arXiv:2304.02999v2 [quant-ph] 2 Jan 2024

具有鲁棒性的量子公钥加密及其在量子密钥分发中的应用

Giulio Malavolta[1,2] 和 Michael Walter[3]

[1]意大利米兰博科尼大学[2]德国波鸿马克斯·普朗克安全与隐私研究所[3]德国波鸿鲁尔大学

摘要

量子密钥分发（QKD）允许 Alice 和 Bob 在通过公共（不受信任的）量子信道进行通信的同时，协商出一个共享的秘密密钥。与经典密钥交换相比，它具有两大优势：（i）该密钥对任何攻击者而言都是无条件地 隐藏的；（ii）其安全性仅依赖于认证经典信道的存在，而在实践中，这可以通过使用诸如数字签名存在性之类的 Minicrypt 假设来实现。另一方面，量子密钥分发协议通常需要进行多轮交互，而经典密钥交换则可以借助公钥加密，以最少的两条消息实现。一个长期悬而未决的问题是：量子密钥分发是否比经典密钥交换需要更多轮交互。

在这项工作中，我们提出了一种双消息量子密钥分发协议，在仅假设量子安全单向函数存在的情况下，即可实现永久性安全。也就是说，只要协议执行期间计算假设成立，共享密钥就能无条件地隐藏。我们的结果基于一种新型量子公钥加密（QPKE）构造，其安全性与经典对应方案颇为相似，仅依赖认证经典信道。

1 引言

量子密钥分发（QKD） [4] 使 Alice 和 Bob 能够通过公共（不可信）量子信道交换秘密密钥。与经典密钥交换相比，它有两大优势：（i）对于任何（可能不受计算能力限制且具有量子能力的）攻击者，密钥都无条件地或在信息论意义上保持隐藏；（ii）它仅依赖认证经典信道的存在，而在实践中，这些信道可以通过 Minicrypt [12] 计算假设来实现。前一优势显然无法在没有量子信息的情况下实现，而且我们也有充分证据 [13]表明，经典密钥交换需要更强结构的（Crypto mania）计算假设。

过去几十年来，量子密钥分发激发了数量惊人的研究，从深奥的理论工作 [19, 17, 18, 22] 一直到大规模实验 [14, 16, 25]。因此，量子密钥分发是量子信息理论中研究最为广泛的主题之一。尽管关于这一主题的文献极其丰富，量子密钥分发协议在各个方面仍无法超越经典密钥交换：经典密钥交换可以使用两条消息 [5], 来实现，这是最优的；但据我们所知，所有已知的量子密钥分发协议都需要超过两轮交互。

这引出了一个问题：对于量子密钥分发而言，更多轮交互是否真的有必要？除了理论上的重要性之外，解决这一问题也有实际原因。事实上，对于这样的实际场景而言，两消息协议尤其理想：参与方可能会在协议执行期间离线，可能希望在稍后的时间发送消息，或者不希望跨轮次保留状态。可以说，正是这种最小化的交互模式，使公钥加密等传统密码学原语如此有用。然而，尽管有着如此强烈的动机，并且经过了近五十年的深入研究，量子密钥分发的最优轮复杂度仍然是一个悬而未决的问题。

1.1 我们的成果

在这项工作中，我们证明只需两条消息就能构造具有永久安全性的量子密钥分发协议。具体而言，我们证明了以下结论：

> 如果量子安全单向函数存在，那么就存在两条消息的量子密钥分发协议。

显然，量子密钥分发至少需要两条消息，因此我们的协议实现了最优轮数复杂度。此外，只有第一条消息（从 Alice 发给 Bob）是量子的，而 Bob 的回复完全是经典的。该协议满足强意义上的永久安全性：只要攻击者在协议执行期间运行于量子多项式时间，共享密钥在信息论意义上就是隐藏的。

我们认为，我们的方法与传统的量子密钥分发协议设计大相径庭 [4, 8],；它受到近期带认证删除的密码学 [3] 和量子公钥加密 [2]研究的启发。我们的协议及其分析都完全基于初等方法，而且足够简单，可以在本科课程中完整讲解。作为比较，研究人员花了十多年时间，才为第一个量子密钥分发协议建立了形式化证明 [4]。

我们的核心技术要素是一种构建量子公钥加密（QPKE）的新框架。QPKE 是一种密码学原语，允许 Alice 生成由量子态 ρ 和经典字符串公钥组成的公钥。该方案具有鲁棒性，也就是说，即使区分器获得公钥，并且可以任意篡改量子态 ρ，安全性仍能得到保证。我们介绍 QPKE 的两个实例：

- （永久安全性）在我们的第一个方案中，只要区分器在协议执行期间受到计算能力限制，消息 m 就能保持信息论意义上的隐藏。即使区分器只获得公钥的单个副本，这一性质仍然成立，而这已足以构建量子密钥分发。

- （计算安全性）在我们的第二个方案中，消息 m 在计算意义上是隐藏的，也就是说，我们只要求安全性能够抵御计算能力受限的区分器。虽然这是一种较弱的安全概念，但该方案的优势在于，即使区分器获得公钥的任意多个 副本，安全性仍然成立。

第一种构造只在我们仅提供一份公钥的模型中安全，这并非偶然。研究表明， [2] 若提供足够多（但数量为多项式级）的公钥副本，无界对手便能发起密钥恢复攻击。这意味着，不存在任何量子公钥加密能够对看到任意多份公钥副本的区分器实现永久安全性，也说明了采用较弱安全概念（计算安全性）的必要性。

永久安全性。 我们指出，与 QKD 的标准攻击者模型相比，我们在本文中考虑的攻击者模型存在一个细微差异。后者（例如在 [23, 24]，中所考虑的模型）将攻击者建模为计算能力不受限的量子信道，但不允许其篡改通过 经典信道 发送的信息。也就是说，该模型仅假设存在认证经典信道，但除此之外不对区分器的运行时间施加任何限制。另一方面，在本文中，除存在认证经典信道外，我们还考虑这样一种攻击者：其在协议执行期间运行于 量子多项式时间 ，但在协议终止后允许其计算能力不受限制。也就是说，我们证明了 [20] 意义下的永久安全性 。

尽管在技术上有所不同，但我们认为，对于大多数实际场景而言，这两个模型实际上是等价的。认证经典信道这一假设通常是通过让每一方使用数字签名对自己的消息进行签名来加以证明的，而这至少要求在协议执行期间计算假设成立。从这个意义上说，认证经典信道的存在本身就已经限制攻击者在协议执行期间以量子多项式时间运行（否则攻击者只需破坏数字签名的安全性即可）。

