arXiv:2601.01058v1 [quant-ph] 3 Jan 2026

I通过经典信道冒充量子秘密

Luowen Qian* Mark Zhandry†

摘要

我们证明，只需有一个简单的窃听者监听潜在纠缠的量子参与方之间的经典通信，最终便能冒充其中任意一方。此外，如果单向谜题不存在，这种攻击就是高效的。直接推论是，对于基于经典信道、使用可能随时间演变的量子预共享秘密的可复用认证方案，单向谜题是其必要条件。

作为另一项应用，我们证明，任何仅通过向任意预言机发起经典查询即可验证的量子货币方案，都不可能达到信息论安全。这显著推广了 Ananth、Hu 和 Yuen（ASIACRYPT'23）先前的工作；他们证明了同样的结论，但仅限于随机预言机这一特定情形。因此，验证量子货币的黑盒构造，本质上需要相干地评估底层密码学工具，而这对于近期的量子设备而言可能很困难。

1 引言

在本文中，我们考虑以下场景：Alice 和 Bob 一开始各自持有大小为多项式规模的秘密量子态，这些量子态可能彼此纠缠。随后，他们通过经典公共信道进行无限期的交互协议。窃听者 Eve 窃听他们的全部通信。Eve 知道该协议，但并不知道 Alice 和 Bob 共享的量子态（至少在最初并不知道）。最终，Eve 将尝试冒充 Alice 与 Bob 通信。事实上，Eve 会试图制备一个可以替换 Alice 的量子态。随后，Alice 和 Bob 再进行几轮交互，只是将 Alice 的量子态替换成 Eve 的量子态；Eve 的目标是让 Bob 无法察觉 Alice 的量子态已被替换，我们称之为冒充 Alice。Bob 的目标则是检测出这次替换。

这种冒充场景很自然，而且正如我们将看到的，它涵盖了一系列有趣的应用。我们的主要结果是，此类协议不可能实现信息论安全。也就是说，在协议中进行足够多轮交互后，计算能力不受限的 Eve 最终能够以除逆多项式概率之外的概率冒充 Alice。我们甚至可以得出更强的结论，即任何以 高效量子对手为防护对象的此类协议，都必然需要密码学假设。更正式地说：

定理 1.1（非正式）。 存在一个（可能效率低下的）*Eve*，在经过足够多次多项式次数的交互后，能够冒充 *Alice*。此外，如果不存在单向谜题，那么 *Eve* 可以在量子多项式时间内运行。

*NTT Research, Inc. luowen.qian@ntt-research.com
†斯坦福大学 & NTT Research, Inc. mzhandry@stanford.edu

单向谜题 [KT24] 是基础性的量子密码学原语。它们被认为是相当温和的假设：例如，单向函数可以推出单向谜题。另一方面，人们认为它们并非最温和的假设，因为量子承诺等概念被认为更加温和。通过查询访问 PP $\subseteq$ PSPACE，可以高效破解单向谜题。

现在我们来说明定理 1.1 的两个看似毫不相关的应用。首先考虑在经典信道上进行重复认证的任务，其中 Alice 和 Bob 的量子密钥可以是任意多项式规模的纠缠量子态。认证次数没有上限。定理 1.1 可直接推出：

推论 1.2 (非正式表述)**.** 如果单向谜题不存在，那么经典信道上的量子认证也不存在。特别是，经典信道上的量子认证不可能达到信息论安全。

对于第二个应用，我们转向公钥量子货币。利用定理 1.1，我们证明，公钥量子货币中的验证者本质上必须对底层密码学构件进行量子查询：

推论 1.3 (非正式表述)**.** 不存在这样一种从任意密码学工具（或工具组合）构造公钥量子货币的黑盒构造：验证者仅对密码学工具进行经典查询。

这显著拓展了 [AHY23]的一项类似成果。他们证明了相同的结论，但仅适用于对称密钥密码学中非常基础的密码学工具。我们的结果彻底解决了关于公钥量子货币的经典查询验证问题。

现在，我们来讨论研究量子认证和量子货币这些概念的一些动机。

1.1 动机

认证与量子密钥分发。量子密钥分发（QKD） [BB14] 使 Alice 和 Bob 能够通过公开信道建立共享秘密密钥。因此，它的作用与经典公钥加密（PKE）类似。然而，值得注意的是，尽管经典 PKE 似乎需要非常强的代数假设，通常形式的 QKD 却完全不需要任何假设。因此，QKD 激发了人们对信息论安全的量子密码协议的浓厚兴趣。

话虽如此，通常即使是量子密码学也需要计算困难性，不过人们希望其弱于经典困难性。例如，与经典密钥交换一样，量子密钥分发仍假设存在经典认证信道。通常可通过公钥基础设施建立此类信道；如果没有（或不愿信任）这样的设置，则可由双方共享一段较短的经典秘密，再用它认证双方交换的经典消息。一种做法是使用计算安全的消息认证码，但只能实现永久安全性；另一种做法是使用密钥回收和信息论消息认证码[MR09, PR14], ，但这种方法需要量子通信，并面临对手发动拒绝服务（DoS）攻击、耗尽秘密随机性的风险。因此，自然会引出这样的问题：能否找到更好的信息论认证方案，或许可以借助量子资源?

我们的量子认证方案可以看作是对经典认证的一种自然推广，适用于最弱但仍有意义的情形，其中：(1) 通信可以是交互式的；(2) Alice 和 Bob 现在可以进行任意的本地量子计算；(3) 他们可以利用会随时间更新的纠缠量子密钥。不失一般性，我们还对设定作了简化：每次认证的都是同一条消息，而这并非易事，因为其中涉及有状态交互。

在这一版本中，即使仅使用经典通信，鉴于相较于经典消息认证码，该协议本身放宽了许多要求，我们也无法事先确定这在信息论意义下是否可行。量子密钥和量子计算的使用意味着，此类认证不再必然蕴含单向函数，并且可以设想其基础假设要温和得多。我们的推论 1.2 表明，任何此类量子认证仍然需要量子通信信道（例如通过密钥回收），或至少需要与单向谜题同等强的计算困难性；即使我们只关注除一轮之外均为被动的攻击，并且这些攻击以高概率成功。

量子计算 + 经典通信协议。近年来，人们对混合经典/量子协议产生了浓厚兴趣：其中通信是经典的，但部分或全部参与方具备本地量子计算能力。一个著名例子是对 [BCM+18]量子性的密码学证明。另一个例子是将 Merkle 谜题改编到量子场景中 [BS08, BHK+19]。最近，人们还开始尝试对这类协议所需的困难性进行下界分析 [ACC+22, LLLL24, AGL25, AKY25]。与本文最相关的工作是[QRZ25] ，其中证明了量子密钥分发（或密钥交换）需要单向谜题或量子通信；我们的第一个应用也将这一结论扩展到了认证场景。

量子货币的障碍。量子货币是不可克隆密码学领域中最基础的密码学原语，该领域利用量子力学的不可克隆性来实现密码学目的。人们早已认识到，要使量子货币实用，它应当支持公开验证：任何人都能验证钞票，但只有铸币机构能够制造钞票。目前已经有若干种此类“公钥”量子货币的构造。

一个根本性问题是，理解实现公钥量子货币需要哪些类型的密码学假设。遗憾的是，目前已知的公钥量子货币构造仅依赖于强大和/或未经检验的计算假设。

Ananth、Hu 和 Yuen[AHY23] 近期的一项工作开启了对量子货币下界的研究，试图为这一现状提供依据。粗略地说，他们证明了以下结论：

定理 1.4 ([AHY23，定理 1], 非正式表述。**不存在基于抗碰撞哈希函数的公钥量子货币“黑盒”构造，其中验证者对哈希函数仅进行经典查询。**

请注意，尽管哈希函数被认为是相对温和的假设——当然远比目前用于构造公钥量子货币的假设温和——定理 1.4 在下界方面取得了显著进展；此前这方面完全没有任何已知结果。

另一方面，定理 1.4 实际上并未排除基于抗碰撞性的任意构造，而只排除了验证者进行经典查询的构造。他们将消除这一限制明确列为一个开放问题，而该问题至今仍未解决。

我们的推论 1.3 并未解决他们提出的开放问题，而是沿着另一个方向对[AHY23] 进行了重大扩展，以处理基于真正任意的 密码学构件的黑盒构造，同时仍保留对经典查询验证者的限制。

对我们结果的一种解读是， [AHY23] 实际上并未对如何从抗碰撞性构建量子货币作出太多论述。相反，它开启了对量子货币中经典查询验证者的研究。依照这种观点，经典查询验证者是他们不可能性结果的主要特点，而其主要局限在于，该结果只适用于基于哈希函数构建的量子货币，而非基于更强构件构建的量子货币。我们的结果完全推广了他们的结果，彻底否定了经典查询验证者存在的可能性。

