n,s,[f(\theta)]}\rangle)$ 的值按下文所述通过数值计算得出。

考虑到这些因素，现在可以求得产额 $Y^Z_{n,s,g(\theta)}$ 的下界。为此，我们首先求解

以下优化问题用于寻找使其目标函数最小化的算子 J_z^{**}

$$\begin{aligned}\min_{J_Z}\ & \mathrm{Tr}\left[\hat{P}(|\varphi_{n,s,[f(\theta)]}\rangle)J_Z\right]\\ \text{s.t.}\ & G_-\left(Q^Z_{\mu,g(\theta)},F(\rho^\mu_{[g(\theta)]},\rho^\mu_{[f(\theta)],M})\right)\le \mathrm{Tr}\left[\rho^\mu_{[f(\theta)],M}J_Z\right]\le G_+\left(Q^Z_{\mu,g(\theta)},F(\rho^\mu_{[g(\theta)]},\rho^\mu_{[f(\theta)],M})\right),\\ & 0\le J_Z\le\mathbb{I}.\end{aligned}\tag{C6}$$

根据公式 (C5)，现定义

$$\hat{Y}^{Z,\mathrm{L}}_{n,s,g(\theta)}:=\\ G_-\left(\mathrm{Tr}\left[\hat{P}(|\varphi_{n,s,[f(\theta)]}\rangle)J^{**}_Z\right],F(|\varphi_{n,s,[g(\theta)]}\rangle,|\varphi_{n,s,[f(\theta)]}\rangle)\right).\tag{C7}$$

最后，通过使用附录 B1 中介绍的论证，我们得到 $Y^Z_{n,s,g(\theta)}$ 的下界为

$$Y^Z_{n,s,g(\theta)}\ge G_-\left(\hat{Y}^{Z,\mathrm{L}}_{n,s,g(\theta)},F^{\mathrm{vec}}_{n,s,g(\theta)}\right):=\tilde{Y}^{Z,\mathrm{L}}_{n,s,g(\theta)}.\tag{C8}$$

ˆ 注意，由于我们不知道 θ_k 的哪些取值会产生使密钥率最小的一组状态 $|\varphi_{n,s,[g(\theta)]}\rangle$，因此我们通过数值方法求得最坏情况。为

此，我们通过考察 $\theta_k\pm\delta_{\max}$ 中的稠密网格取值，对每个 k 进行蒙特卡洛模拟，ˆ并找出使式（θ_k）最小的组合（该式包含式（C8）中的保真度C7）。这使我们能够以任意精度求得所需的下界。另请注意，在本节开头提到的直接求解方法中，需要求解的半定规划数量会迅速增长。采用这种方法，我们通过将问题简化为保真度的简单计算，避开了这一问题，从而大幅降低了计算耗时，尽管所得下界可能较松。

关于相位错误率上界的估计，我们遵循附录 B2中所述的相同步骤。为此，我们首先求解以下有限维半定半无限规划，

$$\begin{aligned}\max_{L_{(\Delta\oplus1)_X}}\ & \mathrm{Tr}\left[\hat{P}(|\bar{\lambda}^{\mathrm{virtual},M}_{\Delta,n,s,[f(\theta)]}\rangle)L_{(\Delta\oplus1)_X}\right]\\ \text{s.t.}\ & G_-\left(Q^{(\Delta\oplus1)_X}_{\mu,b_\alpha},F(\rho^\mu_{[g(\theta)]},\rho^\mu_{[f(\theta)],M})\right)\le \mathrm{Tr}\left[\hat{V}_{b_\alpha}\rho^\mu_{[f(\theta)],M}\hat{V}^\dagger_{b_\alpha}L_{(\Delta\oplus1)_X}\right]\le G_+\left(Q^{(\Delta\oplus1)_X}_{\mu,b_\alpha},F(\rho^\mu_{[g(\theta)]},\rho^\mu_{[f(\theta)],M})\right),\\ & 0\le L_{(\Delta\oplus1)_X}\le\mathbb{I},\end{aligned}\tag{C9}$$