最后，不难证明，永久安全性是 QPKE 的最佳可实现安全概念；也就是说，如果允许区分器在协议执行期间不受时间限制地运行，那么对任何 QPKE方案都存在通用攻击。即使存在认证经典信道，这种攻击仍然有效，并且必定成功。为完整起见，我们在附录 A 中给出这一事实的证明。

1.2 并行工作

一项并行工作 [15] 在鲁棒量子公钥加密方面取得了类似结果，其安全性仅针对允许任意篡改公钥的量子部分的区分器成立。与我们的工作相比，他们仅考虑<styleid='2'>计算安全性的情形，而我们将具有永久安全性的方案视为本工作的主要贡献，正是该方案使我们的双消息量子密钥分发协议成为可能。即使仅关注计算安全性情形，我们的方案也有许多相似之处，但有趣的是，它们并不完全相同。在技术层面上，他们的方法基于针对 Wiesner态的一次性签名，而我们的方法（事后看来）可以被理解为对 $|+\rangle$ 量子态进行一次性签名。另一方面， [15] 提出了一种公钥为纯态的方案，而且他们的方案实现了更强的选择密文攻击安全性概念，而这是我们在本工作中未予考虑的。

1.3 开放问题

我们的工作留下了一系列尚待解答的问题，希望能激发该领域的进一步研究。首先，我们的协议是在量子信道完美（无噪声）的情况下描述的。任何实用协议都需要能够抵御噪声。虽然从理论上讲，可以简单地使用量子纠错码对所有量子态进行编码，但这可能会导致实际效率低下。我们将研究非交互式量子密钥分发协议的变体留作开放问题，以探究其在存在噪声时是否仍然高效。

标准量子密钥分发协议（如 [4] ）的一个突出优点是，所有量子态都是单个量子比特的张量积，而我们的协议则需要多个量子比特态的相干叠加。前者这一特性很可取，因为它使得在当今量子硬件上实现该

协议成为可能。我们认为，在这种逐量子比特模型下构造非交互式量子密钥分发协议是一个引人入胜的研究方向，并相信这可能需要与当前方法截然不同的技术。

1.4 解决方案概述

我们的主要技术贡献是一种构造量子公钥加密的新方法，下面回顾其定义。量子公钥加密的语法由三个算法组成：密钥生成、加密和解密。密钥生成算法生成一对经典密钥 (sk, pk)，以及一个量子态 ρ。密钥对 (pk ρ) 构成公钥。任何人都可以利用该公钥计算经典密文 ct，对给定消息 m 进行加密，而只有秘密密钥的所有者才能解密该密文。在安全性方面，我们要求消息 m 应当在信息论意义上被隐藏，即便允许高效攻击者任意篡改与公钥关联的量子态。

构造量子公钥加密。我们的量子公钥加密构造采用了一种在概念上不同于传统量子密钥分发协议的方法。为了直观理解我们的框架，不妨考虑一个量子态和测量

$$\frac{|0, B_0\rangle + |1, B_1\rangle}{\sqrt{2}} \quad \text{and} \quad \{\Pi, \mathsf{Id} - \Pi\},$$

其中 $|B_0\rangle$和 $|B_1\rangle$ 是由密钥生成算法采样的两个不可伪造基态</style}，而 $\{\Pi, \mathsf{Id} - \Pi\}$ 是一种可高效实现的投影测量，用于验证第二个寄存器是否处于所有此类基态构成的子空间中（无需知道具体使用的是哪些基态）。

事实证明，可以利用这一点来秘密传输信息：解密方保留第一个量子比特，并在哈达玛基下对其进行测量，这会在两个不可伪造的基态之间引入一个随机的相对相位（这实际上可以在密钥生成时完成）。加密方在哈达玛基下测量第二个寄存器，以获得相关随机性，然后利用这种随机性通过（经典的）一次一密安全地掩盖消息。

为了直观理解该方案为何安全，可以看到，把第二个寄存器交给对手，在信息论意义上与随机交给对手两个基态 $|B_0\rangle$ 和 $|B_1\rangle$ 中的一个无法区分。由于假设这些量子态难以伪造，对手能做的只有将它们原样传递（除非他们想让验证投影失败）；此时，进行 Hadamard 测量会得到一个信息论意义上均匀随机的结果。

我们的实际方案使用一次性签名来实现上述抽象模板：隐藏基只是有效的消息—签名对，而投影 Π 可以通过相干地运行验证算法并测量所得的输出比特来高效实现。更多详情请参阅技术章节。

从量子公钥加密到量子密钥分发。 一旦构建好量子公钥加密，构造一个双消息量子密钥分发协议似乎轻而易举：Alice 可以采样一个公钥并发送给 Bob，Bob 再回复一个用随机采样的密钥加密后的密文 $k \in \{0,1\}^\lambda$。然而，分析该协议时有一个微妙之处，这与保密性并不必然意味着安全性这一事实有关。事实上，攻击者可能让 Alice 和 Bob 达成一致的却是不同的密钥，同时不违反量子公钥加密的安全性。我们再次依靠一次性签名来（可证明地）防止这类攻击。

1.5 本文的组织结构

在第2 节中，我们将讨论量子信息和密码学的预备知识，并证明一些有用的技术性结论。在第3节中，我们定义量子公钥加密的概念，并提出两种构造（具有不同的权衡），其安全性可归约于任意后量子单向函数的单向性。在第4 节中，我们将给出双消息量子密钥分发协议的形式化描述及其分析。

2 预备知识

在本文中，我们用 λ 表示安全参数。我们用 1^λ 表示长度为 λ 的全 1 字符串。若函数 negl 关于安全参数 λ 是可忽略的，即 $\mathrm{negl}(\lambda) = \lambda^{\omega(1)}$，则称 negl 为可忽略函数。对于有限集合 S，我们用 $x \leftarrow S$ 表示从 S 中均匀随机采样得到 x。我们用 Tr 表示矩阵或算子的迹。

2.1 量子信息

在本节中，我们提供一些关于量子信息的初步背景知识。有关更深入的介绍，请参阅 [21]。一个由 n 量子比特组成的寄存器 x 由希尔伯特空间 $(\mathbb{C}^2)^{\otimes n}$ 给出，并带有名称或标签 x。给定两个寄存器 x和y，我们将复合寄存器记作$\mathsf{x} \otimes \mathsf{y}$，其希尔伯特空间是各个寄存器希尔伯特空间的张量积。寄存器 x上的一个 纯量子态 是一个单位向量 $|\Psi\rangle_{\mathsf{x}} \in (\mathbb{C}^2)^{\otimes n}$。寄存器 x 上的一个 混合量子态 由$(\mathbb{C}^2)^{\otimes n}$上的密度算子 ρ_{x} 表示，该密度算子是迹为1 的半正定厄米矩阵。任意纯态 $|\Psi\rangle_{\mathsf{x}}$ 也可以被视为混合量子态 $\rho_{\mathsf{x}} = |\Psi\rangle_{\mathsf{x}} \langle\Psi|_{\mathsf{x}}$，但存在并非纯态的混合量子态。在上述内容中，我们使用下标表示寄存器，但在上下文明确时通常将其省略。我们采用以下约定：

$$\{|0\rangle, |1\rangle\} \text{ and } \left\{ \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right\}$$