我们认为，在量子货币中采用经典查询验证者有充分的动机，下面将进一步阐述。一个有别于上述计算难度问题的自然问题是：公钥量子货币方案需要哪些量子资源？具体而言，我们设想，广泛部署的瓶颈在于验证者：铸币机构是中心化的，在不远的将来或许能够拥有构建一台完整容错量子计算机所需的资源，以便制作钞票；但钞票一经分发，就将由普通用户通过手机等相对轻便的设备进行验证。那么，能否构建一种验证所需量子资源较少的公钥量子货币？例如，NISQ 时代设备能否验证公钥量子货币？相比之下，我们已经有了量子密钥分发的实验演示。

值得注意的是，尽管目前所有量子计算机都能运行相对大型的计算任务，却完全无法在叠加态中运行任何经典密码学原语：事实上，许多量子因数分解算法的主要瓶颈在于如何在有限域中相干地乘以两个大数。因此，区分轻量级量子设备与重量级量子设备的一种非常自然的指标，就是它们是否能够相干地运行经典密码学原语。

基于这一区分，刻画 NISQ 验证者的一种有意义的方式，是要求验证者对底层密码学只能进行经典查询。目前还没有任何方案具备这一性质。

基于这一动机和解读，[AHY23] 为近期公钥量子货币设置了初步障碍。随后，我们的工作将 [AHY23] 的结果从抗碰撞性大幅扩展至任何事物，从而彻底解决了量子验证查询这一问题。因此，任何公钥量子货币的实现都必然要求验证者使用能够相干运行密码学工具的量子计算机。尤其是，这表明量子货币验证者很可能需要完整的容错量子计算机。

请注意，我们的推论 1.3 甚至涵盖了本质上属于非黑盒的工具，例如零知识证明或不可区分性混淆（iO）；这些工具可以在其他密码学构造上运行。因此，我们的结果虽然名义上是“黑盒”的，却涵盖了几乎所有密码学技术，甚至包括范围广泛的非黑盒技术。关于这一点的详细讨论，请参见第 6.4 节。

注释 1.5。 我们注意到，关于让铸币机构采用含噪中等规模量子技术，甚至完全采用经典技术这一对偶问题，已有少数研究探讨过。一些协议（例如 *[AC13]* 及后续研究）采用量子铸币器，但铸币机构只对底层密码学工具进行经典查询。更进一步，一些研究 *[RS19, Shm22]* 表明，在适当的密码学假设下，完全采用经典技术的铸币机构实际上是可行的。在下界方面，*[Zha25b]* 展示了公钥量子货币与各种密码学工具之间的黑盒分离，其中铸币机构

受到限制，只能进行经典查询。因此，经典查询铸币机构在文献中更为常见。然而，从资源受限的角度来看，尽量减少验证者所需的量子资源要合理得多。

量子查询的密码学优势。有趣的是，这一结果似乎还为我们提供了一个例子：对预言机进行量子查询，其能力可能在密码学上强于经典查询。回想一下，存在一个经典预言机，相对于该预言机，信息论安全的公钥量子货币存在 [AC13]。然而，我们的结果表明，任何此类方案都必须在验证算法中使用对预言机的量子查询。这说明，正如查询复杂度分离所示 [Sim94，BV97], 对经典函数进行量子叠加访问，也可能在密码学场景中带来更好的安全性。

2 技术概述

2.1 经典直觉

考虑我们设置的经典版本，其中 Alice 和 Bob 共享相关经典字符串。我们将 Alice 的字符串记为 k, 其长度为 n。不失一般性地，我们还假设k 在整个交互过程中始终存在，不过 Alice 也可以另外保留本地动态存储。Alice 和 Bob 随后通过一个信道进行公开对话，窃听者 Eve 可以看到该信道上的内容。Eve 知道协议，但不知道 k。

我们想要证明，Eve 最终将能够冒充 Alice 与 Bob 交互。具体而言，Eve 最终将能够构造出一个密钥 k'；如果用它替换 Alice 的密钥 k，Bob 在数轮交互中将无法察觉。

直观上，对于 Alice 发给 Bob 的每条消息（反之亦然），以下情况之一会发生：

- 在以前消息的条件下，该消息与 k具有显著的相关性。在这种情况下，Alice 发出的消息会透露关于 k的一些信息。
- 在之前消息的条件下，该消息几乎独立于 k。

关键在于，第一种情况只能发生有限次，因为 k 仅包含 n 比特的信息。也就是说，Alice 的熵最终会耗尽，此时她的下一条消息仅由之前的消息决定，并且独立于她的密钥。但在这种情况下，Eve 可以根据截至目前所看到的消息，对 Alice 的密钥条件分布进行采样，k' 将产生与 k大致相同的输出分布。因此，Bob 无法判断 Alice 是否拥有 k 还是 k'。

现在，要精确定义 Eve 冒充 Alice 的含义，需要格外谨慎。首先，k 可能包含一个数值 t，规定 Alice 在前 $t-1$ 条消息中以一种方式行事，而从第 t 条消息起则以另一种方式行事。如果 Eve 试图在第 t条消息处进行冒充，那么无论 k 包含 t 还是 $t+1$，Eve 所看到的信息都将是独立的。但这两种情况会导致 Alice 的行为截然不同，这意味着 Eve 无法正确地冒充 Alice。

另一方面，Alice 的密钥中最多只能大致包含 n 个这样的触发点。Eve 从一个大小远大于 n的集合中随机选择冒充点，便可以避开这些触发点，除非以逆多项式级小概率触发。

更一般地，Eve 只能在短时间内冒充 Alice（因为如果冒充时间过长，她可能会触发另一个触发条件）。但是，Eve 可以让这段时间

变得任意长，只需等待接收更多消息。此外，Eve 的冒充无法达到与 Alice 相比可忽略的误差，但通过更长时间地窃听，可以将误差降至任意小的逆多项式级别。这一结论可以通过谨慎运用经典信息论不等式来证明。

更形式化地说，设 S 是表示 Alice 的秘密 k的随机变量，而 A_1、A_2、... 是发送的消息。直觉中两种情形下的相关性可以用 $I(S; A_i \mid A_{<i})$来刻画，即在给定先前通信记录$A_{<i}$的条件下， S 与最新消息 A_i 之间的互信息。当条件互信息较低时，我们可以借助 Pinsker不等式来论证伪造成功。

2.2 转向量子密钥

转向量子密钥后，整体直觉仍然相同，但情况会变得稍微棘手一些。由于量子力学中的观测者效应，Alice 和 Bob 生成的每条消息都有可能改变他们的状态。事实上，他们的局部状态最终可能具有非常高的熵，而且熵会随着消息数量的增加而增长。由于 Alice 的状态不断扩展，很难论证她的状态最终与新消息之间的条件互信息会很低。事实上，新消息始终可能与她更新后的状态具有最大比特数的条件互信息；例如，Alice 只需在她的状态上交替进行标准基和 Hadamard 基测量，并将测量结果作为消息报告。

为阐明我们的思路，我们从一个简化的信息论任务入手，它抓住了冒充攻击的核心。考虑一个隐藏寄存器 X （以及一个净化环境 E），它经过 n 轮处理。每一轮中，诚实方对 X 施加某个等距映射，然后执行相干测量，得到一个经典结果 Q_i并将其公开给外界，同时保留任何私有工作空间。在这个玩具模型中，我们的目标是证明：在一次足够长、只公开经典交互记录 $Q_1, \ldots, Q_n$ 的交互中，必定存在某一轮 i ，其新泄漏信息 Q_i 所揭示的、关于 E 的信息微乎其微，新 信息也不例外；这些信息是过去的通信记录 $Q_{<i}$中尚未包含的。等价地， Q_i 可以仅根据 $Q_{<i}$ 近似模拟出来。这个简化版本足以证明，Eve 至少可以模拟 Alice 的一条消息。

观察2.1。 给定通信记录 $H(X \mid Q_{\leq i})$ 时，*Alice* 的状态熵绝不会增加；也就是说，测量一个未知的量子态绝不会增加我们对该状态的不确定性。

证明。 令 ρ_0为系统 X上的初始态。在每次迭代 $i = 1, \ldots, n$中，我们从 ρ_{i-1}开始，并执行以下操作以得到 ρ_i:

1. 应用等距映射 $M_{X \to X,\, Q_i}$。 （为方便记号，我们在各轮次中重复使用符号 X 表示这些寄存器；等距映射 M 可能会增加私有寄存器的维数。）2. 应用相干测量等距算子 $CNOT_{Q_i \to Q_i,\, Q_i'}$。

那么对所有 i,

$$
\begin{aligned}
H(X \mid Q_{\leq i-1})_{\rho_{i-1}} &= H(XQ_iQ_i' \mid Q_{<i})_{\rho_i} \\
&\geq H(XQ_i \mid Q_{<i})_{\rho_i} - H(Q_i' \mid Q_{<i})_{\rho_i} \\
&= H(XQ_i \mid Q_{<i})_{\rho_i} - H(Q_i \mid Q_{<i})_{\rho_i} \\
&= H(X \mid Q_{\leq i})_{\rho_i},
\end{aligned}
$$

