arXiv:2302.04236v2 [quant-ph] 8 Sep 2023

噪声存储模型中的容错不经意传输

Cosmo Lupo, [1,2] James T. Peat, [3] Erika Andersson, [3] 和 Pieter Kok[4]

[1]*Dipartimento Interateneo di Fisica, Politecnico di Bari & Università di Bari*, 70126, *Bari, Italy* [2]*INFN, Sezione di Bari, 70126 Bari, Italy* [3]*SUPA, Institute of Photonics and Quantum Sciences, School of Engineering and Physical Sciences, Heriot-Watt University, EH14 4AS Edinburgh, United Kingdom* [4]*Department of Physics and Astronomy, The University of Sheffield, S3 7RH Sheffield, United Kingdom*（日期：2023年9月11日）

量子密码学的噪声存储模型允许在如下假设下实现信息论安全的双方计算：作弊用户最多只能使用不完美且带有噪声的量子存储器，而诚实用户则完全不需要量子存储器。一般而言，作弊用户的量子存储器噪声越大，不经意传输的实现就越安全；不经意传输是一种可用于实现通用安全双方计算和多方计算的基本协议。对于不经意传输的实验实现，还必须考虑到诚实用户持有的设备也存在损耗和噪声，因此需要进行纠错，以修正这些可信误差。预计后者会降低协议的安全性，因为作弊用户可能将自己隐藏在可信噪声之中。本文利用熵不确定性关系，推导出在存在可信噪声和不可信噪声时不经意传输安全性的紧致界限。我们特别讨论了具有独立噪声和相关噪声的噪声存储与有界存储。

一、引言

双方计算指的是一类问题，其目标是让互不信任的两个用户 Alice 和 Bob 计算一个二元函数 $f(x,y)$，其中 Alice 提供 x，Bob 提供y。通俗地说，如果协议向 Alice 泄露的关于 y 的信息，或向 Bob 泄露的关于 x 的信息，不超过他们从 $f(x,y)$ 的值中所能推断出的信息，那么该协议就是安全的。例如，x和 y是 n位字符串，且 $f(x,y) = x\cdot y$，其中 $\cdot$是模 2 标量积。Alice 和 Bob 都不总是能够从 $f(x,y)$ 以及各自的输入 x 或 y中，同时推断出 x和 y。在一篇影响深远的论文[1]，中，Kilian 证明，安全地执行不经意传输（OT）足以实现双方计算。在 OT 中，Alice 发送两个比特，接收方（Bob）恰好可以读出其中一个，从而无法读出另一个比特。如果 Bob 无法获得关于另一个比特的任何信息，且 Alice 不知道 Bob 得知了哪一个比特，那么该协议就是安全的。具体而言，这称为 1 取 2 不经意传输（1-2 OT）[2]。尽管 OT 有多种不同的形式 [3–5]，，我们在此关注 1 取 2 随机化不经意字符串传输（1-2 随机不经意传输$^\ell$）。其他重要的密码学原语包括比特承诺（BC）和弱字符串擦除（WSE）。OT 和 BC 均可由 WSE 构造得到 [6]。

具备计算安全性的双方计算实现依赖于求解某些数学难题的复杂性，例如整数分解 [1, 6]。量子力学无法帮助实现无条件安全的双方计算 [10, 11]。然而，如果用户的能力受到限制，例如只能使用有限的量子资源，就可以实现信息论安全。这种情况可能出现在用户没有量子存储器 [12–14], 或者他们拥有不完美的量子存储器，只能存储有限数量的量子比特，且存储时间有限 [15, 16], 或保真度不足。对存储容量有限的量子存储器所作的假设称为有界量子存储模型 [5, 17, 18]。一般而言，存储器可能既受容量限制又有噪声，在这种情况下，称为噪声存储模型 [6–9]。文献 [5–9, 17–21] 详细讨论了在噪声存储模型下实现不经意传输、比特承诺和弱串流加密的协议，并进行了实验验证 [22, 23]。一般而言，双方计算的实验实现比量子密钥分发（QKD）要求更高。这主要是因为双方计算的用户彼此不信任，从而限制了他们合作的方式。然而，文献 [5–9, 17–23] 表明，尽管如此，不经意传输和比特承诺等基本功能仍可在噪声存储模型下实现并确保安全。通过引入适当的假设，也可以实现设备无关不经意传输 [24, 25]。否则，若不对用户的资源施加任何限制，双方计算只能实现部分安全。在这种情况下，目标是计算不诚实用户成功欺骗的概率上界，参见例如文献 [26, 27] 及其中的参考文献。

本文分析了噪声存储模型中的不经意传输安全性。我们重点研究 Damg˚ard 等人提出的协议 [5]，，该协议基于与著名的量子密钥分发 BB84 协议相同的基本构件 [28]。在文献 [6, 20], 先前结果的基础上，我们推导出更紧的熵不确定性关系，并以条件最小熵量化不经意传输的安全性。与先前研究相比，我们扩大了能够实现安全不经意传输的实验参数范围，并改进了诚实用户设备引入的可信噪声与作弊用户

的量子存储器中的噪声之间的权衡。我们证明，要实现安全不经意传输，对于噪声较大但无界的量子存储器，整体可信噪声应低于 $\simeq$ 22%；而量子存储器中的噪声越小，这一数值也越低。

本文组织如下。我们首先在第二节回顾文献 [5], 中的1-2随机不经意传输$^{\ell}$ 的实现，包括使其能够抵御损耗和噪声的措施 [7, 8, 11]。第三节讨论该协议在噪声存储模型中的安全性。第四节回顾文献 [5, 6, 20] 中推导出的熵不确定性关系及其在证明不经意传输安全性方面的应用。我们利用这些结果，在第五节得到了新的、更紧的熵界。第六节应用这些新界来刻画抗噪声不经意传输的安全性，并确定可信噪声与不可信噪声之间的权衡。第七节讨论具有相关噪声的量子存储器，并展示在这种情况下新界具有特别明显的优势。最后，第八节给出结论。

II. 不经意传输

本文聚焦于1-2随机不经意传输$^{\ell}$这一任务，即1-出2随机化不经意字符串传输，以及参考文献 [5]中Damg˚ard等人提出的协议。在1-2随机不经意传输$^{\ell}$中，发送方Alice输出两个随机字符串，每个字符串包含 ℓ 比特。接收方Bob仅输出其中一个字符串，该字符串是随机选定的。若满足以下条件，则该任务以安全方式执行：（发送方安全性）Bob几乎无法获得或完全无法获得另一个字符串的信息；（接收方安全性）Alice不知道Bob获得了哪一个字符串。该任务可以使用BB84操作 [5], 来实现：Alice使用两组共轭基随机制备状态，而Bob独立地选择其中一组基进行测量。Bob只选择一个基，并用该基测量所接收到的全部物理比特。

此外，通过加入一层纠错 [7]，该协议可以具备抵抗噪声的能力。在处理双方计算中的纠错时需要格外谨慎，因为与量子密钥分发不同，在这里Alice和Bob并不相互信任。因此，他们无法像在量子密钥分发中那样合作估计通信信道及其设备中的损耗和噪声。

注 1 在双方计算中实施纠错前，需要先充分表征损耗和噪声。这包括通信信道中的错误以及诚实用户所持设备中的错误。

这是一项并非易事的要求。请注意，如果用户利用可信第三方来认证噪声水平，那么他们也可以通过经典协议，利用该可信第三方来实现不经意传输。

鉴于光子学应用，并遵循文献 [7,8, 11], ，将损耗和噪声分别处理是合理的。为应对光子损耗，Alice 和 Bob 首先需要商定一个公共时间基准，以便为 Alice 发送的每个光子添加时间标记。如果 Bob 是诚实的，他会在收到每个光子后立即进行测量，并向 Alice 确认已收到。只有成功传送到 Bob 那里的光子才会实际用于协议。其余所有丢失的光子都将被忽略[36]。Bob 最终探测到的光子，其内部自由度仍可能受到噪声影响。为应对这种噪声，Alice 会发送错误综合征，以便 Bob 进行纠错。