其中 $Q^{(\Delta\oplus1)_X}_{\mu\ b_\alpha}$ 表示Bob在Alice 选择强度设置 μ、基 α、比特值 b 时获得结果 $(\Delta\oplus1)_X$ 的观测速率，以及

Bob选择的 X 基。现在，类似于公式（C7），我们定义

$$\hat{e}^{\mathrm{U}}_{n,s,g(\theta)}:=\sum_{\Delta=0}^{1}G_+\left(\mathrm{Tr}\left[\hat{P}(|\bar{\lambda}^{\mathrm{virtual},M}_{\Delta,n,s,[f(\theta)]}\rangle)L^{**}_{(\Delta\oplus1)_X}\right],F(|\bar{\lambda}^{\mathrm{virtual},M}_{\Delta,n,s,[f(\theta)]}\rangle,|\bar{\lambda}^{\mathrm{virtual},M}_{\Delta,n,s,[g(\theta)]}\rangle)\right),\tag{C10}$$

其中，$L^{**}_{(\Delta\oplus1)_X}$ 是方程（C9）的解。由此可得，相位错误率 $e_{n,s,g(\theta)}$ 的上界为

$$e_{n,s,g(\theta)}\le\frac{G_+\left(\hat{e}^{\mathrm{U}}_{n,s,g(\theta)},F^{\mathrm{vec}}_{n,s,g(\theta)}\right)}{\tilde{Y}^{Z,\mathrm{L}}_{n,s,g(\theta)}}:=\tilde{e}^{\mathrm{U}}_{n,s,g(\theta)}.\tag{C11}$$

ˆ 其中，我们再次使用 θ_k 使方程（C11）最大化的组合，以获得相关的上界。

这些界限 $\tilde{Y}^Z_{n,s}$、^{L}、$_{g(\theta)}$ 和 $\tilde{e}^{\mathrm{U}}_{n,s,g(\theta)}$ 用于第VB节所示的模拟中。

如图所示4，较高的 $\delta_{\max}$ 会使参数 N 对密钥率的影响几乎可以忽略不计，正文对此已有解释。

附录 D：基于线性规划的参数估计程序

为求完整起见，本附录总结了 [45], 中提出的参数估计技术，该技术使用线性规划来评估第III节所述协议在完美离散相位随机化情况下的表现。

特别地，鉴于概率密度函数遵循方程，我们将其记为 $f(\theta)$，与前一附录中的记法相同；此外，$N \geq 1$，Alice 发射态的一个纯化可表示为

$$\begin{aligned}|\psi^{\mu,N}_{[f(\theta)]}\rangle &= \sum_{k=0}^{N-1} |k\rangle_A |\sqrt{\mu} e^{2k\pi i/N}\rangle \\ &= \sum_{j=0}^{N-1} |j\rangle_A \left|\beta^\mu_j\right\rangle,\end{aligned} \tag{D1}$$

其中第二个等式对应于施密特分解。注意，在公式（D1）中，我们考虑的是未归一化态；为方便起见，在本附录中我们始终如此处理。这些态 $|j\rangle_A$ 可以解释为具有 N 随机输出的量子硬币，而这些态 $|\beta^\mu_j\rangle$ 表示为

$$|\beta^\mu_j\rangle = \sum_{k=0}^{N-1} e^{-2kj\pi i/N} |e^{2k\pi i/N}\sqrt{\mu}\rangle. \tag{D2}$$

利用公式（2），这些后述状态可改写为

$$\left|\beta^\mu_j\right\rangle = \sum_{l=0}^{\infty} \frac{(\sqrt{\mu})^{lN+j}}{\sqrt{(lN+j)!}} |lN+j\rangle. \tag{D3}$$