分别表示计算基和哈达玛基量子态。

一个量子信道 F 是从寄存器 x到寄存器y 的完全正保迹（CPTP）映射。也就是说，对于输入的任意密度矩阵 ρ_{x}，操作 F 会产生 $F(\rho_{\mathsf{x}}) = \tau_{\mathsf{y}}$，即寄存器$\mathsf{y}$ 上的另一个量子态；当我们将 F 应用于量子态 ρ_{xz}的x 寄存器时，情况也是如此。对于任意酉算子 U，即 $U^\dagger U = UU^\dagger = \mathrm{Id}$，可以得到一个将输入量子态 ρ映射为输出量子态 τ的量子信道：$= U\rho U^\dagger$。泡利算子X、Y、Z 是 2×2矩阵，它们既是酉的又是厄米的。更具体地说：

$$\mathsf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \mathsf{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \mathsf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

一个投影算子 Π 是一个满足 $\Pi^2 = \Pi$的厄米算子。一个投影测量 由一组满足 $\sum_j \Pi_j = \mathrm{Id}$ 的投影算子 $\{\Pi_j\}_j$ 给出。给定一个状态 ρ，测量以概率 $p_j = \mathrm{Tr}(\Pi_j \rho)$ 得到结果 j，此后状态变为 $\Pi_j \rho \Pi_j / p_j$（这可以用量子信道建模，但我们不需要这样做）。对于任意两个寄存器 x 和 y，偏迹 Tr_{y} 是从 $\mathsf{x} \otimes \mathsf{y}$ 到 x 的唯一信道，使得对所有 ρ_{x} 和 τ_{y}，均有 $\mathrm{Tr}_{\mathsf{y}}(\rho_{\mathsf{x}} \otimes \tau_{\mathsf{y}}) = \mathrm{Tr}(\tau_{\mathsf{y}})\rho_{\mathsf{x}}$。

The 两个量子态之间的迹距离 ρ和 τ，记作 $\mathsf{Td}(\rho,\tau)$，定义为

$$\mathsf{Td}(\rho,\tau)=\frac{1}{2}\|\rho-\tau\|_1=\frac{1}{2}\mathsf{Tr}\left(\sqrt{(\rho-\tau)^\dagger(\rho-\tau)}\right).$$

迹距离的操作意义是：$\frac{1}{2}(1+\mathsf{Td}(\rho,\tau))$是两个量子态 ρ和 τ 能够被任意（可能是无界的）量子信道或算法区分的最大概率。如果 $\tau=|\Phi\rangle\langle\Phi|$ 是纯态，则我们有以下版本的 Fuchs-van de Graaf 不等式：

$$1-\langle\Phi|\rho|\Phi\rangle\leq\mathsf{Td}(\rho,\tau)\leq\sqrt{1-\langle\Phi|\rho|\Phi\rangle}. \tag{2.1}$$

量子算法。 非均匀量子多项式时间（*QPT*）机器 $\{\mathcal{A}_\lambda\}_{\lambda\in\mathbb{N}}$ 是一族多项式规模的量子机器 $\mathcal{A}_\lambda$，其中每个机器都以一个多项式规模的辅助态 $|\alpha_\lambda\rangle$初始化。每个 $\mathcal{A}_\lambda$ 都可以用一个 CPTP 映射描述。量子交互式机器就是一系列量子信道，并指定了输入、输出和工作寄存器。我们称两个概率分布 $\mathcal{X}$ 和 $\mathcal{Y}$ 是计算上不可区分的，如果存在一个可忽略函数 negl，使得对所有 QPT 算法 $\mathcal{A}_\lambda$，均有

$$\left|\Pr\left[1\leftarrow\mathcal{A}_\lambda(x):x\leftarrow\mathcal{X}\right]-\Pr\left[1\leftarrow\mathcal{A}_\lambda(y):y\leftarrow\mathcal{Y}\right]\right|=\mathsf{negl}(\lambda).$$

我们称它们是 统计上不可区分，如果对于所有（可能无界的）算法，该性质都成立。

区分蕴含交换。 我们回顾一下区分量子态与在共轭基上进行交换之间等价关系的正式表述。该结果已在 [1] 中证明，下面我们给出一个改写版本，借鉴自 [11]。实际上，我们只陈述该蕴含关系的一个方向（其逆命题也已证明成立，见 [1]），因为这正是我们所需要的。

定理 2.1（区分蕴含交换 [1]）。 设 $|\Psi\rangle$和 $|\Phi\rangle$是正交的 n量子比特量子态，并假设量子多项式时间区分器 $\mathcal{A}_\lambda$ 以优势 δ 区分 $|\Psi\rangle$和 $|\Phi\rangle$，且不使用任何辅助量子比特。那么，存在一个作用于 n 量子比特量子态上的可在多项式时间内计算的酉算子 U，使得

$$\frac{|\langle y|U|x\rangle+\langle x|U|y\rangle|}{2}=\delta\text{ where }|x\rangle=\frac{|\Psi\rangle+|\Phi\rangle}{\sqrt{2}}\text{ and }|y\rangle=\frac{|\Psi\rangle-|\Phi\rangle}{\sqrt{2}}.$$

此外 ，如果 $\mathcal{A}_\lambda$ 不作用于某些量子比特，那么 U 也不作用于这些量子比特。

2.2 信息论

回顾随机变量 X 的最小熵定义如下：

$$H_\infty(X)=-\log\left(\max_x\Pr[X=x]\right).$$

下面回顾平均条件最小熵的定义。

定义 2.2（平均条件最小熵）。 设 X 是一个取值于有限集合 $\mathcal{X}$ 的随机变量， Z 是一个（可能相关的）取值于有限集合 $\mathcal{Z}$ 的随机变量。˜平均条件最小熵 $H_\infty(X|Z)$ 定义为

$$\tilde{H}_\infty(X|Z)=-\log\left(\mathbb{E}_z\left[\max_{x\in\mathcal{X}}\Pr[X=x|Z=z]\right]\right).$$