容错协议如下 [7]。

• Alice 随机选择二进制值 $x'_j \in \{0,1\}$ $\theta'_j \in \{0,1\}$ $j = 1\ 2\ \ldots\ n'$ 和，对于，，。

根据约定的时间基准，在第 j个时刻，Alice 制备状态$|x'_j\rangle$并发送给 Bob，$|\theta'_j\rangle = H^{\theta'_j}|x'_j\rangle$，其中 $|x'_j\rangle \in \{|0\rangle, |1\rangle\}$ 是计算基中的一个元素，H 是 Hadamard门。

• Bob 随机选择一个比特值 $B \in \{0,1\}$，并以基 $\{H^B|0\rangle, H^B|1\rangle\}$测量他收到的所有量子比特。

• 由于光子损耗与探测效率低下，部分量子比特被擦除。Bob 会记录未探测到光子的时间，并将此信息告知 Alice。在协议的其余部分中，只保留与探测到的光子相关联的比特值。若探测到 n 个光子，则可确定与 Alice 的二进制值和基选择相关联的子字符串 $X = x_1$、 ..... 、 x_n 和 $\Theta = \theta_1$、 ..... 、 θ_n。在 Bob 一方，他会记录在自己选择的基下测得的比特值 $Y = y_1$、 ..... 、 y_n。

• 总体损耗由衰减因子 $\eta \in$ (0,1) 描述，该因子表示 Bob 探测到光子的概率。如上所述，诚实用户知道该参数的预期值。如果该值与经验损耗因子 n/n' 不相容，或者在统计误差范围内依赖于 Alice 制备的状态，协议就会中止。

• 协议会暂停一段等待时间 Δt，从预期 Bob 收到最后一个光子的时刻开始计算。

•Alice 公布她的基选择。这对应于揭示两个指标子集 $\mathcal{I}_0, \mathcal{I}_1$，其中 $\mathcal{I}_C = \{j \,|\, \theta_j = C\}$。她还公布了一对哈希函数 F_0 和 F_1 ，它们从 n 映射到 ℓ，以及综合征向量 Σ_0 = syn(X_0) 和Σ_1 =syn(X_1)，其中 X_C 是将 X 限制在 $\mathcal{I}_C$中的指标后得到的子字符串。类似地，定义 Bob 的子字符串 Y_0 和 Y_1。这些综合征向量

用于帮助 Bob 纠正其本地字符串中的错误。

- Alice 输出两个由 ℓ 位构成的字符串， $S_0 = F_0(X_0)$ 和 $S_1 = F_1(X_1)$ [29]。
- Bob 使用伴随式 Σ_B 纠正$\tilde{}$中的错误 Y_B ，并取回 X_B。最后，他应用 $\tilde{}$ 相应的哈希函数并输出 $S_B = \sim F_B(X_B)$。

备注 2 请注意等待时间 Δt 的作用。如果 Bob 是诚实的，他会在收到光子后立即进行测量。如果 Bob 不诚实，并将接收的量子比特存储在量子存储器中，那么等待时间将使 Alice 对 Bob 的量子存储器至少已部分退相干有所保证。

备注 3 如果用户都是诚实的，那么该协议能够正确实现 1-2随机不经意传输$^{\ell}$，但纠错失败的概率为 ϵ_{EC}。纠错成功意味着$\sim X_B = X_B$ 和 $S_B = S_B$。

III. 协议的安全性

安全性分析见文献[5, 7]，并基于以下假设：

1. 用户完全了解并掌控自己的设备；

2. 用户可以使用噪声量子存储器。（安全性分析依赖于对量子存储器中的噪声进行建模。下文将使用几种显式模型）；

3. 通信线路中的损耗和噪声，以及诚实用户所持设备中的损耗和噪声，均为公开已知。

假设 1 将此协议置于设备依赖型密码学的框架下。假设 2 是噪声存储模型的核心假设。假设 3 是实现纠错所必需的。此外，在分析安全性时，我们需要考虑只有一名用户在欺骗（Alice 或 Bob），而另一名用户是诚实的，因为该 OT协议旨在保护至少一名诚实用户。当 Alice 欺骗时，接收方安全性针对 Bob；当 Bob 欺骗时，发送方安全性针对 Alice。

接收方安全性源于物理量子比特只从 Alice 传送到 Bob。请注意，Bob 需要确认哪些光子已到达，因此确实有一些信息从 Bob 流向 Alice。然而，如果 Bob 完全控制自己的设备（根据假设 1），并且行为诚实（这里考虑的是 Alice 可能作弊的情况），Alice 就无法利用这些信息猜出 B的值。事实上，Bob 发给 Alice 的数据仅用于确认收到光子，并不传达任何有关其内部自由度的信息。只有当 Bob 的设备遭到入侵时，接收光子的状态信息才可能泄露给 Alice。

发送方安全性依赖于噪声存储假设。参数 ℓ 取决于等待时间 Δt内影响不诚实的鲍勃的量子存储的噪声量。它还取决于可信噪声，因为错误综合征会泄露一些信息。先考虑无需纠错的理想情况（即诚实用户不存在噪声），ℓ 根据剩余哈希引理进行估计，并用平滑最小熵 [30] 表示（所有对数均以 2 为底）

$$\ell \geq H_{\min}^{\epsilon_{\rm s}}(X_{1-B}|\mathcal{F}(Q)\Theta B) - 2\log\frac{1}{\epsilon_{\rm h}} + 1\,, \qquad (1)$$

其中， Q 是存储在存储器中的量子信息，而 $\mathcal{F}$ 是描述存储时间为 Δt时噪声存储的映射。若 ℓ大于零，则可确保不诚实接收方在确定互补字符串 X_{1-B}的值时，所能做的也不过是随机猜测。从定量角度看，字符串仍然未知的概率由平滑参数与哈希参数之和给出，即 $\epsilon_{\rm s}+\epsilon_{\rm h}$。然而，噪声也会影响诚实用户，因此我们需要采用纠错。反过来，这会降低 ℓ的值，因为作弊接收方原则上可以利用伴随式 Σ_{1-B} 获取有关互补比特串的更多信息，

$$\begin{aligned}\ell &\geq H_{\min}^{\epsilon_{\rm s}}(X_{1-B}|\mathcal{F}(Q)\Theta B\Sigma_{1-B}) - 2\log\frac{1}{\epsilon_{\rm h}} + 1 \qquad (2)\\ &\geq H_{\min}^{\epsilon_{\rm s}}(X_{1-B}|\mathcal{F}(Q)\Theta B) - |\Sigma_{1-B}| - 2\log\frac{1}{\epsilon_{\rm h}} + 1\,, \qquad (3)\end{aligned}$$

其中，在第二行中我们应用了链式法则，而 $|\Sigma_{1-B}|$ 是伴随式的比特数。原则上，只要 $\ell > 0$成立，且 $\epsilon_{\rm s} + \epsilon_{\rm h}$ 足够小，就能实现安全性。注意， $\mathcal{F}$（Q）表示在Bob 获得基信息 Θ^n 时，噪声量子存储器中的量子信息。