事实上，很容易证明，当 N 较大时，$|\beta^\mu_j\rangle$ 会趋近于一个含有 j 个光子的福克态。

如果 Alice 在基 $\{|j\rangle_A\}$ 中测量她的辅助系统 A，其状态为 $|\psi^{\mu,N}_{[f(\theta)]}\rangle$，则她以概率 P^μ_j 得到结果 j，其中概率由以下公式给出。

$$P^\mu_j = \frac{\left\langle \beta^\mu_j \mid \beta^\mu_j \right\rangle}{\sum_{j=0}^{N-1} \left\langle \beta^\mu_j \mid \beta^\mu_j \right\rangle} \tag{D4}$$

$$= \sum_{l=0}^{\infty} \frac{\mu^{lN+j} e^{-\mu}}{(lN+j)!}. \tag{D5}$$

文献 [45] 采用 GLLP 安全性分析 [50]，需要确定 Δ^μ_j 源的基依赖性，这与 X 基和 Z 基中的状态之间的保真度 F^μ_j 密切相关。具体而言，定义如下

$$\Delta^\mu_j = \frac{1 - F^\mu_j}{2Y^Z_{j,\mu,f(\theta)}}, \tag{D6}$$

其中 $Y^Z_{j,\mu,f(\theta)}$ 指的是与在 Z 基中编码的状态 $|\beta^\mu_j\rangle$ 相对应的产额，以及保真度 F^μ_j 可由.....界定

$$F^\mu_j \geq \left| \frac{\sum_{l=0}^{\infty} \frac{\mu^{lN+j}}{(lN+j)!} 2^{-\frac{lN+j}{2}} \left(\cos\frac{lN+j}{4}\pi + \sin\frac{lN+j}{4}\pi\right)}{\sum_{l=0}^{\infty} \frac{\mu^{lN+j}}{(lN+j)!}} \right|. \tag{D7}$$

此外，由于 $\left|\beta^\mu_j\right\rangle \neq \left|\beta^\gamma_j\right\rangle$ 当 $\mu \neq \gamma$ 时，可以将不同强度设置对应的产额和比特错误率联系起来，如下所示 [50]

$$\begin{aligned}&\left|Y_{j,\mu,f(\theta)} - Y_{j,\gamma,f(\theta)}\right| \leq \sqrt{1 - F^2_{\mu\gamma}}, \\ &\left|e^b_{j,\mu,f(\theta)} Y_{j,\mu,f(\theta)} - e^b_{j,\gamma,f(\theta)} Y_{j,\gamma,f(\theta)}\right| \leq \sqrt{1 - F^2_{\mu\gamma}},\end{aligned} \tag{D8}$$

其中 $e^b_{j,\ \mu,\ f(\theta)}$ 表示与状态 $|\beta^\mu_j\rangle$对应的比特错误率，即，Alice 和 Bob 使用相同的基且 Alice 发射状态 $|\beta^\mu_j\rangle$时，两者获得不同结果的概率。另一方面，参数 $F_{\mu\gamma}$定义为

$$F_{\mu\gamma} := \frac{\sum_{l=0}^{\infty} \frac{(\mu\gamma)^{lN/2}}{(lN)!}}{\sqrt{\sum_{l=0}^{\infty} \frac{\mu^{lN}}{(lN)!} \sum_{l=0}^{\infty} \frac{\gamma^{lN}}{(lN)!}}}. \tag{D9}$$

相位错误率$e_{j,\mu,g(\theta)}$ 在 Z 基中，可通过 X 基中的比特错误率$e^b_{j,\mu,g(\theta)}$ 以及基依赖参数 Δ^μ_j 进行上界估计，如下所示[55]

$$\begin{aligned}e_{j,\mu,f(\theta)} \leq\ & e^{b,X}_{j,\mu,f(\theta)} + 4\Delta^\mu_j \left(1 - \Delta^\mu_j\right)\left(1 - 2e^{b,X}_{j,\mu,f(\theta)}\right) \\ &+ 4\left(1 - 2\Delta^\mu_j\right)\sqrt{\Delta^\mu_j\left(1 - \Delta^\mu_j\right) e^{b,X}_{j,\mu,f(\theta)}\left(1 - e^{b,X}_{j,\mu,f(\theta)}\right)},\end{aligned} \tag{D10}$$