已在 [7, 6] 中证明，平均条件最小熵满足一个 链式法则，即

$$\tilde{H}_\infty(X|Z) \geq H_\infty(X) - H_0(Z) \tag{2.2}$$

其中， $H_0(Z)$表示 Z的支撑集大小的对数。接下来，我们回顾带种子的随机性提取器的定义。

定义 2.3 （提取器）。 若函数 Ext : $\{0,1\}^d \times \mathcal{X} \to \{0,1\}^\ell$ 满足以下条件，则称其为一个带种子的强平均情形（k,ε）-提取器：对于支撑集为 $\mathcal{X}$ 的所有随机变量 X ，以及定义在某个~有限支撑集上的 Z ，若 $H_\infty(X|Z) \geq k$，则以下分布之间的统计距离至多为 ε

$$(\mathsf{seed}, \mathsf{Ext}(\mathsf{seed}, X), Z) \approx_\varepsilon (\mathsf{seed}, U, Z)$$

其中，种子 $\leftarrow \{0,1\}^d$ 且 $U \leftarrow \{0,1\}^\ell$。

回顾一下，若哈希函数 Hash : $\mathcal{X} \to \mathcal{Y}$ 满足对所有 $x \neq x' \in \mathcal{X}$ 均有下式成立，则称其为通用哈希：

$$\Pr[\mathsf{Hash}(x) = \mathsf{Hash}(x')] \leq \frac{1}{|\mathcal{Y}|}$$

其中，概率是对哈希函数的选择取平均得到的。文献 [7, 6]证明，任何通用哈希函数都是平均情形随机性提取器。

引理 2.4 （剩余哈希引理）。 设 X 是一个支撑集为有限集合 $\mathcal{X}$ 的随机变量，并设~ Z 是一个（可能相关的）随机变量，其支撑集为有限集合 $\mathcal{Z}$，满足 $H_\infty(X|Z) \geq k$。设 Hash : $\mathcal{X} \to \{0,1\}^\ell$，其中 $\ell \leq k - 2\log\left(\frac{1}{\varepsilon}\right)$，是一个通用函数族。则 Hash 是一个带种子的强平均情形（k,ε）-提取器。

2.3 伪随机函数

我们回顾伪随机函数 [10] 的概念。伪随机函数（PRF）是一种带密钥函数

$$\mathsf{PRF} : \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^\lambda$$

它在计算上不可区分于真正的随机函数。更准确地说，我们要求存在一个可忽略函数 negl，使得对于所有量子多项式时间 $\{\mathcal{A}_\lambda\}$ 和所有 $\lambda \in \mathbb{N}$，以下分布在计算上不可区分

$$\mathcal{A}_\lambda(1^\lambda)^{\mathsf{PRF}(k,\cdot)} \approx \mathcal{A}_\lambda(1^\lambda)^{f(\cdot)}$$

其中， $k \leftarrow \{0,1\}^\lambda$ 和 f 是均匀采样函数。众所周知，抗量子伪随机函数可以由任意单向函数 [10] 构造。

2.4 一次性签名

我们回顾一下 一次性签名方案 [9] 的概念。

定义 2.5 （一次性签名）。 一种一次性签名（*OTS*）方案被定义为算法元组 (SGen,Sign,Ver)，使得：

- (vk, sk) $\leftarrow$ SGen(1^λ)：一个多项式时间算法，输入安全参数 1^λ 后，输出两个比特串 vk 和 sk。

- $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}\ m)$：一个多项式时间算法，在输入签名密钥 sk 和消息 m 后，输出签名 σ。

- $\{0,1\} \leftarrow \mathsf{Ver}(\mathsf{vk}\ m,\sigma)$：一种多项式时间算法，以验证密钥 vk、消息 m 和签名 σ 作为输入，并返回表示接受或拒绝的比特。

一次性签名方案是正确的，若对于所有 $\lambda \in \mathbb{N}$ 和所有消息 m，均有

$$\Pr\left[1 = \mathsf{Ver}(\mathsf{vk}, m, \mathsf{Sign}(\mathsf{sk}, m)) : (\mathsf{vk}, \mathsf{sk}) \leftarrow \mathsf{SGen}(1^\lambda)\right] = 1.$$

接下来，我们定义 OTS 的强存在性不可伪造性概念：即使针对同一条消息，也无法生成一个与签名预言机提供的签名不同的签名。众所周知，强不可伪造签名可以由任意单向函数（OWF）构造而成 [9]。为方便起见，我们定义一个稍弱的概念，其中待签名的消息预先固定——显然，标准概念蕴含这一概念；在标准概念中，攻击者可以自适应地查询签名预言机。

定义 2.6（强存在不可伪造性）。我们称一个一次性签名方案 (SGen,Sign,Ver) 满足（量子安全的）强存在不可伪造性，如果存在一个可忽略函数negl，使得对于所有量子多项式时间 $\{\mathcal{A}_\lambda\}$、所有 $\lambda \in \mathbb{N}$ 以及所有消息 m，均有

$$\Pr\left[\begin{array}{l} 1 = \mathsf{Ver}(\mathsf{vk}, m^*, \sigma^*) \text{ and } (m^*, \sigma^*) \neq (m, \sigma) : \\ \end{array} \begin{array}{l} (\mathsf{vk}, \mathsf{sk}) \leftarrow \mathsf{SGen}(1^\lambda); \\ \sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, m); \\ (m^*, \sigma^*) \leftarrow \mathcal{A}_\lambda(\mathsf{vk}, m, \sigma) \end{array}\right] = \mathsf{negl}(\lambda).$$

签名量子态的不可区分性。我们对签名量子态与相应经典混合态的不可区分性给出形式化陈述及证明。该证明受到 [11] 的研究启发，并与其工作密切相关。

引理 2.7。设(SGen,Sign,Ver) 是满足强存在性不可伪造性的一次性签名方案。那么，以下分布族在计算上不可区分

$$\left\{\frac{|0,\sigma_0\rangle + |1,\sigma_1\rangle}{\sqrt{2}} \frac{\langle 0,\sigma_0| + \langle 1,\sigma_1|}{\sqrt{2}}, (\mathsf{vk}_0, \mathsf{vk}_1)\right\} \approx \left\{\frac{|0,\sigma_0\rangle\langle 0,\sigma_0| + |1,\sigma_1\rangle\langle 1,\sigma_1|}{2}, (\mathsf{vk}_0, \mathsf{vk}_1)\right\}$$

其中 $(\mathsf{vk}_b,\mathsf{sk}_b) \leftarrow \mathsf{SGen}(1^\lambda)$ 且 $\sigma_b \leftarrow \mathsf{Sign}(\mathsf{sk}_b, b)$，对于 $b \in \{0,1\}$。