给定合适的噪声存储模型后，可以计算最小熵和伴随式的长度。下一节将对此进行详细讨论。

备注 4：Alice 需要进行统计检验，以检查经验衰减因子是否与预期值相符。这种检验具有概率性，可能以 ϵ_{test} 的概率失败，这会影响协议的安全参数。

总之，如果协议没有中止，那么它就能以不超过失败概率$\epsilon_{\rm EC}$ 的概率正确实现1-2随机不经意传输$^{\ell}$。该实现能够抵御使用噪声存储的欺骗性接收方，安全性失效的概率不超过 $\epsilon_{\rm s}+\epsilon_{\rm h}+\epsilon_{\rm test}$。

IV. 熵界综述

本节回顾文献中用于证明1-2随机不经意传输 $^{\ell}$ [5, 6, 20]安全性的若干熵不确定性关系，尤其是用于确立发送方安全性的关系。事实上，可以应用熵不确定性关系，为Bob猜测另一字符串时的不确定性给出一个下界。

首先，考虑一个简化的情景，即 Bob 不具备任何量子存储器。因此，他必须在获得量子态后立即对其进行测量。如果协议通过统计检验，我们将关注那些已被标记为已接收的 n 光子。Alice 使用包含两个共轭基的 BB84编码方案，将变量 X 编码到它们的量子态中。经过等待时间 Δt 后，Alice 宣布了她的基选择 Θ。在这一情景中，至关重要的是，当基信息被公布时，Bob 已经完成了对其量子态的测量。例如，这可能是因为 Bob 根本没有量子存储器，或者因为他的量子存储器在等待时间 Δt 后完全退相干。无论哪种情况，都可以预期 Bob 在收到基信息时已经测量了这些状态；也就是说，他没有可依赖的量子侧信息。在这一情景中，以下熵界适用 [5],

$$H_{\min}^{\epsilon}(X|\Theta) \geq \left(\frac{1}{2} - 2\lambda\right) n\,, \tag{4}$$

其中参数 λ 可以在开区间 $(0, 1/2)$ 中选择，使得

$$\epsilon = \exp\left[-\frac{\lambda^2 n}{32(\log(4/\lambda))}\right]. \tag{5}$$

为了让问题更有趣，考虑这样一种情况：作弊接收方在获得基信息后，其量子存储器 Q 中仍存储着 $q = \nu n$ 个尚未测量的量子比特。在这种情况下，我们有

$$\begin{aligned} H_{\min}^{\epsilon}(X|Q\Theta) &\geq H_{\min}^{\epsilon}(X|\Theta) - q && (6)\\ &\geq \left(\frac{1}{2} - 2\lambda\right) n - q && (7)\\ &= \left(\frac{1}{2} - \nu - 2\lambda\right) n\,, && (8)\end{aligned}$$

其中，第一个不等式由链式法则得出。参数 $\nu \in (0,1)$ 表示量子存储率。当 n 趋于无穷时，公式 (8) 中的界在 $\nu < 1/2$ 时是非平凡的，即作弊接收方至多只能存储 [31]个量子比特的一半。

A. 噪声存储

在噪声存储的情况下，存储在量子存储器中的量子比特会部分退化。为了分析此情景下不经意传输的安全性，我们需要为噪声量子存储器指定一个模型，该模型由量子信道 $\mathcal{F}$ 描述。考虑一种量子存储器，其中每个量子比特都受到独立同分布（i.i.d.）噪声的影响。例如，每个量子比特都会经历退极化噪声

$$\rho \to r\rho + (1-r)I/2\,, \tag{9}$$

该过程以概率 $1-r$ 将 ρ 映射为最大混合态，并以概率r使其保持不变。

注意，作弊接收方不知道某个特定量子比特是否已被退极化。然而，如果我们向他提供这一额外信息，就等于降低了其量子存储器中的噪声。反过来，这意味着他对该字符串的不确定性只会减少[6, 32]。平均而言，如果 $q = \nu n$ 个量子比特存储在量子存储器中，其中约有 $r\nu n$ 个可以无噪声地保留，而其余 $(1-r)\nu n$ 个则会被完全退极化。因此，从 (8) 出发，我们得到最小熵的以下下界（当 n 趋于无穷时）：

$$H_{\min}^{\epsilon}(X|\mathcal{F}(Q)\Theta) \geq \left(\frac{1}{2} - r\nu - 2\lambda\right) n\,. \tag{10}$$

当 n 足够大时，只要满足 $r\nu < 1/2$ [31]，这就是一个非平凡界。

利用量子信道传输经典信息的强反演这一概念，可以改进该界 [6, 33]。已知噪声量子存储器由作用于存储在量子存储器中的量子比特的映射 $\mathcal{F}$ 描述，该信道保留（经典）信息的能力可由下式量化：

$$P_{\text{succ}}^{\mathcal{F}}(nR) = \max_{\{\rho_x, D_x\}_x} \frac{1}{2^{nR}} \sum_{x\in\{0,1\}^{nR}} \text{Tr}[D_x \mathcal{F}(\rho_x)]\,, \tag{11}$$

该式表示最大可实现的（平均）猜测概率，其中最大化范围涵盖编码态 ρ_x 和解码 POVM D_x；比特率为每个量子比特 R 比特。K¨onig 等人 [6] 给出的界为

$$H_{\min}^{\epsilon+\epsilon'}(X|\mathcal{F}(Q)\Theta) \geq -\log P_{\text{succ}}^{\mathcal{F}}\left(H_{\min}^{\epsilon}(X|\Theta) - \log\frac{1}{\epsilon'}\right). \tag{12}$$

如果信道 $\mathcal{F} = \mathcal{N}^{\otimes n}$ 是独立同分布的，那么对于任意 $R > C_{\mathcal{N}}$，熵界都可以显式写出，其中 $C_{\mathcal{N}}$ 是信道 $\mathcal{N}$ 的强反演容量；并且，如果已知错误指数 $\gamma(R)$ 满足

$$P_{\text{succ}}^{\mathcal{N}^{\otimes n}}(nR) \leq 2^{-n\gamma(R)}\,. \tag{13}$$

注意，如果强反演存在，那么对于任意 $R > C_{\mathcal{N}}$，均有 $\gamma(R) > 0$。

$\mathcal{N}$ 对于式（9）中的退极化信道，强逆容量为 [33]

$$C_{\mathcal{N}} = 1 - h\left(\frac{1+r}{2}\right) \tag{14}$$

其中

$$h(x) := -x\log x - (1-x)\log(1-x) \tag{15}$$

是二元香农熵，而错误指数为

$$\gamma_r(R) = 1 + \max_{\alpha>1} \frac{(\alpha-1)(R-1) - \log\left[(1+r)^\alpha + (1-r)^\alpha\right]}{\alpha}. \tag{16}$$

由此得到熵界

$$H_{\min}^{\epsilon+\epsilon'}(X|\mathcal{F}(Q)\Theta) \geq n\gamma_r\left(\frac{H_{\min}^{\epsilon}(X|\Theta) - \log(1/\epsilon')}{n}\right). \tag{17}$$

利用公式 (4)，我们得到

$$H_{\min}^{\epsilon+\epsilon'}(X|\mathcal{F}(Q)\Theta) \geq n\gamma_r\left(\frac{1}{2} - 2\lambda - \frac{1}{n}\log\frac{1}{\epsilon'}\right). \tag{18}$$

当 n 足够大时，我们得到渐近熵率的一个界（请注意，该熵率以及本文中计算的所有熵率均以每个接收光子的比特数表示）

$$h_{\min} = \lim_{n\to\infty}\frac{1}{n} H_{\min}^{\epsilon+\epsilon'}(X|\mathcal{F}(Q)\Theta) \geq \gamma_r(1/2), \tag{19}$$