其中，我们在比特错误率中加入了上标 X，以强调该错误率指的是 X 基上的比特错误率。

综上，我们有：对在 Z 基中编码的产额 $Y^Z_{j,\ s,\ f(\theta)}$ 的下界，可以通过以下线性规划进行估计

$$\begin{aligned}&\min\ Y^Z_{j,s,f(\theta)} \\ &\text{s.t.}\ \left|Y^Z_{j,\mu,f(\theta)} - Y^Z_{j,\gamma,f(\theta)}\right| \leq \sqrt{1 - F^2_{\mu\gamma}}, \\ &\quad \forall \mu,\gamma \in \{s,\nu,\omega\},\ \mu \neq \gamma, \\ &\quad Q^Z_{\mu,f(\theta)} = \sum_{j=0}^{N-1} P^\mu_j Y^Z_{j,\mu,f(\theta)}, \forall \mu \in \{s,\nu,\omega\}.\end{aligned} \tag{D11}$$

同样，比特错误率的上界 $e^{b,X}_{j,\mu,\ ,g(\theta)}$可以通过以下线性规划计算

$$\begin{aligned}&\max\ \xi^X_{j,s,f(\theta)} \\ &\text{s.t.}\ \left|\xi^X_{j,\mu,f(\theta)} - \xi^X_{j,\gamma,f(\theta)}\right| \leq \sqrt{1 - F^2_{\mu\gamma}}, \\ &\quad \forall \mu,\gamma \in \{s,\nu,\omega\},\ \mu \neq \gamma, \\ &\quad E^X_{\mu,f(\theta)} Q^X_{\mu,f(\theta)} = \sum_{j=0}^{N-1} P^\mu_j \xi^X_{j,\mu,f(\theta)}, \forall \mu \in \{s,\nu,\omega\},\end{aligned} \tag{D12}$$

其中 $\xi^{X}_{j,s,f(\theta)} = e^{b,X}_{j,sf,(\theta)} Y^{X}_{j,s,f(\theta)}$。特别地，令$\xi^{X*}_{j,s,f(\theta)}$ 表示上述线性规划的解，则有

$$e^{b,X}_{j,s,f(\theta)} \leq \frac{\xi^{X*}_{j,s,f(\theta)}}{Y^{X,\mathrm{L}}_{j,s,f(\theta)}} := e^{b,X,\mathrm{U}}_{j,s,f(\theta)}, \tag{D13}$$

其中 $Y^{X,\mathrm{L}}_{j,sf,(\theta)}$ 表示产额的一个下界$Y^{X}_{j,s,f(\theta)}$ 在 X 基中。该量可通过式（D11）给出的线性规划直接计算，方法是将上标 Z 替换为 X。

最后，可通过式 $e_{j,\mu,f(\theta)}$在 Z 基中的相位错误率，利用式（D10）计算，具体方法是将$e^{b,X}_{j,\mu f,(\theta)}$ 替换为其上界，并将 Δ^{μ}_{j} 替换为在式（D6）中将产额的一个下界替换后得到的上界。重要的是，采用这种方法无需投影到有限维子空间。这意味着在计算式（6）给出的密钥率公式时，概率$p^{L}_{n|s,f(\theta)}$ 可直接由式 P^{μ}_{j} （D4）中定义的 P^{μ}_{j} 得到。