其中该不等式由 Araki–Lieb不等式（引理 3.1）的第一部分得出。 □

这给出了一串不等式 $H(X)_{\rho_0} \geq H(X \mid Q_1)_{\rho_1} \geq \cdots \geq H(X \mid Q_{\leq n})_{\rho_n} \geq 0$。取第一行和第四行的右端，我们得到：对于每个 n，都存在 $i \leq n$使得

$$H(XQ_iQ_i' \mid Q_{<i})_{\rho_i} - H(X \mid Q_{\leq i})_{\rho_i} \leq H(X)_{\rho_0}/n. \tag{1}$$

现在我们将 X 对应的纯化寄存器 E 考虑在内。具体来说，根据定义，一开始有$H(XE)_{\rho_0} = 0$ 。从 ρ_{i-1} 过渡到 ρ_i时，我们只对 Q_i进行偏迹，因此根据归纳法，对于所有 i ，$H(XE \mid Q_{\leq i})_{\rho_i} = 0$ 也成立。此外， $H(XQ_iQ_i'E \mid Q_{<i})_{\rho_i}$ =$H(XE \mid Q_{<i})_{\rho_{i-1}} = 0$ 也成立。因此，由 (1) 可得，

$$I(E; Q_i \mid Q_{<i})_{\rho_i} = H(E \mid Q_{<i})_{\rho_i} - H(E \mid Q_{\leq i})_{\rho_i} = H(XQ_iQ_i' \mid Q_{<i})_{\rho_i} - H(X \mid Q_{\leq i})_{\rho_i} \leq H(X)_{\rho_0}/n.$$

直观地说，这个不等式表明，最终新的测量结果几乎独立于环境寄存器。因此，无需知道 E，也可以从 $Q_{<i}$ 重现 Q_i 。这一直觉可通过量子 Pinsker 不等式加以形式化。

引理2.2 （量子平克斯克不等式 [HOT81，定理 3.3]）。设 ρ_{XY} 为一个密度矩阵，且 $\sigma_{XY} := \rho_X \otimes \rho_Y$。则 $\|\rho - \sigma\|_1 \leq \sqrt{2 \ln 2 \cdot I(X;Y)_\rho}$。

综合以上结果，我们得到 $\frac{1}{2}\left\|(\rho_i)_{EQ_i} - (\rho_i)_E \otimes (\rho_i)_{Q_i}\right\|_1 \leq \sqrt{\frac{H(X)_{\rho_0}}{2} \frac{\ln 2}{2 \cdot n}}$。这意味着，在迹距离上至多损失 $\sqrt{\frac{H(X)_{\rho_0}}{2} \frac{\ln 2}{2 \cdot n}}$ 的情况下，可以从 $Q_{<i}$ 模拟 Q_i。

推广到一般的冒充任务。要推广到开篇概述的冒充任务，还需要多做一些工作。首先，我们需要处理多轮消息的冒充。其次，我们需要模拟 Alice 的实际状态，而不只是她的消息。为了模拟她的状态，我们从给定目前为止所见消息这一条件下她的状态条件分布中采样。我们需要确保这个伪造的状态仍能产生 Alice 会生成的近似消息分布。一种思路是考察一组消息，并确定条件互信息总量较低的情形。然而，这仍然比较微妙，因为现在 Alice 在收到交换后的状态后可能会生成多条消息；而我们在上文中只论证了第一条消息不会有问题。另一种做法是更新我们的判断，并在每次看到新消息时都伪造一个新状态。

更具挑战性的问题是，我们还需要考虑 Bob 的消息以及 Bob 所持有的那部分状态。Bob 的消息可能会向 Alice 泄露有关她的状态的一些信息，从而使辨别交换后的状态变得更容易。在完整证明中，我们通过精心构造的混合论证来处理所有技术细节。

2.3 应用

推论 1.2 中关于在经典信道上实现信息论量子认证的不可能性，几乎可以直接由我们在定理 1.1 中提出的冒充攻击得出。

为将定理 1.1 应用于推论 1.3 中的量子货币不可能性结果，我们把量子货币验证者视为我们冒充博弈的一个实例：该验证者向底层密码学工具发起经典查询，其中 Alice 是公开验证者，Alice 的状态是

量子钞票，而 Bob 则是银行和密码学工具。窃听者只需观察验证者向预言机发出的查询，就能（仅凭观察这些查询）创建一个可通过验证的新量子钞票状态。由于 Alice 仍持有量子钞票状态，Alice 与窃听者联手便将一张钞票变成了两张，从而破坏了量子货币方案的安全性。

3 预备知识

3.1 符号与约定

安全性与渐近分析。令 $\lambda \in \mathbb{N}$ 表示安全参数。若算法的运行时间关于 λ为多项式，则称其为量子多项式时间（QPT）算法。若对于每个多项式 p，都存在 λ_0，使得对所有 $\lambda \geq \lambda_0$，$\nu(\lambda) < 1/p(\lambda)$，则称函数 $\nu(\lambda)$ 可忽略。全文通常省略安全参数，并将其视为所有函数和算法的隐式输入。

信息度量。所有对数均以 2 为底。对于密度算子 ρ_X，$H(X)_\rho := -\mathrm{Tr}(\rho_X \log \rho_X)$。对于联合状态 ρ_{XY}，（量子）条件熵为 $H(X \mid Y)_\rho := H(XY)_\rho - H(Y)_\rho$。互信息为 $I(X;Y)_\rho := H(X)_\rho + H(Y)_\rho - H(XY)_\rho$，条件互信息为 $I(X;Y \mid Z)_\rho := H(XZ)_\rho + H(YZ)_\rho - H(Z)_\rho - H(XYZ)_\rho$。迹范数为 $\|A\|_1 := \mathrm{Tr}\sqrt{A^\dagger A}$，状态 ρ、σ 之间的迹距离为 $\frac{1}{2}\|\rho - \sigma\|_1$。对于多体态 ρ_{XYZ}，我们用下标表示约化态，例如 $(\rho)_{XY} := \mathrm{Tr}_Z(\rho)$ 和 $\rho_X := \mathrm{Tr}_{YZ}(\rho)$。因此，$\rho_X$ 可能隐含地涉及对除 X以外的所有寄存器取偏迹。

迹距离的数据处理不等式指出，对于任意量子信道 Ψ 以及量子态 ρ、σ、$\|\rho - \sigma\|_1 \geq \|\Psi(\rho) - \Psi(\sigma)\|_1$。

经典条件化。如果 Q 是经典的，我们用 $\rho \mid Q{=}q$（或者在上下文中 Q 明确时用 $\rho \mid q$）表示（归一化的）测量后状态，并将 $Q_{\leq i} := (Q_1, \ldots, Q_i)$ 和$Q_{<i} := (Q_1, \ldots, Q_{i-1})$简记为此。对于经典-量子态，关于 Q 的条件化等价于像上文那样对各个测量结果取平均：$H(X \mid Q)_\rho = \sum_q p_q H(X)_{\rho|q}$，条件互信息也类似。

F或者对于具有形式 $\rho_{XQ} = \sum_q p_q \rho_X^{(q)} \otimes |q\rangle\langle q|$的经典-量子（cq）态，有

$$H(X \mid Q)_\rho = \sum_q p_q H(\rho_X^{(q)}),$$
$$I(X;Y \mid Q)_\rho = \sum_q p_q I(X;Y)_{\rho|Q=q};$$

例如，参见[Wil17，第 11]节。

引理 3.1 (Araki–Lieb不等式 [AL70, (3.1)])。设 ρ_{ABC} 为任意混合态，则 $|H(A)_\rho - H(B)_\rho| \leq H(AB)_\rho \leq H(A)_\rho + H(B)_\rho$。

延迟测量与相干副本。测量计算基观测量并将结果记录在经典寄存器中，可以等价地表示为一个等距映射$|x\rangle \mapsto |x\rangle\,|x\rangle$（例如 CNOT），前提是之后不再使用第二个寄存器。根据延迟测量原理，任何仅以经典方式控制后续计算的测量，都可以假设在最后进行，而不失一般性。

通信信道与预言机访问。 公开认证经典信道可提供完整性，但不提供机密性：对手可以观察所有消息，但不能篡改它们。我们区分经典预言机访问（查询为经典字符串）与量子（叠加）访问，后者由 $|x\rangle|y\rangle \mapsto |x\rangle|y + f(x)\rangle$ 所描述的酉算子实现。

3.2 量子密码学

现在我们来考虑强经典→量子外推任务，它是 [QRZ25] 中定义的经典→量子任务的强化版本。

定义 3.2。 经典→量子外推问题由一个电路 Gen 指定，该电路生成一个纯态，可表示为

$$|\mathsf{Gen}\rangle = \sum_s \alpha_s |s\rangle_A \otimes |\psi_s\rangle_B$$

其中，$\alpha_s \geq 0$ 且 $|\psi_s\rangle$为单位向量。我们称（一个一致族的）Gen 是 p-强困难的，如果对于任意量子多项式时间对手 Adv （可能带有辅助输入），其输出与正确状态 $|\psi_s\rangle$ 的重叠度至多为 p，给定经典部分 s，即

$$\mathbb{E}[\mathrm{Tr}(|\psi_s\rangle\langle\psi_s| \mathsf{Adv}(s))] = \mathrm{Tr}\left(\sum_s \alpha_s^2 |\psi_s\rangle\langle\psi_s| \mathsf{Adv}(s)\right) \leq p$$