对于所有满足 $C_{\mathcal{N}} < 1/2$ 的 r 值，这是一个非平凡界。

图1展示了退极化信道的渐近熵率 $h_{\min}$ 的比较：该熵率分别由公式 (10)（$\nu = 1$，蓝色虚线）和公式 (19)（橙色实线）计算得出。这表明，对于退极化噪声信道，公式 (19) 通常更紧；但当退极化参数 r 较小时，公式 (10) 更紧，不过两者之间的差距相对较小。

为简单起见，在本文余下的大部分内容中，我们假设 $\nu = 1$。有界存储的一般情形（ν <1）将在第 VI A 节讨论。

B. 任意噪声大小下的不确定性关系

正如我们在退极化信道的情形中所看到的，如果信道的噪声不够大，我们得到的熵界就会变得平凡。这与我们的物理直觉相悖：物理直觉表明，即使噪声相对较弱，也可能抹去至少一部分信息。本节回顾 Dupuis等人得到的一个熵界 [20], ，即使对于低噪声量子存储器，该熵界仍然是非平凡的。

为了明确写出这个熵界，首先考虑类BB84协议的一种纯化：Alice制备 n 份最大纠缠双量子比特态 Ψ，并将每对中的一个量子比特发送给Bob。对这些存储在欺骗者Bob的量子存储器中的状态施加某个噪声信道，得到$2n$量子比特

$$\sigma_{AE} = \mathrm{id}\otimes\mathcal{F}(\Psi^{\otimes n}), \tag{20}$$

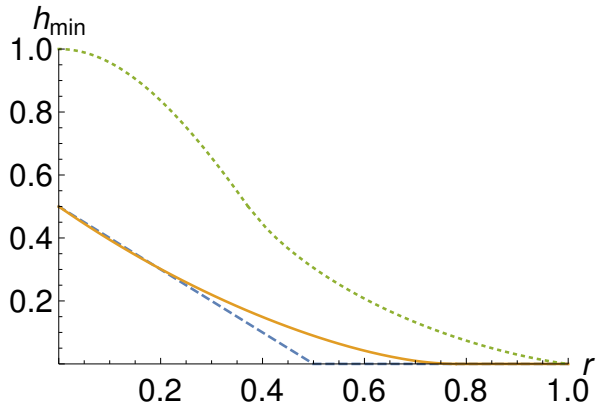


图1：最小熵率与退极化信道参数的关系。蓝色虚线：根据式（10）和 $\nu = 1$ 计算。橙色实线：根据式（19）计算。绿色点线：根据式（29）计算。

其中，id是作用于每对中第一个量子比特的恒等信道。Alice一侧的量子比特统称为 A，量子存储器中存储的量子比特统称为 $E = \mathcal{F}(Q)$。

该熵界用这种状态的碰撞熵率表示：

$$h_2(\sigma) := \frac{1}{n} H_2(A|E)_\sigma. \tag{21}$$

回顾一下，双部态 σ的碰撞熵定义为

$$H_2(A|E)_\sigma = -\log \mathrm{Tr}\left[\left(\sigma_E^{-1/4}\sigma_{AE}\,\sigma_E^{-1/4}\right)^2\right], \tag{22}$$

其中，$\sigma_E = \mathrm{Tr}_A\sigma_{AE}$ 是通过偏迹得到的约化态。

以下最小熵界已在文献 [20] 中得到证明：

$$H_{\min}^{\epsilon}(X|E\Theta) \geq n\Gamma(h_2(\sigma)) - 1 - \log\frac{2}{\epsilon^2}, \tag{23}$$

其中，函数 Γ 定义为

$$\Gamma(x) = \begin{cases} x & \text{if } x \geq 1/2, \\ g^{-1}(x) & \text{if } x < 1/2. \end{cases} \tag{24}$$

and

$$g(y) = -y\log y - (1-y)\log(1-y) + y - 1. \tag{25}$$

如果噪声量子存储器由独立同分布的退极化信道描述，那么状态 σ 是一个直积，即 $\sigma = \tau^{\otimes n}$，其中

$$\tau = r\Psi + (1-r)I/2\otimes I/2, \tag{26}$$

碰撞熵表示为

$$h_2(\sigma) = -\log 2\mathrm{Tr}(\tau^2) = 1 - \log(1+3r^2). \tag{27}$$

这就得到

$$H_{\min}^{\epsilon}(X|\mathcal{F}(Q)\Theta) \geq n\Gamma[1-\log(1+3r^2)] - 1 - \log\frac{2}{\epsilon^2}. \tag{28}$$

注意，至少对于足够大的 n，即使 r 任意接近 1，该界仍然是非平凡的，此时渐近熵率为

$$h_{\min} \geq \Gamma[1-\log(1+3r^2)]. \tag{29}$$

其结果绘于图1（绿色虚线）中，表明后一个界优于前面章节中得到的界。

V. 改进的最小熵界

在本节中，我们利用参考文献 [20] 中的不确定性关系推导出一个新的最小熵界。该论证类似于第 IV A 节中用于得到式（10）的论证。不同之处在于，式（10）由不确定性关系（4）得到，而这里我们以式（23）中的不确定性关系为出发点。为得到该界，我们假设 Bob 接收到的每个量子比特都受到同分布独立噪声的影响。如上所述，这种量子比特噪声被建模为退极化信道。

考虑式（26）中的退极化信道，该信道以 r 的概率保持状态不变，并以 $1-r$ 的概率将其完全退极化。在量子存储器中存储给定量子比特时，欺骗的 Bob 不知道该量子比特是否已被退极化。然而，如果我们向他提供这一额外信息，退极化信道就会被擦除信道所替代：

$$\tau' = r\Psi + (1-r)I/2\otimes\omega, \tag{30}$$

其中，ω 是擦除标志，Bob 可以通过执行非破坏性测量来确定该状态是否已无误存储。给定 n_1 个量子比特已无误保留，且 $n-n_1$ 个量子比特已被擦除，则总体 n 量子比特状态为

$$\sigma' = \Psi^{\otimes n_1}\otimes(I/2\otimes\omega)^{\otimes(n-n_1)}. \tag{31}$$

假设 Bob 获知哪些量子比特已被擦除。记 X^{n_1} 为与未经噪声影响而保留的量子比特对应的比特子串，记 X^{n-n_1} 为与已被擦除的量子比特对应的子串，其中 $X = X^{n_1}X^{n-n_1}$。于是，我们可以写出最小熵的下界：

$$H_{\min}^{\epsilon}(X|E\Theta) \geq H_{\min}^{\epsilon}(X^{n-n_1}|E\Theta) \tag{32}$$

$$\geq (n-n_1)\Gamma(h_2(\sigma'')) - 1 - \log\frac{2}{\epsilon^2}, \tag{33}$$

其中，第一个不等式源于比特串的《熵》总是大于子串的《熵》，第二个不等式则是式（23）的应用

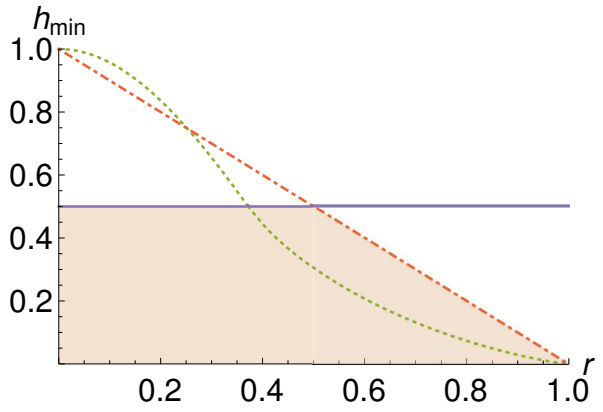


图2：最小熵率与退极化噪声参数的关系。绿色点线：根据式（29）计算（与图1所示相同）。红色点划线：根据式（35）计算。对于 r 的每个取值，最佳熵率通过取两条曲线中的最大值获得，如公式 (36)所示。蓝色实线：诚实接收方的最小熵，根据公式 (4) 在 n较大极限下获得。如果接收方采取理性行为，其熵率始终高于阴影区域。