证明。由凸性，只需证明，任何作用于寄存器v 和x上的量子多项式时间对手都无法以不可忽略的概率区分量子态 $|\Psi_0\rangle$ 和 $|\Psi_1\rangle$，其中

$$|\Psi_b\rangle = \sum_{(\mathsf{vk},\mathsf{sk})} \sqrt{D(\mathsf{vk},\mathsf{sk})}\, |\mathsf{vk},\mathsf{sk}\rangle_{\mathsf{s}}\, |\mathsf{vk}\rangle_{\mathsf{v}} \otimes \frac{|0,\sigma_0\rangle_{\mathsf{x}} + (-1)^b\, |1,\sigma_1\rangle_{\mathsf{x}}}{\sqrt{2}}$$

并且我们采用以下符号约定：

$$\mathsf{sk} = \{\mathsf{sk}_0, \mathsf{sk}_1\}\ ;\ \mathsf{vk} = \{\mathsf{vk}_0, \mathsf{vk}_1\}\ ;\ \sigma_b = \mathsf{Sign}(\mathsf{sk}_b, b) \text{ and } D(\mathsf{vk},\mathsf{sk}) = \Pr[(\mathsf{vk},\mathsf{sk}) = \mathsf{SGen}(1^\lambda)].$$

反设存在一个作用于寄存器v、x以及辅助寄存器 $|\alpha_\lambda\rangle_{\mathsf{a}}$ 的QPT 区分器，其成功概率为 δ。那么，根据定理 2.1，存在一个可在多项式时间内计算的酉算子 U 使得

$$\frac{1}{2}\left|\begin{array}{l}\langle\Psi_1'|_{\mathsf{s,v,x}}\langle\alpha_\lambda|_{\mathsf{a}}\left(U_{\mathsf{v,x,a}}\otimes\mathsf{Id}_{\mathsf{s}}\right)|\Psi_0'\rangle_{\mathsf{s,v,x}}|\alpha_\lambda\rangle_{\mathsf{a}}\\+\langle\Psi_0'|_{\mathsf{s,v,x}}\langle\alpha_\lambda|_{\mathsf{a}}\left(U_{\mathsf{v,x,a}}\otimes\mathsf{Id}_{\mathsf{s}}\right)|\Psi_1'\rangle_{\mathsf{s,v,x}}|\alpha_\lambda\rangle_{\mathsf{a}}\end{array}\right|=\delta$$

其中

$$\left|\Psi_b'\right\rangle=\frac{|\Psi_0\rangle+(-1)^b|\Psi_1\rangle}{\sqrt{2}}=\sum_{(\mathsf{vk},\mathsf{sk})}\sqrt{D(\mathsf{vk},\mathsf{sk})}\,|\mathsf{vk},\mathsf{sk}\rangle_{\mathsf{s}}|\mathsf{vk}\rangle_{\mathsf{v}}\otimes|b,\sigma_b\rangle_{\mathsf{x}}.$$

因此，必然是以下两种情况之一

- $\langle\Psi_1'|_{\mathsf{s,v,x}}\langle\alpha_\lambda|_{\mathsf{a}}\left(U_{\mathsf{v,x,a}}\otimes\mathsf{Id}_{\mathsf{s}}\right)|\Psi_0'\rangle_{\mathsf{s,v,x}}|\alpha_\lambda\rangle_{\mathsf{a}}\geq\delta$, or
- $\langle\Psi_0'|_{\mathsf{s,v,x}}\langle\alpha_\lambda|_{\mathsf{a}}\left(U_{\mathsf{v,x,a}}\otimes\mathsf{Id}_{\mathsf{s}}\right)|\Psi_1'\rangle_{\mathsf{s,v,x}}|\alpha_\lambda\rangle_{\mathsf{a}}\geq\delta$.

不失一般性，我们假设前者成立，但同样的论证也适用于后者。我们将证明这会与针对 OTS 一次性不可伪造性的归约产生矛盾。事实上，我们将考虑一个更弱的定义，其中对手不会收到签名。

在输入验证密钥vk_1 和建议 $|\alpha_\lambda\rangle_{\mathsf{a}}$ 后，归约算法均匀采样 $(\mathsf{vk}_0,\mathsf{sk}_0)\leftarrow\mathsf{SGen}(1^\lambda)$，并设置 $\mathsf{vk}=\{\mathsf{vk}_0,\mathsf{vk}_1\}$。然后计算 $\sigma_0\leftarrow\mathsf{Sign}(\mathsf{sk}_0,0)$ 并

$$U_{\mathsf{v,x,a}}|\mathsf{vk}\rangle_{\mathsf{v}}|0,\sigma_0\rangle_{\mathsf{x}}|\alpha_\lambda\rangle_{\mathsf{a}}$$

以及 r 返回在计算基下对 x 寄存器进行测量的结果。

现在，我们分析对于固定密钥对 $(\mathsf{vk}_1,\mathsf{sk}_1)$，该归约生成有效签名的成功概率。记 Σ_1 为在 vk_1, 下对 1的所有有效签名的集合，并记为 $\sigma_1=\mathsf{Sign}(\mathsf{sk}_1,1)$。那么，归约的成功概率等于

$$\begin{aligned}&\sum_{\sigma_1'\in\Sigma_1}|\Sigma_1|\cdot\left\|\left\langle1,\sigma_1'\right|_{\mathsf{x}}U_{\mathsf{v,x,a}}|\mathsf{vk}\rangle_{\mathsf{v}}|0,\sigma_0\rangle_{\mathsf{x}}|\alpha_\lambda\rangle_{\mathsf{a}}\right\|^2\\&\qquad\geq\left\|\langle1,\sigma_1|_{\mathsf{x}}U_{\mathsf{v,x,a}}|\mathsf{vk}\rangle_{\mathsf{v}}|0,\sigma_0\rangle_{\mathsf{x}}|\alpha_\lambda\rangle_{\mathsf{a}}\right\|^2\\&\qquad\geq\left|\langle\mathsf{vk}|_{\mathsf{v}}\langle1,\sigma_1|_{\mathsf{x}}\langle\alpha_\lambda|_{\mathsf{a}}U_{\mathsf{v,x,a}}|\mathsf{vk}\rangle_{\mathsf{v}}|0,\sigma_0\rangle_{\mathsf{x}}|\alpha_\lambda\rangle_{\mathsf{a}}\right|^2\\&\qquad=\left|\langle\mathsf{vk},\mathsf{sk}|_{\mathsf{s}}\langle\mathsf{vk}|_{\mathsf{v}}\langle1,\sigma_1|_{\mathsf{x}}\langle\alpha_\lambda|_{\mathsf{a}}\left(U_{\mathsf{v,x,a}}|\mathsf{vk}\rangle_{\mathsf{v}}\otimes\mathsf{Id}_{\mathsf{s}}\right)|\mathsf{vk},\mathsf{sk}\rangle_{\mathsf{s}}|0,\sigma_0\rangle_{\mathsf{x}}|\alpha_\lambda\rangle_{\mathsf{a}}\right|^2\end{aligned}$$