对于所有足够大的输入长度。

经典→量子外推问题的强困难性等价于 [KT25] 中定义的 $(1-p)$-弱态谜题；该文还进一步证明了以下结论。

定理 3.3 ([KT25，定理 1。7])。 对于任意与1相差逆多项式有界的 p，当且仅当存在一个 p-强困难的经典→量子外推问题时，单向谜题才存在。

4 我们的主要定理

设定如下。Alice 和 Bob 最初获得一个共享量子态 ρ_0。随后，他们进行一个交互协议 Π。我们将把该协议划分为若干轮，在每一轮中，Alice 向 Bob 发送若干条经典消息 t，并接收 Bob 相应的 t 答复。由于他们可能会测量自己的状态以生成消息，Alice 和 Bob 的状态会持续演变。令 ρ_i 为第 i 条消息之后的状态，那么第 k 轮之后的状态为 ρ_{kt}。令 $(\rho_i)_{\mathcal{A}}$ 为 Alice 持有的那部分状态。令 T_i 为前 i 条消息的通信记录。

冒充攻击。 针对协议 Π的冒充攻击（我们将其称为 Eve）是一种量子算法，它可以查看 Alice 和 Bob 之间传递的经典消息。Eve 不知道初始态 ρ_0。在某个选定的轮次 k （由 Eve 以概率方式选定）之后，Eve 会为 Alice 生成一个伪造量子态 $(\rho'_k)_{\mathcal{A}}$。接着，$(\rho_k)_{\mathcal{A}}$ 被替换为 $(\rho'_k)_{\mathcal{A}}$，Alice 和 Bob 再进行一轮交互。令 T'_{kt+1} 为通信记录，其中包括前 k 轮诚实生成的消息，以及使用 $(\rho'_k)_{\mathcal{A}}$ 生成的第 $k+1$ 轮消息。

我们的定理。 现在给出主要定理：

定理 4.1。 令 n 为 *Alice* 一方所含的量子比特数。令 t 为每轮交换的消息数。令 ϵ 为任意给定的逆多项式概率。则存在一个冒充攻击 *Eve*，使得：

- 被动轮次 k 至多为 $\lceil \frac{2nt}{\epsilon^2 \ln 2} \rceil$；
- 分布 (k, T_{tk+1}) 与 (k, T'_{tk+1}) 之间的统计距离为 ϵ-近似。

此外，如果 *Alice* 和 *Bob* 都是高效的，且不存在单向谜题，那么 *Eve* 也是高效的。

请注意，尽管我们的定理没有考虑任一方的私有量子态，但很容易将其扩展到这种情况：考虑原协议的一个变体，在这些轮次结束时增加一轮通信，由 Alice 或 Bob 运行最优区分器，并将结果发送给另一方。

证明。为建立证明，我们先引入用于描述诚实认证过程的形式化记号。

设 ρ_0 是 Alice 和 Bob 的初始态。通过向 Bob 提供任意一种纯化，我们可以不失一般性地假设 ρ_0 是纯态；这不会影响 Alice 的状态大小。

我们将联合系统 ρ_0 划分为两个寄存器 XY，其中 Alice 持有 X，Bob 持有 Y。此外，Alice 还持有寄存器 Q_1，她将对其进行测量（在计算基下），以获得要发送给 Bob 的第一条经典消息。在每次迭代 $i = 1, 2, \cdots$ 中，我们从 ρ_{i-1} 开始，并执行以下操作以得到 ρ_i：

1. 应用相干测量等距算子 $CNOT_{Q_i \to Q_i,\ Q'_i}$。将该状态记为 α_i。 2. Bob 对 YQ_i 进行测量并应用等距映射 M'（不失一般性地，我们可以假设先将 Q_i 以经典方式复制到 Y），得到更新后的寄存器 Y 和一个经典随机变量 A_i。（同样，我们通过在单独的寄存器 A'_i 中保留该随机变量的标准基副本来表示这个经典随机变量。）将该状态记为 β_i。将 A_i 交给 Alice。 3. Alice 应用等距映射 $M_{XA_i \to X,\ Q_{i+1}}$，其中 A_i 同样仅以经典方式使用。（这一步可以像上面那样展开为两个步骤，但为了分析 X 部分，没有必要这样做。）

我们用 q_i 表示实际发送给 Bob 的经典消息，用 a_i 表示响应。因此，T_i包含 $(q_j, a_j)_{j \le i}$。注意，对所有 i，

$$
\begin{aligned}
H(XQ_i \mid Q_{\le i-1} A_{\le i-1})_{\rho_{i-1}} &= H(XQ_i Q'_i \mid Q_{<i} A_{<i})_{\alpha_i} \\
&\ge H(XQ_i \mid Q_{<i} A_{<i})_{\alpha_i} - H(Q'_i \mid Q_{<i} A_{<i})_{\alpha_i} \\
&= H(XQ_i \mid Q_{<i} A_{<i})_{\alpha_i} - H(Q_i \mid Q_{<i} A_{<i})_{\alpha_i} \\
&= H(X \mid Q_{\le i} A_{<i})_{\alpha_i} \\
&= H(X \mid Q_{\le i} A_{<i})_{\beta_i} \\
&\ge H(X \mid Q_{\le i} A_{\le i})_{\beta_i} \\
&= H(XQ_{i+1} \mid Q_{\le i} A_{\le i})_{\rho_i}.
\end{aligned}
$$

第一个不等式根据 Araki–Lieb（引理 3.1）得出，第二个不等式则是因为对额外的经典变量 A_i 进行条件化不会增加条件熵。同样，我们可以对上述链中的单轮递减量取平均，从而得到一个下降幅度较小的指标 i，这与技术概述中的简化情形相同。具体而言，对于每个 i，差值

$$H(XQ_iQ_i' \mid Q_{<i}A_{<i})_{\alpha_i} - H(X \mid Q_{\le i}A_{<i})_{\alpha_i} = H(XQ_i \mid Q_{\le i-1}A_{\le i-1})_{\rho_{i-1}} - H(X \mid Q_{\le i}A_{<i})_{\alpha_i}$$

不超过每轮实际下降量 $H(X \mid Q_{\le i-1}A_{\le i-1})_{\rho_{i-1}} - H(X \mid Q_{\le i}A_{\le i})_{\beta_i}$，而这些下降量在 $i = 1, 2, \ldots$ 上形成望远镜求和，至多为 $H(X)_{\rho_0} \le n$。因此，我们得到

$$\sum_i H(XQ_iQ_i' \mid Q_{<i}A_{<i})_{\alpha_i} - H(X \mid Q_{\le i}A_{<i})_{\alpha_i} \le H(X)_{\rho_0} \le n. \tag{2}$$

和之前一样，现在我们将 Y 视为 X 的一个纯化“环境”，并以迄今为止揭示的经典交互记录为条件。事实上，ρ_0 在 XYQ_1 上是纯态，而且我们使用的每个操作，要么通过等距映射复制经典寄存器（即生成 Q_i' 的 CNOT），要么测量到一个明确记录下来的经典寄存器中（Bob 的 A_i），因此，以 $Q_{<i}$，$A_{<i}$ 为条件后，XYQ_iQ_i' 上的联合状态仍为纯态。因此，
$H(Y \mid Q_{<i}A_{<i})_{\alpha_i} = H(XQ_iQ_i' \mid Q_{<i}A_{<i})_{\alpha_i}$ 和 $H(Y \mid Q_{\le i}A_{<i})_{\alpha_i} = H(X \mid Q_{\le i}A_{<i})_{\alpha_i}$，式 (2) 变为

$$\begin{aligned}\sum_i I(Y; Q_i \mid Q_{<i}A_{<i})_{\alpha_i} &= \sum_i H(Y \mid Q_{<i}A_{<i})_{\alpha_i} - H(Y \mid Q_{\le i}A_{<i})_{\alpha_i} \\ &= \sum_i H(XQ_iQ_i' \mid Q_{<i}A_{<i})_{\alpha_i} - H(X \mid Q_{\le i}A_{<i})_{\alpha_i} \\ &\le H(X)_{\rho_0} \le n.\end{aligned}$$

直观地说，由于这些条件互信息之和受初始熵$H(X)_{\rho_0}$限制，大多数增量必然很小；特别是，存在一个指标使得 $I(Y; Q_i \mid Q_{<i}A_{<i})$很小。根据量子 Pinsker 不等式（应用于给定通信记录的条件状态），对于这样的指标，新的结果 Q_i 在给定 $(Q_{<i}, A_{<i})$的情况下几乎独立于环境 Y，因此可以根据 $Q_{<i}$模拟 Q_i。