[1] F. Xu、X. Ma、Q. Zhang、H.-K.Lo 和J.-W. Pan，使用现实设备实现安全的量子密钥分发，《现代物理评论》92，025002（2020）。[2] S. Pirandola、U.L. Andersen、L. Banchi、M. Berta、D.Bunandar、R.Colbeck、D. Englund、T.Gehring、C. Lupo、C.Ottaviani、 *et al.*，量子密码学进展，《光学与光子学进展》12，1012（2020）。[3] H.-K.Lo、M.Curty和 K. Tamaki，安全的量子密钥分发，《自然·光子学》8，595（2014）。[4] W. K. Wootters 和 W. H. Zurek，单个量子不可克隆，《自然》299，802–803（1982）。[5] G. S. Vernam，用于秘密有线和无线电报通信的密码打印电报系统，《美国电气工程师学会汇刊》XLV，295（1926）。[6] M.Sasaki、M.Fujiwara、H. Ishizuka、W. Klaus、K. Wakui、M. Takeoka、S. Miki、T.Yamashita、Z. Wang、A. Tanaka、 *et al.*，东京量子密钥分发网络中的量子密钥分发现场测试，《光学快报》19，10387（2011）。[7] D. Stucki、M. Legr´e、F.Buntschu、B. Clausen、N. Felber、N. Gisin、L.Henzen、P. Junod、G.Litzistorf、P. Mon *et al.* baron，瑞士量子量子密钥分发网络在现场环境中的长期性能，《新物理学杂志》13，123001（2011）。[8] J.F. Dynes、A. Wonfor、W. W. S.Tam、A. W. Sharpe、R. Takahashi、M.Lucamarini、A. Plews、Z.L.Yuan、A. R.Dixon、J.Cho、 *et al.*，剑桥量子网络，《npj量子信息》5，101（2019）。[9] Y.-A. Chen、Q.Zhang、T.-Y. Chen、W.-Q.Cai、S.-K. Liao、J.Zhang、K.Chen、J. Yin、J.-G. Ren、Z. Chen、*et al.*，跨越4600公里的一体化天地量子通信网络，《自然》589，214（2021）。[10] C.H.Bennett 和 G. Brassard，量子密码学：公钥分发与抛硬币，在 *Proceedings of IEEE International Conference on Computers、 Systems、 and Signal Processing* 1984 175 179 ( )第 – 页。[11] B. Huttner 、 N.Imoto 、 N. Gisin 和 T. Mor，使用相干态的量子密码学，《物理评论A》51，1863（1995）。[12] G. Brassard、N. L¨utkenhaus、T. Mor 和B. C. Sanders，实用量子密码学的局限性，《物理评论快报》85，1330（2000）。[13] W.-Y.Hwang，高损耗条件下的量子密钥分发：迈向全球安全通信，《物理评论快报》91, 057901 (2003). [14] X.-B. Wang，实用量子密码学中击败光子数分离攻击，《物理评论快报》94, 230503 (2005). [15] H.-K. Lo、X. Ma 和 K. Chen，诱骗态量子密钥分发，《物理评论快报》94, 230504 (2005). [16] C. C. W. Lim、M. Curty、N. Walenta、F. Xu 和 H. Zbinden，实用诱骗态量子密钥分发的简明安全界，《物理评论A》89, 022307 2014( ). [17] Y. Zhao、B. Qi、X. Ma、H.-K. Lo 和 L. Qian，基于诱骗态的实验量子密钥分发，《物理评论快报》96, 70502 (2006). [18] D. Rosenberg、J. W. Harrington、P. R. Rice、P. A. Hiskett、C. G. Peterson、R. J. Hughes、A. E. Lita、S. W. Nam 和 J. E. Nordholt，光纤中的长距离诱骗态量子密钥分发，《物理评论快报》98, 10503 (2007). [19] T. Schmitt-Manderbach、H. Weier、M. F¨urst、R. Ursin、F. Tiefenbacher、T. Scheidl、J. Perdigues、Z. Sodnik、C. Kurtsiefer、J. G. Rarity、 *et al.*，在144 km自由空间距离上演示自由空间诱骗态量子密钥分发，《物理评论快报》98, 10504 (2007). [20] Y. Liu、T.-Y. Chen、J. Wang、W.-Q. Cai、X. Wan、L.- K. Chen、J.-H. Wang、S.-B. Liu、H. Liang、L. Yang、*et al.*，利用偏振光子在200 km距离上进行诱骗态量子密钥分发，《光学快报》18, 8587 (2010). [21] B. Fr¨o hlich、M. Lucamarini、J. F. Dynes、L. C. Coman- dar、W. W.-S. Tam、A. Plews、A. W. Sharpe、Z. Yuan 和 A. J. Shields，能够抵御相干攻击的长距离量子密钥分发，《光学》4, 163 (2017). [22] Z. Yuan、A. Murakami、M. Kujiraoka、M. Lucamarini、Y. Tanizawa、H. Sato、A. J. Shields、A. Plews、R. Taka- hashi、K. Doi、 *et al.*，10 Mb/s量子密钥分发，《光波技术杂志》36, 3427 (2018). [23] A. Boaron、G. Boso、D. Rusca、C. Vulliez、C. Autebert、M. Caloz、M. Perrenoud、G. Gras、F. Bussi`eres、M.-J. Li、*et al.*，通过421 km光纤实现安全量子密钥分发，《物理评论快报》121, 190502 (2018). [24] S.-K. Liao、W.-Q. Cai、W.-Y. Liu、L. Zhang、Y. Li、J.-G. Ren、J. Yin、Q. Shen、Y. Cao、Z.-P. Li、 *et al.*，卫星到地面的量子密钥分发，《自然》549, 43 (2017). [25] S.-K. Liao、W.-Q. Cai、J. Handsteiner、B. Liu、J. Yin、L. Zhang、D. Rauch、M. Fink、J.-G. Ren、W.-Y. Liu、