其中，第二个不等式源于插入 $\langle\mathsf{vk}|_{\mathsf{v}}$ 和 $\langle\alpha_\lambda|_{\mathsf{a}}$ 只会减小范数。现在，考虑 (vk,sk) 的随机选择，归约的成功概率可以下界为

$$\begin{aligned}&\mathbb{E}_{(\mathsf{vk},\mathsf{sk})}\left[\left|\langle\mathsf{vk},\mathsf{sk}|_{\mathsf{s}}\langle\mathsf{vk}|_{\mathsf{v}}\langle1,\sigma_1|_{\mathsf{x}}\langle\alpha_\lambda|_{\mathsf{a}}\left(U_{\mathsf{v,x,a}}|\mathsf{vk}\rangle_{\mathsf{v}}\otimes\mathsf{Id}_{\mathsf{s}}\right)|\mathsf{vk},\mathsf{sk}\rangle_{\mathsf{s}}|0,\sigma_0\rangle_{\mathsf{x}}|\alpha_\lambda\rangle_{\mathsf{a}}\right|^2\right]\\&\geq\left|\mathbb{E}_{(\mathsf{vk},\mathsf{sk})}\left[\langle\mathsf{vk},\mathsf{sk}|_{\mathsf{s}}\langle\mathsf{vk}|_{\mathsf{v}}\langle1,\sigma_1|_{\mathsf{x}}\langle\alpha_\lambda|_{\mathsf{a}}\left(U_{\mathsf{v,x,a}}|\mathsf{vk}\rangle_{\mathsf{v}}\otimes\mathsf{Id}_{\mathsf{s}}\right)|\mathsf{vk},\mathsf{sk}\rangle_{\mathsf{s}}|0,\sigma_0\rangle_{\mathsf{x}}|\alpha_\lambda\rangle_{\mathsf{a}}\right]\right|^2\\&\geq\delta\end{aligned}$$

其中，第一个不等式由詹森不等式得出。这与 OTS 的不可伪造性相矛盾，从而完成了证明。

□

3 量子公钥加密

下面我们将定义并构造本文的核心密码学原语，称之为量子公钥加密。

3.1 定义

该原语的语法几乎逐字取自 [2], ，尽管在本文中我们考虑的是更强的安全性概念。为便于记号，我们定义该原语用于加密一位消息，但通过标准的逐位加密，很容易将这一概念及相应构造推广到多位。多位构造的安全性可由标准的混合论证得到。

定义 3.1 (QPKE)。一个量子公钥加密（*PKE*）方案定义为算法元组 (SKGen, PKGen, Enc, Dec)，满足：

- sk $\leftarrow$ SKGen(1^λ)：一种 PPT 算法，在输入安全参数 1^λ 后输出一个秘密比特字符串 sk。

- (ρ, 公钥) $\leftarrow$ PKGen(sk)：一种量子多项式时间算法，以密钥 sk 为输入，输出一个（可能为混合态的）量子态 ρ 和一个比特串公钥。
- ct $\leftarrow$ Enc(ρ,pk m)：一种量子多项式时间算法，以公钥 (ρ,pk) 和消息 $m \in \{0,1\}$ 作为输入，输出密文 ct。
- $m \leftarrow$ Dec(sk,ct)：一种量子多项式时间算法，以私钥 sk 和密文 ct 为输入，输出消息 $m \in \{0,1\}$。

一个QPKE方案（SKGen、PKGen、Enc、Dec）满足 正确性，当且仅当对于所有 $\lambda \in \mathbb{N}$ 和所有 $m \in \{0,1\}$，均有：

$$\Pr\left[m = \mathsf{Dec}(\mathsf{sk},\mathsf{ct}) : \mathsf{sk} \leftarrow \mathsf{SKGen}(1^\lambda); (\rho,\mathsf{pk}) \leftarrow \mathsf{PKGen}(\mathsf{sk}); \mathsf{ct} \leftarrow \mathsf{Enc}(\rho,\mathsf{pk},m)\right] = 1.$$

永久安全性。 接下来，我们定义量子公钥加密的永久安全性 这一安全概念。通俗地说，我们要求消息对攻击者无条件隐藏，即使允许量子多项式时间攻击者任意篡改公钥也是如此。不过，攻击者只会获得公钥的单份副本 。

定义 3.2 （永久安全性）。 对于一族 QPT 算法 $\{\mathcal{A}_\lambda\}_{\lambda\in\mathbb{N}}$，我们将实验 $\mathsf{Exp}^{\mathcal{A}_\lambda}(1^\lambda, m)$ 定义如下：

1. 采样sk $\leftarrow$ SKGen(1^λ)，并且(ρ, 公钥) $\leftarrow$ PKGen(sk)，然后将相应的公钥(ρ,公钥)发送给 $\mathcal{A}_\lambda$。
2. $\mathcal{A}_\lambda$ 返回两个量子寄存器。第一个寄存器被解析为修改后的公钥寄存器，而第二个寄存器是任意的，将被称为对手的内- 部寄存器。 3.通过将由Enc(·, 公钥 m) 定义的映射应用于对手在上一轮返回的公钥寄存器，计算密文。

4. 实验的输出定义为密文与对手的内部寄存器的联合状态。

那么，如果存在可忽略函数 negl，使得对于所有 $\lambda \in \mathbb{N}$ 和所有量子多项式时间 $\mathcal{A}_\lambda$，均有永久安全性，我们就称 QPKE 方案 (SKGen, PKGen, Enc, Dec) 满足该性质：

$$\mathsf{Td}\left(\mathsf{Exp}^{\mathcal{A}_\lambda}(1^\lambda, 0), \mathsf{Exp}^{\mathcal{A}_\lambda}(1^\lambda, 1)\right) = \mathsf{negl}(\lambda).$$

我们对上述定义作几点说明。首先，我们指出，只要相应扩展加密方案的语法，该定义就可以轻松推广到多比特消息的情形。我们还提到，另一种定义也可以允许对手对实验的输出进行任意后处理。然而，由于迹距离具有单调性，我们的定义与之等价，而且可以说更简单。