注意，X、Q_i 与 Y、A_i 的作用是对称的。因此，类似的论证也可以得出

$$\sum_i I(X; A_i \mid Q_{\le i}A_{<i})_{\alpha_i} \le H(Y)_{\rho_0} = H(X)_{\rho_0} \le n.$$

现在，我们考虑如下冒充算法 Eve。Eve 为$\ln 2$选择一个随机的 $k \leftarrow [K]^{K \ge \frac{2nt}{\epsilon^2}}$，同时记录经典查询通信记录。

看到前 k 轮的通信记录 T_{kt} 后，伪造算法会准备状态为 $\rho_{kt} \mid T_{kt}$的寄存器XQ_{kt+1}。这一步是唯一可能效率低下的步骤。由于这恰好对应一个经典量子外推问题，如果不存在单向谜题，那么整个攻击就是高效的。

引理 4.2. 真实通信记录与伪造算法针对其所选轮次生成的通信记录之间的迹距离至多为 $\sqrt{\frac{2t \cdot H(X)_{\rho_0}}{K} \ln 2} \le \sqrt{\frac{2tn}{K} \ln 2}$。

证明。 我们首先通过平克斯克不等式和经典条件化，将可模拟性保证形式化。对于每一步 i，以及每个固定的记录前缀 $(q_{<i}, a_{<i})$，定义

$$\Delta_i^Y(q_{<i}, a_{<i}) := \tfrac{1}{2}\left\|(\alpha_i)_{YQ_i|q_{<i},a_{<i}} - (\alpha_i)_{Y|q_{<i},a_{<i}} \otimes (\alpha_i)_{Q_i|q_{<i},a_{<i}}\right\|_1,$$

类似地

$$\Delta_i^X(q_{\le i}, a_{<i}) := \tfrac{1}{2}\left\|(\beta_i)_{XA_i|q_{\le i},a_{<i}} - (\beta_i)_{X|q_{\le i},a_{<i}} \otimes (\beta_i)_{A_i|q_{\le i},a_{<i}}\right\|_1.$$

对每个固定的通信记录应用量子平克斯克不等式，可得

$$\Delta_i^Y(q_{<i}, a_{<i}) \le \sqrt{\tfrac{1}{2\ln 2} I(Y; Q_i \mid q_{<i}, a_{<i})_{\alpha_i}}, \qquad \Delta_i^X(q_{\le i}, a_{<i}) \le \sqrt{\tfrac{1}{2\ln 2} I(X; A_i \mid q_{\le i}, a_{<i})_{\beta_i}}.$$

对经典交互记录取平均，并利用詹森不等式（平方根函数的凹性），可得

$$\mathbb{E}[\Delta_i^Y] \le \sqrt{\tfrac{1}{2\ln 2} I(Y; Q_i \mid Q_{<i}A_{<i})_{\alpha_i}}, \qquad \mathbb{E}[\Delta_i^X] \le \sqrt{\tfrac{1}{2\ln 2} I(X; A_i \mid Q_{\le i}A_{<i})_{\beta_i}}.$$

对一次运行中以 k 为索引的 t 步求和（即 $i = kt+1$、…、$kt+t$），并应用柯西–施瓦茨不等式，

$$\mathbb{E}\left[\sum_{i=kt+1}^{kt+t} \Delta_i^Y\right] \le \sum_{i=kt+1}^{kt+t} \sqrt{\tfrac{1}{2\ln 2} I(Y; Q_i \mid Q_{<i}A_{<i})_{\alpha_i}} \le \sqrt{\frac{t}{2\ln 2}} \sqrt{\sum_{i=kt+1}^{kt+t} I(Y; Q_i \mid Q_{<i}A_{<i})_{\alpha_i}},$$
$$\mathbb{E}\left[\sum_{i=kt+1}^{kt+t} \Delta_i^X\right] \le \sqrt{\frac{t}{2\ln 2} \sum_{i=kt+1}^{kt+t} I(X; A_i \mid Q_{\le i}A_{<i})_{\beta_i}}.$$

进一步对 $k \in [K]$ 的随机选择取平均，并利用界 $\sum_i I(Y; Q_i \mid Q_{<i}A_{<i})_{\alpha_i} \le H(X)_{\rho_0}$ 和 $\sum_i I(X; A_i \mid Q_{\le i}A_{<i})_{\alpha_i} \le H(X)_{\rho_0}$ 以及詹森不等式，可得

$$\mathbb{E}_{k,q,a}\left[\sum_{i=kt+1}^{kt+t} \Delta_i^Y\right] \le \sqrt{\frac{t \cdot H(X)_{\rho_0}}{2\ln 2 \cdot K}}, \qquad \mathbb{E}_{k,q,a}\left[\sum_{i=kt+1}^{kt+t} \Delta_i^X\right] \le \sqrt{\frac{t \cdot H(X)_{\rho_0}}{2\ln 2 \cdot K}}.$$

我们考虑如下混合实验序列 Hyb_0、…、Hyb_t，其中 Hyb_i 定义如下：

1. 我们先运行原始算法，直到步骤 $kt+i$，得到 $q_{kt+1\ldots kt+i}, a_{kt+1\ldots kt+i}$。 2. 我们根据当前通信记录制备一个状态 $\rho_{kt+i} \mid q_{\le kt+i}a_{\le kt+i}$ 的新副本。然后，我们用这个新副本中对应的寄存器替换 XQ_{kt+i+1} 寄存器。3. 最后，我们继续运行算法，得到 $q_{kt+i+1\ldots kt+t}, a_{kt+i+1\ldots kt+t}$。

我们可以看到，真实通信记录对应于 Hyb_t，而伪造算法生成的通信记录对应于 Hyb_0。因此，只需证明对于所有 i，Hyb_i与 Hyb_{i+1} 之间的迹距离都很小。

对于每个 i，我们还考虑一个额外的混合实验 Hyb_i'，在消息 q_{kt+i+1} 之后，我们用一份新鲜的 $\alpha_{kt+i} \mid q_{\le kt+i+1}a_{\le kt+i}$ 副本中依据当前通信记录条件化得到的状态，替换 YA_{kt+i+1} 寄存器。

注意，要界定 Hyb_i 与 Hyb'_i 之间的差异，只需界定测量 q_{kt+i+1} 后这两个状态之间的迹距离；对于 Hyb'_i，则只需界定刷新 Y 寄存器后的迹距离。根据 Δ_i^Y 的定义，这一替换对总迹距离的贡献至多为 Δ^Y_{kt+i+1}，这是由迹距离的数据处理不等式得出的；同理，XA 替换的贡献至多为 Δ^X_{kt+i+1}。对 $i=0$、...、$t-1$ 求和，并利用上文关于 Δ 之和的条件化界，我们得出

$$\tfrac{1}{2}\left\|\mathsf{Hyb}_0-\mathsf{Hyb}_t\right\|_1 \le \mathop{\mathbb{E}}_{k,q,a}\sum_{i=0}^{t-1}\left(\Delta^Y_{kt+i+1}+\Delta^X_{kt+i+1}\right) \le \sqrt{\frac{2t\cdot H(X)_{\rho_0}}{K\ln 2}}.$$

□

将任意 $K \ge \frac{2nt}{\epsilon^2\ln 2}$ 代入引理 4.2，即可得到定理 4.1。 □

5 量子认证下界

定义5.1。 经典信道上的量子认证方案由以下过程组成：

1. 设置阶段：*Alice* 和 *Bob* 最初共享一个联合量子态 $|\mathsf{Init}\rangle_{AB}$。*2.* 认证阶段：*Alice* 和 *Bob* 通过公开认证经典信道（具备完整性但不具备机密性）交互式地交换 t 对经典消息；最后，*Bob* 对认证作出接受或拒绝的决定。该阶段可以重复进行，此时双方会使用上一轮留下的剩余状态运行相同的协议。

如果经过 K 轮认证阶段后，*Bob* 以至少 c 的概率在所有 K 轮中均接受，我们就称该方案具有 K 次完备性 c。

K 次攻击是指恶意方 *Eve* 被动窃听 *Alice* 与 *Bob* 之间的所有经典通信，并与 *Alice* 进行至多 K 轮认证交互，但在某个时刻，*Eve* 需要在 K 轮中的某一轮冒充 *Alice* 向 *Bob* 发信，而无法看到 *Alice* 原本会发送的内容。如果 *Bob* 在该轮接受，则认为攻击成功。如果对于任意 K 次攻击，*Bob* 接受的概率至多为 s，我们就称该方案具有 K 次可靠性 s。

该可靠性定义刻画了信息论设定。在计算设定中，我们转而考虑由 λ 索引的此类方案族；计算可靠性则通过将 Eve 限定为量子多项式时间，并要求可靠性误差在 λ 中可忽略来定义。

定理 4.1 几乎立即推出以下结论：

推论5.2。 如果存在一种在公开认证经典信道上运行、轮数为无界多项式、具有计算可靠性且完备性与1的差可忽略的量子认证方案，那么单向谜题就存在。

证明。 在每次认证结束时，我们让 Bob 发送一个比特，表示他接受还是拒绝。根据完备性，这些比特各自以概率 c 为 1。接着应用定理 4.1，该定理表明，Eve 可以选择某一轮与 Bob 交互，使 Bob 的接受比特以接近 c 的概率为 1。换句话说，Eve 使 Bob 接受了。