et al.，卫星中继的洲际量子网络，《物理评论快报》120，030501（2018）。[26] P. Sibson、C. Erven、M. Godfrey、S.Miki、T.Yamashita、M. Fujiwara、M. Sasaki、H. Terai、M.G.Tanner、C. M. Natarajan，*et al.*，基于芯片的量子密钥分发，《自然·通讯》8，13984（2017）。[27] D. Bunandar、A. Lentine、C. Lee、H. Cai、C.M. Long、N.Boynton、N. Martinez、C.DeRose、C.Chen、M.Grein，*et al.*，基于硅光子的城域量子密钥分发，《物理评论X》8，021009（2018）。[28] T. K. Para¨ıso、I. DeMarco、T. Roger、D. G. Marangon、J. F.Dynes、M. Lucamarini、Z.Yuan 和 A.J. Shields，无调制器量子密钥分发发射机芯片，《npj量子信息》5，42（2019）。[29] I. D. Marco、R. I. Woodward、G. L. Roberts、T. K. Para{vv9}ıso、T. Roger、M. Sanzaro、M. Lucamarini、Z. Yuan 和 A. J. Shields，多速率、多协议量子密钥分发发射机的实时运行，《光学》8，911（2021）。[30] Id quantique sa，https://www.idquantique.com/。[31] Toshiba europe limited，https://www.global.toshiba/ww/products-solutions/security-ict/qkd.html。[32] Quantumctek co., ltd.，http://www.quantum-info.com/English/。[33] Thinkquantum s.r.l.，https://www.thinkquantum.com。[34] Quantum telecommunications italy s.r.l.，https://www.qticompany.com。[35] Z. L. Yuan、A. W. Sharpe 和 A. J. Shields，使用诱骗脉冲实现无条件安全的单向量子密钥分发，《应用物理快报》90，011118（2007）。[36] A. R. Dixon、Z. L. Yuan、J. F. Dynes、A. W. Sharpe 和 A. J. Shields，具有1 Mbit/s安全密钥速率的吉赫兹诱骗量子密钥分发，《光学快报》16，18790（2008）。[37] Y. Liu、T.-Y. Chen、J. Wang、W.-Q. Cai、X. Wan、L.- K. Chen、J.-H. Wang、S.-B. Liu、H. Liang、L. Yang，*et al.*，利用偏振光子在200 km距离上实现诱骗态量子密钥分发，《光学快报》18，8587（2010）。[38] M. Lucamarini、K. A. Patel、J. F. Dynes、B. Fr¨ohlich、A. W. Sharpe、A. R. Dixon、Z. L. Yuan、R. V. Penty 和 A. J. Shields，具有量化安全性的高效诱骗态量子密钥分发，《光学快报》21，21（2013）。[39] R. Valivarthi、Q. Zhou、C. John、F. Marsili、V. B. Verma、M. D. Shaw、S. W. Nam、D. Oblak 和 W. Tittel，面向量子网络的经济型测量设备无关量子密钥分发系统，《量子科学与技术》2，04LT01（2017）。[40] Z. Yuan、A. Plews、R. Takahashi、K. Doi、W. Tam、A. Sharpe、A. Dixon、E. Lavelle、J. Dynes、A. Murakami，*et al.