我们定义的一个重要特点（也是它与先前工作的区别）是，攻击者可以任意修改量子态，但不能篡改经典信息（例如公钥 pk 或密文 ct）。这模拟了认证经典信道的存在；我们假设这些信道能够忠实地传递经典信息。值得注意的是，标准经典PKE 的概念也采用了相同的假设（尽管这一点不那么显而易见）：在 CPA/CCA 安全性实验中，加密算法的输入始终是由挑战者采样的正确公钥。当然，这一限制是必要的，因为如果允许攻击者任意选择公钥，那么该定义就不可能实现。

最后，我们提到，更强的定义将允许对手看到数量为多项式的公钥副本，而不是仅看到一个。不幸的是，[2] 的工作表明，如果攻击者获得了足够多的公钥副本，并且可以在无界时间内运行，则其针对任何量子公钥加密都可以发起密钥恢复攻击。这立即排除了在存在数量为多项式的公钥副本时具有永久安全性的任何量子公钥加密，因为无界区分器可以简单地运行这样的密钥恢复算法，并使用诚实解密算法解密挑战密文。为克服这一限制，我们定义计算安全性的概念。

计算安全性。我们定义量子公钥加密的较弱计算安全性概念，其中要求消息仅对计算有界对手保持隐藏。其要点在于，即使对手能够获取公钥的多个副本，该性质仍然可以成立。下面给出形式化定义。

定义3.3（计算安全性）。对于一族 QPT 算法 $\{\mathcal{A}_\lambda\}_{\lambda\in\mathbb{N}}$，我们将实验 $\mathsf{Exp}^{\mathcal{A}_\lambda}(1^\lambda, m, n)$ 定义如下：

1.采样 $\mathsf{sk} \leftarrow \mathsf{SKGen}(1^\lambda)$，并用 $\{(\rho_i, \text{公钥}_i) \leftarrow \mathsf{PKGen}(\mathsf{sk})\}_{i=1,\ldots,n}$，然后将相应的公钥（$\rho_i$，公钥$_i$）发送给 $\mathcal{A}_\lambda$。2. $\mathcal{A}_\lambda$ 返回两个量子寄存器。第一个寄存器被解析为修改后的公钥寄存器，而第二个寄存器是任意的，将被称为对手的内部寄存器。3. 通过将 $\mathsf{Enc}(\cdot, \text{公钥}_1, m)$ 定义的映射应用于对手在上一轮返回的公钥寄存器，计算密文。4. 实验的输出定义为密文与对手内部寄存器的联合状态。

然后，我们称 QPKE方案 (SKGen,PKGen,Enc,Dec)满足 计算安全性 ，如果存在一个可忽略函数 negl，使得对于所有 $\lambda \in \mathbb{N}$、所有多项式 $n = n(\lambda)$ 以及所有 QPT $\mathcal{A}_\lambda$，都有以下分布

$$\mathsf{Exp}^{\mathcal{A}_\lambda}(1^\lambda, 0, n) \approx \mathsf{Exp}^{\mathcal{A}_\lambda}(1^\lambda, 1, n)$$

在计算上不可区分。

3.2 永久安全的量子公钥加密

我们将在下文介绍该方案。作为唯一的计算性构件，我们假设存在一个抗量子安全的强存在不可伪造一次性签名方案 (SGen, Sign, Ver)，参见第 2.4 节。如前所述，该方案可由任意抗量子安全的单向函数构造。

- SKGen(1^λ):
  - Sample two key pairs $(\mathsf{sk}_0, \mathsf{vk}_0) \leftarrow \mathsf{SGen}(1^\lambda)$ and $(\mathsf{sk}_1, \mathsf{vk}_1) \leftarrow \mathsf{SGen}(1^\lambda)$.
  - Compute $\sigma_0 \leftarrow \mathsf{Sign}(\mathsf{sk}_0, 0)$ and $\sigma_1 \leftarrow \mathsf{Sign}(\mathsf{sk}_1, 1)$.
  - Sample a bit $d_0 \leftarrow \{0,1\}$.
  - Return $\mathsf{sk} = (\mathsf{vk}_0, \mathsf{vk}_1, \sigma_0, \sigma_1, d_0)$.
- PKGen(sk):
  - 定义状态
    $$|\Psi\rangle = \frac{|0,\sigma_0\rangle + (-1)^{d_0}|1,\sigma_1\rangle}{\sqrt{2}}.$$
    通过制备一个 EPR 对，并在第一个量子比特的值控制下，将签名的比特通过受控非门复制到辅助寄存器中，即可高效地计算出该状态。随后，可通过使用 d_0控制 Z 门的施加，从而添加相对相位。
  - 将公钥 ρ 的量子部分设为状态 $|\Psi\rangle$，并将公钥的经典部分和经典私钥设为 pk $=$ (vk_0,vk_1)。
- Enc(ρ, pk m):
  - 将 ρ 投影到 0 和 1 的有效签名子空间，分别对应 vk_0 和 vk_1,。更准确地说，令 Σ_0 和 Σ_1 分别表示在 vk_0和 vk_1,下对 0 和 1 的接受签名，并考虑投影算子
    $$\Pi = \sum_{\sigma\in\Sigma_0} |0,\sigma\rangle\langle 0,\sigma| + \sum_{\sigma\in\Sigma_1} |1,\sigma\rangle\langle 1,\sigma|.$$
    施加投影测量 $\{\Pi$,Id $-\Pi\}$，若测量得到第二个结果，则中止执行（返回 $\perp$）。注意，可以通过相干地运行验证算法，将输出位通过受控非门复制到单独的寄存器中，再对其进行测量，从而高效实现该测量。
  - 测量残余状态的哈达玛基，获得比特串（d_1,d_2），其中我们将测量结果的第一比特记为 $d_1 \in \{0,1\}$，其余部分记为 d_2。

– 将以下内容作为经典密文返回：

$$\mathsf{ct} = (m \oplus d_1, d_2). \tag{3.1}$$

- Dec(sk, ct)：

– 解析 $\mathsf{ct} = (\mathsf{ct}_1, \mathsf{ct}_2)$，其中 $\mathsf{ct}_1 \in \{0,1\}$ 是一个比特，并返回

$$m = d_0 \oplus \mathsf{ct}_1 \oplus \mathsf{ct}_2 \cdot (\sigma_0 \oplus \sigma_1). \tag{3.2}$$