□

6 量子货币的应用

6.1 可模拟预言机

经典预言机是一个指数规模的对象，因此通常无法高效地构造或求值。不过，许多预言机都可以模拟。如果对于任意多项式 q 以及任何进行 q 次查询的（可能效率低下的）算法 A，都存在一个量子多项式时间有状态模拟器 S，使得 $|\Pr_{O\leftarrow\mathcal{O}}[A^O()=1]-\Pr[A^S()=1]|$ 可忽略，那么我们就称一个预言机上的分布$\mathcal{O}$ O 可高效模拟。

密码学中用于预言机分离的许多预言机都是可模拟的。例如，随机预言机和置换都是可模拟的 [Zha12, Zha25a]。事实上，密码学中使用的许多预言机都是由随机预言机/置换与其他高效计算构成的，这意味着此类预言机是可高效模拟的。

注 6.1。 就在最近，在完全无关的背景下，数项工作 *[LMW25, DMR25, GGW25]* 展示了某些密码学原语相对于所有可能的“密码”预言机的分离。这些工作同样给出了相对于极其庞大的函数族的分离。请注意，它们所定义的密码预言机是可模拟的（因为这些预言机是查询内部随机预言机的高效函数），而密码预言机和可模拟预言机都只是所有可能预言机的严格子集。因此，我们的预言机族甚至比它们的更广。

6.2 相对于预言机的量子货币，以及具有经典查询的验证者

在此，我们定义相对于预言机的公钥量子货币。为简化符号表示，我们默认所有过程都是安全参数的函数，但不显式标出安全参数。该定义大体遵循 [AHY23], ，但由于它在重要方面不同于量子货币的标准定义，我们先讨论这一新定义的动机。

预言机。我们将考虑相对于从分布 $\mathcal{O}$ 中 O 抽取的预言机定义的方案。所有参与方，包括量子货币方案的算法和对手，都可以向 O 发起查询。

迷你方案。 为简化起见，我们只考虑量子货币的“迷你方案”。粗略地说，可以将其视为量子货币的一种版本：铸币机构只会创建一张钞票，而对手看到这张钞票后，试图创建两张钞票。迷你方案简化了讨论；特别是，迷你方案的不可能性意味着完整方案的不可能性。因此，就我们的目的而言，仅考虑迷你方案反而会使我们的结果更强。反过来，利用数字签名 [AC13], 可以将迷你方案扩展为完整方案，而数字签名又可以由任意单向函数构建。尽管通常尚不清楚单向函数与量子货币之间的确切关系，但我们注意到，我们预计大多数具有密码学实用价值的经典预言机都能提供单向函数。由于我们将考虑利用此类预言机的方案，因此在我们所考虑的环境中，迷你方案应当被视为与完整方案基本等价。

经典查询验证者与正确性。 在量子货币的典型定义中，只要铸币机构生成的有效钞票能够通过验证，就认为该方案是正确的。具体而言，该定义只要求钞票第一次验证通过。但人们可能会担心，验证钞票实际上会将其摧毁，这将使量子货币方案相当无用。幸运的是，在量子货币的通常设定中，标准的一次性正确性概念实际上意味着钞票在验证过程中会得到保留，尤其是后续验证也将通过。这是因为正确性要求以压倒性概率通过验证，而温和测量引理 [Win99, Aar05]表明，可以以对状态影响可忽略的方式执行此类测量。

然而，在我们的设定中，我们无法应用温和测量来得到多次正确性。这是因为我们要求验证者只能向预言机进行经典查询，而这需要测量量子货币状态以获得查询。应用温和测量会使这一过程变成相干过程，这意味着验证者不再只进行经典查询。

因此，遵循 [AHY23], ，我们直接在正确性定义中规定：经典查询验证者对于任意多项式次数的验证，都会继续接受该状态。这意味着，尽管验证可能会改变状态，受扰动的钞票仍能通过验证。

注释 6.2. 多次正确性确实是量子货币"正确"的正确性概念，因为我们希望能够多次验证钞票。它之所以在文献中并不常见，唯一的原因是，对于任意验证者而言，较简单的单次定义就足以满足要求。

注释 6.3. 多次正确性对我们的结果至关重要，例如， *[AC13]* 的验证可以改为只进行经典查询。因此，存在一个预言机，相对于该预言机，存在一种由经典查询验证者验证且满足单次正确性的量子货币。问题在于，在这种验证者验证后得到的状态无法通过第二次验证。如果对这个修改后的验证者应用温和测量，得到的验证者又会进行量子查询。

多次正确性对于 *[AHY23]* 的技术同样至关重要。不过需要注意的是，即使是仅具备一次正确性的量子货币，也可能无法基于抗碰撞性构造[1]。

现在给出定义。

定义 6.4 （量子货币，语法）。 一个带预言机辅助的公钥量子货币方案是由一对量子多项式时间预言机算法 $\Pi^O = (\mathsf{Gen}^O、\mathsf{Ver}^O)$ 组成，其中：

- $\mathsf{Gen}^O()$ 生成一个公钥 pk 和一个量子态 $\$$。
- $\mathsf{Ver}^O(\mathsf{pk}, \$)$ 以pk，$\$$为输入，并输出一个比特 b 以及一个验证后状态 $\$'$。

如果 Π^O 具有经典查询验证器（分别地，铸币机构），则称其具有经典查询验证器（分别地，铸币机构）；当 Ver（分别地，Gen）仅向 O 发出经典查询时，即满足此条件。

定义 6.5 (量子货币，可重复正确性**)**。 对于分布 $\mathcal{O}$，预言机辅助公钥量子货币方案 Π^O 相对于 $\mathcal{O}$ 是可重复正确 的，当且仅当满足以下条件。对于任意多项式 t，考虑实验 $O \leftarrow \mathcal{O}$, $(\mathsf{pk}, \$_1) \leftarrow \mathsf{Gen}^O()$，然后 $(b_i, \$_{i+1}) \leftarrow \mathsf{Ver}^O(\mathsf{pk}, \$_i)$，其中 $i = 1, \cdots, t$。接着要求：对于所有多项式 t，存在一个可忽略的 ϵ，使得$\Pr[b_1 = b_2 = \cdots = b_t = 1] \geq 1 - \epsilon$。

[1]毕竟，这正是 [AHY23] 最初想要证明的。

定义 6.6 (量子货币，预言机安全性)。 对于分布 $\mathcal{O}$，预言机辅助公钥量子货币方案 Π^O 相对于 $\mathcal{O}$ 是查询安全 的，当且仅当对于所有量子算法 A，若其向 O 发起的经典查询次数为多项式级，则存在一个可忽略函数 ϵ，使得:

$$\Pr[\mathsf{Ver}(\mathsf{pk},\$_1)=\mathsf{Ver}(\mathsf{pk},\$_2)=1,\ O\leftarrow\mathcal{O},\ (\mathsf{pk},\$)\leftarrow\mathsf{Gen}^{\mathcal{O}}(1^\lambda),\ \$_{1,2}\leftarrow A^{\mathcal{O}}(\mathsf{pk},\$)]\leq\epsilon(\lambda)\ ,$$

其中 $\$_{1,2}$ 是由两个可能纠缠的量子货币态$\$_1$,$\$_2$组成的联合系统 .

Π^O 相对于 $\mathcal{O}$ 是计算安全的，当且仅当上述结论仅对总体计算时间为多项式的 A 成立。

6.3 不可能性

定理 6.7。 对于任意预言机分布 $\mathcal{O}$，不存在满足以下条件的公钥量子货币方案Π^O :

- Π^O 具有经典查询验证器。
- Π^O 具有可重复正确性
- Π^O 具有查询安全性。

此外，在以下假设下，最后一项甚至可以放宽为计算安全：*(1)* 单向谜题不存在，并且 *(2)* $\mathcal{O}$ 可高效模拟。

证明。 我们首先描述 Alice 与 Bob 之间的一个协议。为初始化他们的联合状态，采样 $O\leftarrow\mathcal{O}$，并令 $(\mathsf{pk}、\$)\leftarrow\mathsf{Gen}^O()$。将 \$ 发送给 Alice，并将 pk O发送给 Bob。

现在 Alice 和 Bob 按如下方式进行交互。Alice 令 $\$_1=\$$。然后对于 $i=1、2\cdots$，Alice 执行以下操作:

- Alice 运行 $(b_i,\$_{i+1})\leftarrow\mathsf{Ver}(\mathsf{pk}、\$_i)$，但每当 Ver 发出一次（经典）预言机查询$x_j$ 至 O时，Alice 就将 x_j 发送给 Bob。Bob 知道 O，计算出 $y_j=O(x_j)$ 并将 y_j 发送给 Alice。
- Alice 向 Bob 发送比特 b_i 。