，且 $\sigma'' = (I/2\otimes\omega)^{\otimes(n-n_1)}$。注意到$h_2(I/2\otimes\omega) = 1$ 以及 $\Gamma(1) = 1$，我们得到

$$H_{\min}^{\epsilon}(X|E\Theta) \geq n - n_1 - 1 - \log\frac{2}{\epsilon^2}. \tag{34}$$

当 n 很大时，预期近乎擦除的量子比特数为 $n-n_1 \simeq (1-r)n$。因此，我们得到渐近最小熵率的下界

$$h_{\min} \geq 1 - r. \tag{35}$$

图2中将这个新的下界与先前的下界一并展示。总之，对于退极化信道，目前得到的熵率最佳下界为

$$h_{\min} \geq \max\{\gamma[1-\log(1+3r^2)], 1-r\}. \tag{36}$$

如图所示，对于较小的 r （噪声较大的量子存储器），最佳下界为 $h_{\min} = \gamma[1-\log(1+3r^2)]$,；而对于较大的 r （噪声较小的量子存储器），最佳下界为 $h_{\min} = 1-r$。

A. 不诚实接收方的最优策略

目前得到的熵界使我们能够根据影响量子存储器的噪声，估算不诚实接收方猜中 Alice 的字符串时所面临的不确定性。回想一下，这里的噪声描述的是 Bob 获得基信息 Θ时，存储在量子存储器中的量子比特的状态。我们假设 Bob 没有诚实行事，因为按照协议，他应在收到量子比特后立即进行测量。方程（36）表明，量子存储器中的噪声越大，不确定性也越大。

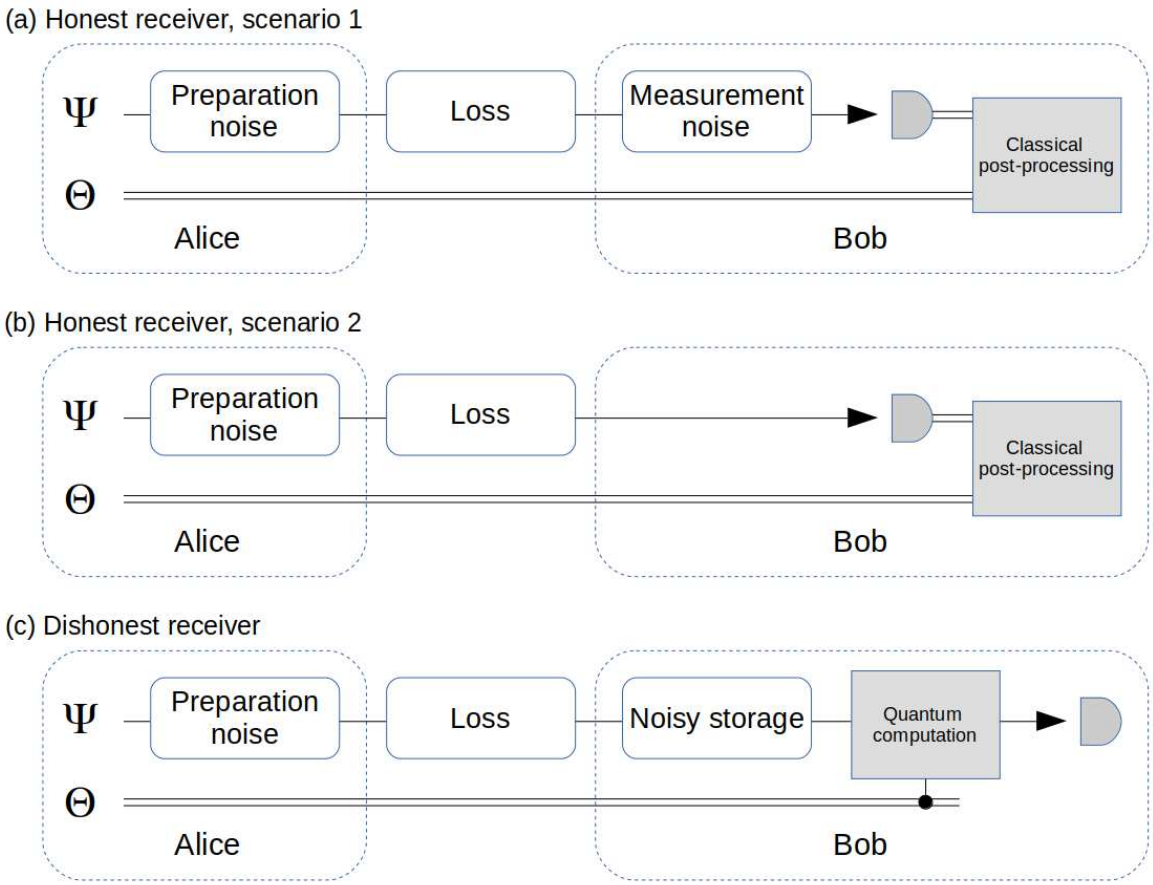


图 3：制备噪声与发送方（Alice）一侧相关。损耗，包括制备阶段中发生的损耗以及由探测器效率低下导致的损耗，都与 Alice 和 Bob 之间的通信信道相关。(a) 在场景1中，诚实接收方 Bob 一拿到量子态就立即使用有噪声的测量装置进行测量。(b) 在场景2中，诚实接收方的测量装置噪声可忽略不计。(c) 作弊接收方将量子态保存在有噪声的量子存储器中，直到从 Alice 那里收到基信息。

最终，如果存储器的噪声过大，犯罪便不再有利可图，采取不诚实行为（即 Bob 等待基公告后再进行测量）也不再是理性选择。

事实上，根据公式 (4)，我们知道诚实接收方的最小熵率为 $h_{\min} \geq 1/2$。因此，当公式 (36) 右侧的值大于 $1/2$ 时，不诚实行为便不再理性。当接收方采取理性行动并采用最佳策略时，熵率为

$$h_{\min} \geq \min\left\{1/2, \max\left\{\gamma[1-\log\left(1+3r^2\right)], 1-r\right\}\right\} \tag{37}$$

$$= \min\left\{1/2, 1-r\right\}. \tag{38}$$

总之，对于理性接收方，熵率始终高于图 2 中的阴影区域。

这一结果确实很直观。诚实的接收方可以无误地测量约 50% 的量子比特，因此，只要量子存储器会破坏超过 50% 的量子比特，诚实行事就是理性的选择。因此，我们预期界 (38) 是紧的，前提是将存储器建模为擦除信道（带有标记），其中 $1-r$ 是擦除量子比特的概率。不过，对于退极化信道，我们预计这一界并不紧，或许还有改进的空间。

VI. 容错 OT

前面各章节中的熵不确定性关系可以直接用于界定接收方 Bob 对字符串 X 的不确定性。不过需要注意的是，在应用于不经意传输时，我们关注的是界定作弊接收方的不确定性；关注的并不是整个字符串 X，而只是子串 X_{1-B}。因此，我们需要像公式 (1) 中那样，给出 X_{1-B} 的最小熵下界。当 n 足够大时，预计子串 X_{1-B} 的大小约为 $n/2$ 位，这些位是从 X 中随机抽样得到的。根据参考文献 [6]，中讨论的最小熵抽样，随机选取子串的最小熵率与 X 相同，只要 n 足够大