*，10 Mb/s量子密钥分发，《光波技术杂志》36，3427（2018）。[41] Y. Zhao、B. Qi 和 H.-K. Lo，采用主动相位随机化的实验性量子密钥分发，《应用物理快报》90，044106（2007）。[42] S.-H. Sun 和 L.-M. Liang，主动相位随机化及监测模块的实验证明，用于量子密钥分发，《应用物理快报》101, 071107 (2012)。[43] P.Sibson, C. Erven, M. Godfrey, S.Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M.G.Tanner,C. M.Natarajan，*et al.*，基于芯片的量子密钥分发，《自然·通讯》8,13984 (2017)。[44] D.Bunandar, A. Lentine, C. Lee, H. Cai, C. M. Long, N.Boynton,N.Martinez,C.DeRose,C.Chen, M. Grein, *et al.*，基于硅光子学的城域量子密钥分发，《物理评论X》8, 021009 (2018)。[45] Z. Cao,Z. Zhang,H.-K.Lo, and X.Ma，离散相位随机化相干态光源及其在量子密钥分发中的应用，《新物理学杂志》17, 053014 (2015)。[46] G. Curr´as-Lorenzo, L.Wooltorton,and M. Razavi，采用完全离散相位随机化的双场量子密钥分发，《物理评论·应用》15, 014016 (2021)。[47] R. Renner and J.I.Cirac，无限维量子系统的 deFinetti 表示定理及其在量子密码学中的应用，《物理评论快报》102, 110504 (2009)。[48] G. Curr´as-Lorenzo,K.Tamaki,andM.Curty，不完美相位随机化下诱骗态量子密钥分发的安全性，预印本 arXiv:2210.08183 (2022)。[49] H.-K. Lo，从无中获得一些东西，《量子信息与计算》5, 413 (2005)。[50] D. Gottesman, H.-K. Lo, N. L¨utkenhaus,andJ.Preskill，不完美设备下量子密钥分发的安全性，《量子信息与计算》4, 325(2004)。[51] M.Koashi，基于互补性的量子密钥分发简单安全性证明，《新物理学杂志》8,045018(2009)。[52] K.Tamaki, M.Curty,G.Kato,H.-K. Lo,andK. Azuma，采用不完美光源的抗损耗量子密码学，《物理评论A》90, 052314(2014)。[53] S. Nahar, *Decoy-State Quantum Key Distribution with Arbitrary Phase Mixtures and Phase Correlations*，硕士论文，滑铁卢大学 (2022)。[54] T. Upadhyaya, T. Himbeeck, J. Lin, andN.L¨utkenhaus，连续变量和离散变量协议量子密钥分发中的降维，《物理评论X·量子》2, 020325 (2021)。[55] H.-K.Lo andJ.Preskill，使用具有非随机相位的弱相干态进行量子密钥分发的安全性，《量子信息与计算》8, 431(2007)。[56] M. Pereira, G. Kate, A. Mizutani,M.Curty,andK. Tamaki，采用相关光源的量子密钥分发，《科学进展》6,eaaz4487(2020)。[57] A.Winter，量子信道的编码定理与强逆定理，《IEEE信息论汇刊》45, 2481 (1999)。[58] D.Farenick andM. Rahaman，算子代数上的布雷斯压缩信道，《纽约数学杂志》23, 1369–1393 (2017)。