注意，根据该协议的可重复正确性，Alice 发送给 Bob 的所有比特 b_i 以压倒性概率都将为 1。

令 ρ_i 表示第 i 轮交互之前 Alice 的状态。注意， ρ_i 包含 $\$_i$，还包含 Ver 期间产生的任何信息，例如来自 O 的查询和响应。

现在我们使用冒充攻击者 Eve。一般而言，Eve 的效率不高。但如果 $\mathcal{O}$ 可模拟，那么 Alice 的视图就可以被高效模拟。如果单向谜题也不存在，那么 Eve 甚至可以做到高效：这是因为 Eve 唯一可能需要低效完成的任务，就是根据经典交互记录推断 Alice 的内部状态。

经过若干次 k 迭代后，Eve 将能够构造一个量子态 ρ'_{k+1}。 ρ'_{k+1}的一部分将是模拟的货币态 $\$'_{k+1}$，但 ρ'_{k+1} 也可能包含其他信息。现在用 ρ'_{k+1}替换ρ_{k+1} 。Eve 作出的保证是，以至少（比如说）1/2 的概率，Alice 与 Bob 之间的下一轮交互（但使用 Eve 的 ρ'_{k+1}）将得到 $b_{k+1}=1$。特别地，由于 Alice 与 Bob 交互就只是运行 Ver，因此我们有 $\Pr[\mathsf{Ver}^O(\mathsf{pk},\$'_{k+1})=1]\geq1/2$。

现在，我们可以描述 Alice 和 Eve 的对手 A:

- 输入 $(\mathsf{pk},\$=\$_1)$后， A会反复运行 $(b_i,\$_{i+1})\leftarrow\mathsf{Ver}^O(\mathsf{pk},\$_i)$。等价地， A会运行 Alice，但发送给 Bob 的消息会改为作为查询发送给 O。

- A 也会运行 Eve。在由 Eve 选择的步骤 k，Eve 将生成一个量子态 ρ'_{k+1}，其中尤其包含一个货币态 $\$'_{k+1}$。
- A 输出 $\$_{k+1}$、$\$'_{k+1}$。

根据正确性，$\Pr[\mathsf{Ver}^O(\mathsf{pk}, \$_{k+1}) = 1] \geq 3/4$；根据 Eve 的保证，$\Pr[\mathsf{Ver}^O(\mathsf{pk}, \$'_{k+1}) = 1] \geq 1/2$。因此，$\Pr[\mathsf{Ver}^O(\mathsf{pk}, \$_{k+1}) = \mathsf{Ver}^O(\mathsf{pk}, \$'_{k+1}) = 1] \geq 1/4$，这违反了 Π 的安全性。 □

6.4 释义

密码学的一项主要目标，是论证某种密码学构件 P 无法用于构建另一种密码学原语 Q。一般来说，我们可能认为 P 和 Q 都存在，因此，一种构建 Q 的简单方法是从 P 出发，让 Q 直接忽略 P，并使用假定存在的 Q 实例化。为了论证 Q 无法由 P 构建，我们需要以某种方式将范围限制在这样的 Q 实例化上：它们在某种意义上确实使用了 P。

继 Impagliazzo 和 Rudich [IR89], 之后，密码学中的标准方法是使用预言机分离。在这种方法中，给出一个预言机 O，相对于该预言机，P 可被证明存在，但 Q 不存在。这类预言机分离表明，任何相对化的构造技术——也就是仅将 P 作为黑盒来查询的技术——即使能相对于预言机运行，也不能用来从 P构造 Q 。绝大多数技术都是黑盒技术，因此这种形式的预言机／黑盒分离排除了从 P构造 Q 的“典型”或“自然”技术。这类分离通常有两种形式，两者都足以达到这一目的:

- 允许所有算法在预言机之外免费进行计算，但将“高效”算法定义为只向预言机发起多项式数量的查询的算法。
- 保留“高效”的定义，即总计算时间为多项式，但另外提供一个预言机，使其能够攻破某个复杂性类，例如 NP 或 PSPACE。这会攻破任何不向 P的预言机发起查询的 Q 实现。因此，这迫使 Q “使用” P。

这两种格式都足以证明黑盒分离，但后一种格式更加细致。

与 [AHY23]的比较。我们的结果大幅拓展了 [AHY23]的结果：从随机预言机（它刻画了单向函数或抗碰撞性等对称密码原语）拓展到所有预言机，涵盖了几乎任何密码学构件。将范围限定在随机预言机时，我们的结果也对[AHY23]的结果略有改进。具体来说，[AHY23]采用后一种格式，证明相对于随机预言机加 PSPACE 预言机，不存在带经典验证器的公钥量子货币。由于随机预言机可以被高效模拟，我们的结果表明，实际上，随机预言机加上一个能够破解（无预言机）单向谜题的预言机就足够了。这样的单向谜题破解器可以通过 PP 实现，因此其能力可能弱于 PSPACE 破解器。

超越黑盒技术。黑盒技术是指那些不具备相对化性质的技术。这类技术通过利用 P 的底层电路描述来构造 Q。非黑盒技术已成功用于克服黑盒不可能性。一个著名的例子是利用密码学群构造基于身份的加密；[PRV12], 证明，黑盒技术无法实现这一点，但 [DG17]随后表明，非黑盒技术可以做到。

因此，大多数预言机分离的一个主要局限在于，它们无法对非黑盒技术进行推理，从而可能错误地表明某种真正的不可能性。尽管如此，预言机

分离对于展示大量无效技术仍然十分重要。这可能意味着确实存在某种不可能性；即便并非如此，至少也能引导未来的研究转向能够克服这种不可能性的技术。

然而，事实证明，许多常见的非黑盒技术甚至可以通过适当的预言机来刻画。Asharov 和 Segev [AS15] 最早在不可区分性混淆（iO）的背景下观察到这一点，随后 Zhandry [Zha22]对此进行了更一般的探讨。尽管非黑盒技术可能会利用底层电路表示，但通常会将这类技术抽象为一种作用于电路的密码学原语，例如零知识证明 [GMR85],、混淆电路 [Yao86], 或不可区分性混淆 [BGI+01]。这些工作的核心观察是，这种抽象实际上可以通过恰当选择预言机来实现。

例如，考虑零知识证明的情形：证明者要证明一个 NP 陈述，却不泄露有关底层见证的任何信息。密码学中一种典型的非黑盒技术，是针对涉及某种密码学原语 P的陈述计算零知识证明。零知识证明属于非黑盒技术，因为它们会将涉及 P 的 NP 陈述转换为电路，然后对该电路进行操作。然而，这种设置可以按如下方式转化为预言机。该预言机包含两个部分：第一部分实现密码学原语 P，第二部分实现零知识证明。重要的是，为了刻画非黑盒技术，我们需要让零知识证明能够处理涉及 P的陈述。当 P 作为预言机提供时，现实世界中的零知识证明无法做到这一点。但在相对化世界中，我们可以允许零知识证明处理带有预言机辅助的陈述，而这些陈述本身会向 P发出查询。定义这类预言机并证明它们确实实现了所需的密码学原语，都很直接。

解读我们的结果。我们的预言机分离结果适用于任意预言机。因此，该结果适用于上文所述的 P-加零知识预言机，也适用于实现混淆电路或不可区分性混淆的预言机。事实上，任何甚至是非黑盒技术，只要能够建模为一个以带预言机辅助的电路为输入的预言机，也都适用于我们的不可能性结果。这涵盖了密码学中使用的绝大多数技术。与典型的预言机分离相比，这给出了强得多的分离；典型的预言机分离通常仅限于单个预言机，而该预言机通常无法涵盖非黑盒技术。

致谢

在准备本文期间，作者使用大语言模型为某些章节生成了初稿。作者审阅并修订了这些内容，并对全部内容承担责任，确保其正确性和完整性。

参考文献

[Aar05] Scott Aaronson：《量子建议与单向通信的局限性》。载于：计算理论 1.1（2005），第 1–28 页。doi：10.4086/toc.2005.v001a001 （引自第 15 页）。