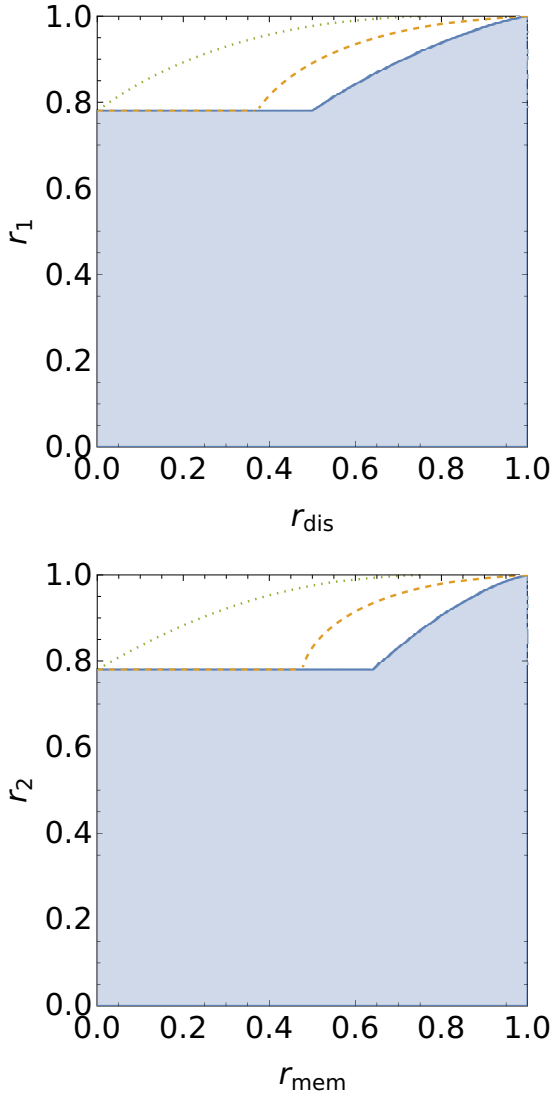


图 4：上：场景1。在 r_{dis}-r_1 平面中，阴影区域以上可以实现安全OT。下：场景2。在 r_{mem}-r_2 平面中，阴影区域以上可以实现安全OT。为了与 [6,20], 中的先前结果进行比较，点状绿色线表示使用式（19）的最小熵界时所得到的安全区域与非安全区域之间的边界 [见式（44）和（47）]。橙色虚线表示由式（29）中的最小熵率得到的边界 [见式（45）和（48）]。

，除有限尺寸修正外。因此，在 n 很大的渐近极限下，我们可以使用前面各章节中得到的最小熵率。为了考虑其设备中的噪声，Alice 和 Bob 还将进行纠错，这会进一步降低最小熵，如公式（3）所示。

我们考虑图 3(a) 和 3(b) 所示的两种情景。在这两种情景中，Alice 的设备在态制备阶段会引入一些噪声，且从 Alice 到 Bob 的传输过程中会发生光子损耗。在场景1中，Bob 的设备存在噪声和损耗，例如由于探测器效率不为 1——这会导致这种情况。在场景2中，Bob 的设备没有噪声，只受到损耗的影响。为简化分析，在这两种情况下，我们都将所有噪声（态制备和测量中的噪声）建模为退极化噪声。此外，态制备和测量过程中的损耗（不失一般性）均归入通信信道。这是合理的，因为损耗与退极化噪声可交换。令 η 表示总衰减因子，涵盖态制备、传输和测量（探测效率不为 1）中的损耗。如上所述，为了处理损耗，Alice 需要知道 η 的期望值；如果实测值与考虑统计涨落后的期望值相差过大，她就会中止协议。

在场景1中，总噪声由两个退极化信道（分别对制备噪声和测量噪声进行建模）合并得到，从而形成一个参数为

$$r_1 = r_{\mathrm{pre}} r_{\mathrm{mea}} \,. \tag{39}$$

场景2的噪声较小，退极化仅由制备阶段引起，

$$r_2 = r_{\mathrm{pre}} \,. \tag{40}$$

这些关系对于两个场景中的诚实接收方均成立。如果接收方不诚实并将量子比特存储在量子存储器中，则从他的角度来看，量子存储器中的噪声会与制备阶段的噪声相结合，如图 3(c)所示。与上文一样，我们将噪声存储建模为参数为 r_{mem}的退极化信道。这意味着，不诚实接收方将经历参数为

$$r_{\mathrm{dis}} = r_{\mathrm{pre}} r_{\mathrm{mem}} \,. \tag{41}$$

注意，$r_{\mathrm{dis}} = r_2 r_{\mathrm{mem}} \leq r_2$，而场景2对诚实用户更有利，因为作弊接收方经历的噪声始终大于诚实接收方经历的噪声。

对于每种情景，每次信道使用所需的纠错信息量渐近等于

$$h_{\mathrm{EC}} = h\left(\frac{1+r_j}{2}\right) , \tag{42}$$

根据所考虑的情景，对 $j = 1$ 而言为 2。由此，我们可以利用公式（3）计算渐近通信速率，单位为每次信道使用的比特数。对于场景1，我们得到

$$b := \lim_{n\to\infty} \ell/n = \min\{1/2, 1 - r_{\mathrm{dis}}\} - h\left(\frac{1+r_1}{2}\right) . \tag{43}$$

图 4（上）展示了比特率的等高线图。当 r_{dis} 和 r_1 的取值位于阴影区域上方时，该协议是安全的。图中还展示了这一结果相较于现有文献的改进。绿色虚线

和橙色虚线分别是根据式（19）和式（29）得到的安全与非安全OT区域之间的边界。具体而言，对于理性接收方，根据式（19）可得比特率

$$\min\left\{1/2,\gamma_{r_{\rm dis}}\left(1/2\right)\right\}-h\left(\frac{1+r_1}{2}\right). \tag{44}$$

同样，由式（29）可得

$$\min\left\{1/2,\Gamma[1-\log\left(1+3r_{\rm dis}^2\right)]\right\}-h\left(\frac{1+r_1}{2}\right). \tag{45}$$

对于场景2，我们可以将 $r_{\rm mem}$ 作为自变量，渐近速率为

$$b=\min\left\{1/2,1-r_2r_{\rm mem}\right\}-h\left(\frac{1+r_2}{2}\right). \tag{46}$$

此界的等高线图如图4（下）所示，在 $r_{\rm mem}$-r_2 平面中，阴影区域上方可实现安全OT。图中还显示了利用式（19）和式（29）中的最小熵界得到的安全OT与非安全OT区域之间的边界。后者由以下比特率计算得出

$$\min\left\{1/2,\gamma_{r_2r_{\rm mem}}\left(1/2\right)\right\}-h\left(\frac{1+r_2}{2}\right), \tag{47}$$

$$\min\left\{1/2,\Gamma[1-\log\left(1+3(r_2r_{\rm mem})^2\right)]\right\}-h\left(\frac{1+r_2}{2}\right). \tag{48}$$

请注意，场景2对诚实用户而言始终更有利，但在这两种情况下，只有当可信噪声参数 r_j 满足 $h((1+r_j)/2)\leq 1/2$，即 $r_j\gtrsim 0.78$ 时，才可能实现安全OT。这对应的最大可容忍可信噪声约为22%。

A. 有界存储

在有噪声且有界的存储情形下，假设作弊接收方至多只能存储一定比例的接收的量子比特，该比例由量子存储率 ν 表示。因此，方程（36）替换为

$$h_{\min}\geq\frac{1-\nu}{2}+\nu\max\left\{\gamma[1-\log\left(1+3r^2\right)],1-r\right\}. \tag{49}$$

对于理性接收方，式（38）替换为

$$\begin{aligned}h_{\min}&\geq\frac{1-\nu}{2} \\ &\quad+\nu\min\left\{1/2,\max\left\{\gamma[1-\log\left(1+3r^2\right)],1-r\right\}\right\} \\ &=\frac{1-\nu}{2}+\nu(1-r)=1/2+\nu(1/2-r).\end{aligned} \tag{50, 51}$$

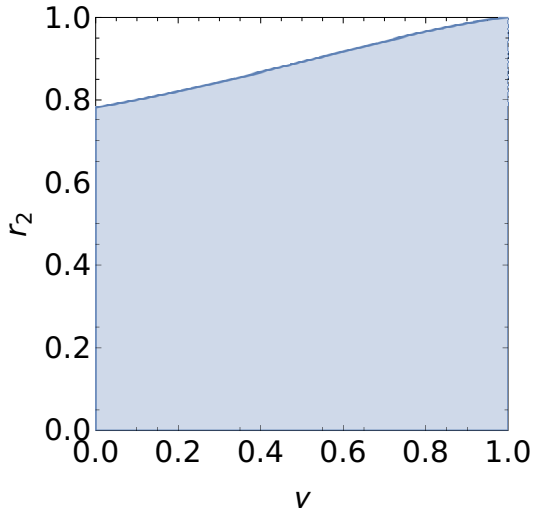


图 5： $r_{\rm mem}=0$下的场景2。这指的是一种无噪声但有界的量子存储器，其存储率为 ν。阴影区域对应于 ν–r_2 平面中协议不安全的区域，其中 r_2 为可信噪声参数。

最后，场景1的渐近速率变为

$$b=\min\left\{1/2,1/2+\nu(1/2-r_{\rm dis})\right\}-h\left(\frac{1+r_1}{2}\right). \tag{52}$$

同样，对于场景2，我们得到

$$b=\min\left\{1/2,1/2+\nu(1/2-r_2r_{\rm mem})\right\}-h\left(\frac{1+r_2}{2}\right). \tag{53}$$

让我们更详细地考虑场景2。对于无噪声但有界的量子存储器，令 $r_{\rm mem}$ =1，比特率变为

$$b=\min\left\{1/2,1/2+\nu(1/2-r_2)\right\}-h\left(\frac{1+r_2}{2}\right). \tag{54}$$

图 5 显示了ν–r_2 平面中比特率消失的区域。当 ν 趋近于零时，我们恢复出 22% 可信噪声的阈值。该阈值会随着 ν的增加而近似线性地降低。

VII. 相关噪声

本节讨论受相关噪声 [34]影响的量子存储器情形。我们考虑一种突发错误模型，其中 $m>1$ 个相邻量子比特同时发生退极化。整数 m 起相关参数的作用。给定 m 份最大纠缠双量子比特态 Ψ，该模型可用映射表示为

$$\Psi^{\otimes m}\to\sigma_{AE}=r\Psi^{\otimes m}+2^{-2m}(1-r)I^{\otimes 2m}, \tag{55}$$

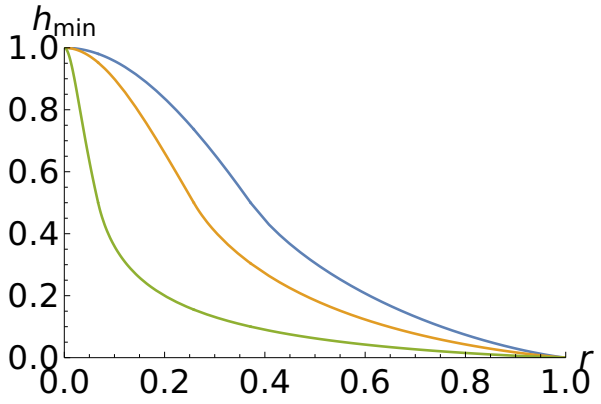


图 6：式 (57) 中的最小熵界随噪声参数 r 的变化曲线。图中展示了相关参数 m 取不同值时的情况。从上到下，这些曲线分别对应 $m = 1$、2、5。

该映射取代式（26）。为了计算式（23）中的界，我们首先需要计算状态σ_{AE}的碰撞熵；结果为

$$h_2 = 1 - \frac{1}{m} \log \left[1 + (2^{2m} - 1)r^2\right] , \tag{56}$$

它将式 (27) 扩展到了任意 $m > 1$。由此我们得到相关噪声量子存储器的最小熵率：

$$h_{\min} \geq \Gamma \left[1 - \frac{1}{m} \log \left[1 + (2^{2m} - 1)r^2\right]\right] . \tag{57}$$

如图 6 所示，该界随 m 增大而降低。

与第五节中的做法一样，我们现在通过引入虚拟擦除信道来改进这个界。这次擦除信道作用于 m 个量子比特。以概率 $(1 - r)$ 擦除一组 m 个相邻量子比特。若发生擦除，我们会得到擦除标志 ω。为了观察该信道对整个 n 个量子比特集合的作用，我们可以将它们分成若干组，每组包含 m 个相邻量子比特。每组以概率 $(1-r)$ 被擦除。总体而言，当 n 很大时，我们预计约有 $n_e = (1-r)n$ 个量子比特被擦除。这对应于 n 量子比特状态

$$\sigma' = \Psi^{\otimes(n-n_e)} \otimes (I/2 \otimes \omega)^{\otimes n_e} \tag{58}$$

$$= \Psi^{\otimes rn} \otimes (I/2 \otimes \omega)^{\otimes(1-r)n} . \tag{59}$$

根据这一状态，我们计算出最小熵率

$$h_{\min} \geq 1 - r , \tag{60}$$

它与 m 无关，且等于独立同分布噪声情形下得到的界。

总之，我们的新界限始终更紧，而且与先前界限之间的差距会随着相关参数 m 的增大而增大。

VIII. 结论

量子力学使得双方计算能够实现信息论安全。然而，与量子密钥分发不同，双方计算并非无条件安全，而是需要对作弊方的能力作出额外假设。特别是，如果接收方 Bob 的量子存储器在容量或质量上受到限制，就可以实现从 Alice 到 Bob 的可证明安全的不经意传输，这种情形称为量子密码学中的噪声存储模型。

不经意传输的实验实现尤其具有挑战性，远比量子密钥分发更具挑战性，因为在双方计算中，用户彼此并不信任。这一点需要特别注意，因为 Alice 和 Bob 无法像在量子密钥分发中那样相互合作，以估计通信信道中的噪声并进行纠错。在双方计算中，诚实用户需要预先了解通信信道及其可信设备的噪声与损耗特性。

直观而言，诚实用户的设备噪声越大，作弊用户就越容易藏身于这种可信噪声之中。这就形成了可信噪声（可信用户设备中的噪声）与不可信噪声（作弊接收方量子存储器中的噪声）之间的权衡。这种权衡最终由用于评估 OT 协议安全性的不确定性关系加以量化。

本文提出了改进的熵不确定性关系，并将其用于刻画可信噪声与量子存储器噪声之间的权衡。我们还指出，如果量子存储器的噪声过大，欺骗就不是理性行为。我们证明，即使量子存储器的噪声任意大但存储容量无界，建模为退极化噪声的可信噪声也不能超过 22%。对于低噪声量子存储器，只有当可信噪声也较低时，才能实现安全OT；如图4所示，此时二者之间的权衡关系有所改善。有限存储的情形也能实现安全OT。