[AC13] Scott Aaronson 和 Paul Christiano：《来自隐藏子空间的量子货币》。载于：计算理论 9.9（2013），第 349–401 页。doi： 10.4086/toc.2013.v009a009（引自第 4、5、14、15 页）。[ACC+22] Per Austrin、Hao Chung、Kai-Min Chung、Shiuan Fu、Yao-Ting Lin 和 Mohammad Mahmoody：《关于量子随机预言机下密钥协商的不可能性》。载于：密码学进展——CRYPTO 2022。2022 年，第 165–194 页。doi： 10.1007/978-3-031-15979-4_6 （引自第 3 页）。[AGL25] Prabhanjan Ananth、Aditya Gulati 和 Yao-Ting Lin。《伪随机酉算子的局限性》。2025 年。arXiv：2509.24484（引自第 3 页）。[AHY23] Prabhanjan Ananth、Zihan Hu 和 Henry Yuen：《关于基于抗碰撞哈希函数的公钥量子货币的（不）可信性》。载于：密码学进展——ASIACRYPT 2023。2023 年，第 39–72 页。doi： 10.1007/978-981-99-8742-9_2（引自第 2–4、14、15、17 页）。[AKY25] Prabhanjan Ananth、Fatih Kaleoglu 和 Henry Yuen：《同时 Haar 不可区分性及其在不可克隆密码学中的应用》。载于：第 16 届理论计算机科学创新会议（ITCS 2025）。第 325 卷。2025 年。doi： 10.4230/LIPIcs.ITCS.2025.7 （引自第 3 页）。[AL70] Huzihiro Araki 和 Elliott H. Lieb：《熵不等式》。载于：数学物理通讯 18.2（1970 年 1 月），第 160–170 页。doi： 10.1007/BF01646092 （引自第 8 页）。[AS15] Gilad Asharov 和 Gil Segev：《不可区分性混淆与函数加密能力的界限》。载于：2015 年 IEEE 第 56 届计算机科学基础年度研讨会。2015 年，第 191–209 页。doi：10.1109/FOCS.2015.21 （引自第 18 页）。[BB14] Charles H. Bennett 和 Gilles Brassard：《量子密码学：公钥分发与抛硬币》。载于：理论计算机科学 560（2014）。量子密码学的理论方面——庆祝 BB84 诞生 30 周年，第 7–11 页。doi：10.1016/j.tcs.2014.05.025 （引自第 2 页）。[BCM+18] Zvika Brakerski、Paul Christiano、Urmila Mahadev、Umesh Vazirani 和 Thomas Vidick：《利用单个量子设备进行量子性测试与可认证随机性》。载于：2018 年 IEEE 第 59 届计算机科学基础年度研讨会（FOCS）。2018 年，第 320–331 页。doi：10.1109/FOCS.2018.00038 （引自第 3 页）。[BGI+01] Boaz Barak、Oded Goldreich、Rusell Impagliazzo、Steven Rudich、Amit Sahai、Salil Vadhan 和 Ke Yang：《关于程序混淆的（不）可能性》。载于：密码学进展——CRYPTO 2001。2001 年，第 1–18 页。doi： 10.1007/3-540-44647-8_1（引自第 18 页）。[BHK+19] Gilles Brassard、Peter Høyer、Kassem Kalach、Marc Kaplan、Sophie Laplante 和 Louis Salvail：《量子世界中的 Merkle 式密钥建立》。载于：密码学杂志 32.3（2019），第 601–634 页。doi： 10.1007/s00145-019-09317-z（引自第 3 页）。

[BS08] Gilles Brassard 和 Louis Salvail。“量子默克尔谜题”。载于：第二届量子、纳米与微技术国际会议（ICQNM 2008）。2008 年，第 76–79 页。doi: 10.1109/ICQNM.2008.16 （引文见第 3 页）。[BV97] Ethan Bernstein 和 Umesh Vazirani。“量子复杂性理论”。载于：SIAM 计算杂志 26.5（1997），第 1411–1473 页。doi: 10.1137/S0097539796300921 （引文见第 5 页）。[DG17] Nico Döttling 和 Sanjam Garg。“基于 Diffie–Hellman 假设的基于身份的加密”。载于：密码学进展——CRYPTO 2017。第 10401 卷。2017 年，第 537–569 页。doi: 10.1007/978-3-319-63688-7_18 （引文见第 17 页）。[DMR25] Nico Döttling、Anne Müller 和 Mahesh Sreekumar Rajasree。《将伪随机码与局部预言机分离》。2025 年。doi: 10.60882/cispa.30316222.v1（引文见第 14 页）。[GGW25] Sanjam Garg、Sam Gunn 和 Mingyuan Wang。《黑盒密码学对伪随机码毫无用处》。2025 年。arXiv: 2506.01854（引文见第 14 页）。[GMR85] Shafi Goldwasser、Silvio Micali 和 Charles Rackoff。“交互式证明系统的知识复杂度”。载于：第十七届 ACM 计算理论年度研讨会论文集。1985 年，第 291–304 页。doi: 10.1145/22145.22178（引文见第 18 页）。[HOT81] Fumio Hiai、Masanori Ohya 和 Makoto Tsukada。“冯·诺伊曼代数中的充分性、KMS 条件与相对熵”。载于：太平洋数学杂志 96.1（1981），第 99–109 页。doi: 10.2140/pjm.1981.96.99（引文见第 7 页）。[IR89] Russell Impagliazzo 和 Steven Rudich。“关于单向置换可证明推论的局限”。载于：第二十一届 ACM 计算理论年度研讨会论文集。1989 年，第 44–61 页。doi: 10.1145/73007.73012 （引文见第 17 页）。[KT24] Dakshita Khurana 和 Kabir Tomer。“基于量子单向性的承诺”。载于：第 56 届 ACM 计算理论年度研讨会论文集。2024 年，第 968–978 页。doi: 10.1145/3618260.3649654（引文见第 2 页）。[KT25] Dakshita Khurana 和 Kabir Tomer。“以量子优势为量子密码学奠基，或：迈向基于 #P 困难性的密码学”。载于：第 57 届 ACM 计算理论年度研讨会论文集。2025 年，第 178–188 页。doi: 10.1145/3717823.3718145（引文见第 9 页）。[LLLL24] Longcheng Li、Qian Li、Xingjian Li 和 Qipeng Liu。“如何（不）在迷你密码学中构建量子公钥加密”。载于：密码学进展——CRYPTO 2024。第 14926 卷。2024 年，第 152–183 页。doi: 10.1007/978-3-031-68394-7_6 （引文见第 3 页）。[LMW25] Wei-KaiLin、Ethan Mook 和 Daniel Wichs。“黑盒密码学对双重高效私人信息检索毫无用处”。载于：密码学进展——EUROCRYPT 2025。第 15606 卷。2025 年，第 65–93 页。doi: 10.1007/978-3-031-91095-1_3 （引文见第 14 页）。[MR09] Jörn Müller-Quade 和 Renato Renner。“量子密码学中的可组合性”。载于：新物理学杂志 11.8（2009），第 085006 页。doi: 10.1088/1367-2630/11/8/085006（引文见第 2 页）。[PR14] Christopher Portmann 和 Renato Renner。“量子密钥分发的密码学安全性”。载于：（2014）。arXiv: 1409.3525（引文见第 2 页）。

[PRV12] Periklis A. Papakonstantinou、Charles W. Rackoff 和 Yevgeniy Vahlis。DDH困难群有多强大？2012 年。密码学电子印本档案： 2012/653 （引文见第 17 页）。[QRZ25] Luowen Qian、Justin Raizes 和 Mark Zhandry。“量子密码学中的困难量子外推”。载于：密码学进展——EUROCRYPT 2025。第 15607 卷。2025 年，第 53–81 页。doi: 10.1007/978-3-031-91098-2_3（引文见第 3、9 页）。[RS19] Roy Radian 和 Or Sattath。“半量子货币”。载于：第一届 ACM金融技术进展会议论文集。2019 年，第 132–146 页。doi: 10.1145/3318041.3355462（引文见第 4 页）。[Shm22] Omri Shmueli。“具有经典银行的公钥量子货币”。载于：第 54 届 ACM SIGACT计算理论研讨会论文集。2022 年，第 790–803 页。doi: 10.1145/3519935.3519952 （引文见第 4 页）。[Sim94] Daniel R. Simon。“论量子计算的能力”。载于：第 35 届计算机科学基础研讨会论文集。1994 年，第 116–123 页。doi: 10.1109/SFCS.1994.365701 （引文见第 5 页）。[Wil17] Mark M. Wilde。《量子信息论》。第 2 版。剑桥大学出版社，2017 年。doi: 10.1017/9781316809976 （引文见第 8 页）。[Win99] Andreas Winter。“量子信道的编码定理与强逆定理”。载于：IEEE信息论汇刊 45.7（1999），第 2481–2485 页。doi: 10.1109/18.796385（引文见第 15 页）。[Yao86] Andrew Chi-Chih Yao。“如何生成并交换秘密”。载于：第 27 届计算机科学基础年度研讨会（sfcs 1986）。1986 年，第 162–167 页。doi: 10.1109/SFCS.1986.25 （引文见第 18 页）。[Zha12] Mark Zhandry。“量子随机预言机模型中的安全基于身份的加密”。载于：密码学进展——CRYPTO 2012。第 7417 卷。2012 年，第 758–775 页。doi: 10.1007/978-3-642-32009-5_44 （引文见第 14 页）。[Zha22] Mark Zhandry。“增强随机预言机”。载于：密码学进展——CRYPTO 2022。第 13509 卷。2022 年，第 35–65 页。doi: 10.1007/978-3-031-15982-4_2 （引文见第 18 页）。[Zha25a] Mark Zhandry。“关于量子安全伪随机置换的一则注记”。载于：Quantum 9（2025），第 1696 页。doi: 10.22331/q-2025-04-08-1696 （引文见第 14 页）。[Zha25b] Mark Zhandry。“论量子货币与规避性混淆”。载于：密码学进展——EUROCRYPT 2025。第 15603 卷。2025 年，第 187–216 页。doi: 10.1007/978-3-031-91131-6_7 （引文见第 4 页）。