我们讨论了退极化噪声，但我们的结果可直接应用于以下形式的更一般噪声模型

$$\rho \to r\rho + (1 - r)\rho_0 , \tag{61}$$

其中，ρ_0 是一个与 ρ无关的固定点。为使阐述简洁明了，本文聚焦于大量信道使用的渐近极限。不过，我们的方法也可应用于有限规模情形。

致谢

本工作获得了EPSRC量子通信中心（EP/T001011/1）的合作伙伴资源计划以及欧盟地平线欧洲研究与创新计划的资助，资助项目为“量子安全网络合作伙伴关系”（QSNP，资助协议编号101114043）。C.L. ac-

感谢意大利国家复苏与韧性计划意大利大学与研究部项目 PE0000023-NQSTI 提供的资金支持。

[1] J. Kilian，《基于不经意传输建立密码学》，第二十届美国计算机协会计算理论研讨会论文集，第20–31页（1988年）。[2] S. Even、O. Goldreich和A. Lempel，《一种随机化的合同签署协议》，《美国计算机协会通讯》28，637–647（1985年）。[3] M. O. Rabin，《如何通过不经意传输交换秘密》，国际密码学研究协会密码学电子印本档案2005，187（2005年）。[4] G. Brassard和C. Cr´epeau，《不经意传输与隐私放大》，国际密码学理论与应用会议，第334–347页（1997年）。[5] I. B. Damg˚ard、S. Fehr、R. Renner、L. Salvail和C. Schaffner，《具有应用的紧致高阶熵量子不确定性关系》，载于《密码学进展——CRYPTO 2007》，第360–378页（2007年）。完整版本：arXiv:0612014（2006年）。[6] R. K¨onig、S. Wehner和J. Wullschleger，《基于噪声量子存储的无条件安全性》，IEEE信息论汇刊58，1962（2012年）。[7] S. Wehner、C. Schaffner、B. Terhal，《基于噪声存储的密码学》，物理评论快报100，220502（2008年）。[8] C. Schaffner、B. Terhal、S. Wehner，《噪声量子存储模型中的稳健密码学》，《量子信息与计算》9，963（2009年）。[9] C. Schaffner，《噪声量子存储模型中的不经意传输和安全识别简单协议》，物理评论A 82，032308（2010年）。[10] D. Mayers，《无条件安全的量子比特承诺是不可能的》，物理评论快报78，3414（1997年）。[11] H.-K. Lo，《量子安全计算的不安全性》，物理评论A 56，1154（1997年）。[12] H. Buhrman、M. Christandl、P. Hayden、H.-K. Lo和S. Wehner，《量子比特串承诺的可能性、不可能性与作弊敏感性》，物理评论A 78，022316 2008( )。[13] D. P. DiVincenzo、M. Horodecki、D. W. Leung、J. A. Smolin和B. M. Terhal，《量子态中的经典关联锁定》，物理评论快报92，067902（2004年）。[14] S. Guha、P. Hayden、H. Krovi、S. Lloyd、C. Lupo、J. H. Shapiro、M. Takeoka和M. M. Wilde，《量子谜机与量子信道的锁定容量》，《物理评论X》4，011016（2014年）。[15] C. Lupo，《针对具有限时存储的窃听者的安全通信量子数据锁定》，《熵》17，3194（2015年）。[16] Z. Huang、P. P. Rohde、D. W. Berry、P. Kok、J. P. Dowl- ing、C. Lupo，《光子量子数据锁定》，Quantum 5，447（2021年）。[17] I. B. Damg˚ard、S. Fehr、L. Salvail和C. Schaffner，《有界量子存储模型中的密码学》，载于第46届IEEE计算机科学基础研讨会论文集，第449–458页，2005年。ArXiv:0508222（2005年）。[18] I. Damg˚ard、S. Fehr、L. Salvail和C. Schaffner，《有界量子存储模型中的安全识别与量子密钥分发》，CRYPTO 2007，《计算机科学讲义》4622，第342–359页。完整版本 arXiv:0708.2557（2007）。[19] S. Wehner、M. Curty、C. Schaffner 和 H.-K. Lo，《噪声存储模型中双方协议的实现》，物理评论A 81，052336（2010）。[20] F. Dupuis、O. Fawzi、S. Wehner，《纠缠采样及其应用》，电气电子工程师学会信息论汇刊 61，1093（2015）。[21] N. Ng、M. Berta 和 S. Wehner，《有限尺寸密码学的最小熵不确定性关系》，物理评论A 86，042315（2012）。[22] N. H. Y. Ng、S. K. Joshi、C. C. Ming、C. Kurtsiefer 和 S. Wehner，《噪声存储模型中比特承诺的实验实现》，自然·通讯 3，1326（2012）。[23] C. Erven、N. H. Y. Ng、N. Gigov、R. Laflamme、S. Wehner 和 G. Weihs，《噪声存储模型中不经意传输的实验实现》，自然·通讯 5，3418（2014）。[24] Jeremy Ribeiro、Le Phuc Thinh、Jedrzej Kaniewski、Jonas Helsen、Stephanie Wehner，《无记忆设备下双方密码学与位置验证的设备无关性》，物理评论A 97，062307（2018）。[25] A. Broadbent 和 P. Yuen，《基于有界量子存储模型和计算假设的设备无关不经意传输》，arXiv: 2111.08595（2021）。[26] R. Amiri、R. St´arek、D. Reichmuth、I. V. Puthoor、M. Mi˘cuda、L. Mi˘sta, Jr.、M. Du˘sek、P. Wallden 和 E. Andersson，《不完美的 1-out-of-2 量子不经意传输：界、协议及其实验实现》，PRX Quantum 2，010335（2021）。[27] L. Stroh、N. Horov´a、R. St´arek、I. V. Puthoor、M. Mi˘cuda、M. Du˘sek、E. Andersson，《非交互式异或量子不经意传输：最优协议及其实验实现》，PRX Quantum 4，020320（2023）。[28] C. H. Bennett、G. Brassard，《量子密码学：公钥分发与抛硬币》。电气电子工程师学会国际计算机、系统与信号处理会议论文集，印度班加罗尔，1984年12月10日至12日；175，第8页。[29] 请注意， X_0 和 X_1 比 n位短，而哈希函数的输入长度为 n 位，输出长度为 ℓ 位。记号F_C（X_C）隐含表示在 X_C后附加足够数量的 0。[30] M. Tomamichel，《非渐近量子信息论框架》，博士论文，苏黎世瑞士联邦理工学院（ETH Zurich），2012，arXiv:1203.2142（2012）。[31] K¨onig *et al.* [6] 将此界表述为 $1/4$，而非 $1/2$。这是由于 n的定义不同。[32] C. Schaffner，《有界量子存储模型中的密码学》，博士论文，奥胡斯大学，2007。arXiv:0709.0289（2007）。[33] R. K¨onig 和 S. Wehner，《利用纠缠输入进行经典信道编码的强反演》，物理评论快报 103，070504（2009）。[34] F. Caruso、V. Giovannetti、C. Lupo、S. Mancini，《量子

通道与记忆效应》，《现代物理评论》86，1203（2014）。[35] M. Bozzio、A. Cavaill`es、E. Diamanti、A. Kent 和 D. Pital´ua-Garc´ıa，《不信任量子密码中的多光子攻击与侧信道攻击》，PRX Quantum 2，030338（2021）。[36] 这是一项非平凡的假设，因为一般而言，这可能使不诚实接收方更容易作弊：当其未能接收到光子时，声称自己没有收到光子，便能更频繁地以某种方式进行欺骗，也可能让发送方有机可乘：发送更容易或更不容易损耗的脉冲；脉冲是否损耗这一事实，可能会透露它是如何被测量的，或更可能得到什么结果（参见讨论相关问题的文献 [35] ）。本文不考虑这一问题，因为我们假设损耗和噪声已得到充分表征（见第三节）。