分析。 我们声称该方案满足正确性。首先注意，作为输入的状态 ρ 属于投影算子 Π的像空间，该投影算子如上所定义。因此，应用投影测量 $\{\Pi, \mathsf{Id} - \Pi\}$ 后，必定得到与 Π 相关联的结果，且状态不会发生改变。对状态 $|\Psi\rangle$应用哈达玛变换，得到

$$\mathsf{H}|\Psi\rangle \propto \sum_{d_1,d_2} (-1)^{(d_1,d_2)\cdot(0,\sigma_0)} |d_1,d_2\rangle + (-1)^{d_0 \oplus (d_1,d_2)\cdot(1,\sigma_1)} |d_1,d_2\rangle = \sum_{d_1,d_2\,:\,(d_1,d_2)\cdot(1,\sigma_0\oplus\sigma_1)=d_0} |d_1,d_2\rangle,$$

省略整体归一化因子。因此，测量会返回一个均匀随机的比特串 (d_1, d_2)，满足

$$d_1 \oplus d_2 \cdot (\sigma_0 \oplus \sigma_1) = d_0.$$

将式 (3.1) 代入式 (3.2)，并利用这一关系，可得

$$d_0 \oplus \mathsf{ct}_1 \oplus \mathsf{ct}_2 \cdot (\sigma_0 \oplus \sigma_1) = d_0 \oplus (m \oplus d_1) \oplus d_2 \cdot (\sigma_0 \oplus \sigma_1) = m,$$

正如所需。接下来，我们证明该方案满足永久安全性。

定理 3.4 (永久安全性)。 如果量子安全单向函数存在，则量子公钥加密(SKGen,PKGen, Enc, Dec) 满足永久安全性。

证明。我们通过定义一系列混合实验来展开论证，并证明从任何（可能是无界的）算法的角度来看，这些混合实验是不可区分的。为方便起见，我们定义

$$\mathsf{Adv}(i) = \mathsf{Td}\left(\mathsf{Hyb}_i^{\mathcal{A}_\lambda}(1^\lambda, 0), \mathsf{Hyb}_i^{\mathcal{A}_\lambda}(1^\lambda, 1)\right).$$

- $\mathsf{Hyb}_0^{\mathcal{A}_\lambda}(1^\lambda, b)$: 这是定义 3.2 中所定义的原始实验 $\mathsf{Exp}^{\mathcal{A}_\lambda}(1^\lambda, b)$。
- $\mathsf{Hyb}_1^{\mathcal{A}_\lambda}(1^\lambda, b)$：在该实验中，我们修改PKGen算法，在输出 ρ之前，在计算基下测量状态 $|\Psi\rangle$。

由于实验中未使用 SKGen算法的结果 sk，我们只需说明这一修改不会改变 (pk ρ) 的约化量子态。事实确实如此，因为根据标准的 Pauli Z 旋转平均论证，添加随机相位等同于在计算基中进行测量。因此，从对手的角度来看，这两个实验完全相同，故 Adv(0) =Adv(1)。

• $\mathrm{Hyb}_2^{\mathcal{A}_\lambda}(1^\lambda, b)$：在此实验中，我们进一步修改 PKGen算法，按如下方式采样状态 ρ。抛一枚随机硬币 $c \leftarrow \{0,1\}$。如果 $c=0$，则返回 $|0,\sigma_0\rangle\langle 0,\sigma_0|$；否则返回 $|1,\sigma_1\rangle\langle 1,\sigma_1|$。

注意 ，修改后的 PKGen 算法返回的状态 ρ 是经典混合态 re

$$\rho = \frac{|0,\sigma_0\rangle\langle 0,\sigma_0| + |1,\sigma_1\rangle\langle 1,\sigma_1|}{2}$$

该状态与前一个混合步骤中返回的状态相同。因此，Adv(1) =Adv(2)。接下来，我们将对手在实验第 2 步返回的修改后的公钥寄存器的约化密度矩阵记为 ρ^* 。我们假设对手返回的状态 ρ^* 使得加密算法以非可忽略的概率接受（即不执行中止）；否则，Adv(2) = negl(λ)，结论即得。于是可以证明，状态 ρ^*投影到 Π的像空间后，与 PKGen 算法生成的状态在迹距离上必然相差可忽略。

命题 3.5. 存在一个可忽略函数 negl，使得对于 $c \in \{0,1\}$ Gen 算法中抛掷硬币的结果，

$$\mathsf{Td}\left(\frac{\Pi\rho^*\Pi}{\mathsf{Tr}\left(\Pi\rho^*\right)}, |c,\sigma_c\rangle\langle c,\sigma_c|\right) = \mathsf{negl}(\lambda).$$

命题 *3.5* 的证明。 证明通过归约到一次性签名方案的不可伪造性得出。确切地说，反设测量后的状态与 $|c,\sigma_c\rangle$ 的迹距离非可忽略。根据式 (2.1)，这等价于：若在计算基下进行测量，则得到结果 (c,σ_c) 的概率比 1 小一个非可忽略量。由于测量后的状态支撑于 Π 的值域上，因此若在计算基下进行测量，则以非可忽略的概率必定会得到一个结果 (z,σ)，使得

$$(z,\sigma) \neq (c,\sigma_c) \quad \text{and} \quad \mathsf{Ver}(\mathsf{vk}_z, z, \sigma) = 1,$$

也就是说，$(z,\sigma) \neq (c,\sigma_c)$ 是一个有效的消息-签名对。由于对手、投影测量 $\{\Pi, I-\Pi\}$ 和标准基测量都在量子多项式时间内运行，且投影测量以非可忽略的概率返回 Π，这与一次性签名方案的强存在不可伪造性相矛盾。

□

我们得出结论 通过证明消息 m 在最后一个实验中具有统计隐藏性 t.

命题 3.6。 存在一个可忽略函数 negl，使得 Adv(2) =negl(λ)。

命题 *3.6* 的证明。根据命题 3.5，测量后的量子态与量子态 $|c,\sigma_c\rangle$ 仅有可忽略的差异。由于后者是纯态，且纯态的扩展总是处于张量积中，根据乌尔曼定理可知，测量后的寄存器与对手的内部寄存器近似处于张量积中。因此，只需证明当输入为 $|c,\sigma_c\rangle$ 时，Enc 算法的输出分布不依赖于消息 m 。为此，注意到在哈达玛基中旋转后的量子态，除整体归一化因子外，可表示为

$$\mathsf{H}\,|c,\sigma_c\rangle \propto \sum_{d'} (-1)^{d'\cdot(c,\sigma_c)}\,\left|d'\right\rangle,$$

因此，测量会返回均匀随机的比特串 $d' = (d_1, d_2)$。特别地，密文 $=(m \oplus d_1, d_2)$ 对于 $m \in \{0,1\}$具有相同的分布。如上所述，它与对手的内部寄存器之间也仅以可忽略的差距近似独立，因此结论成立。 □

根据断言 3.6，我们有

$$\mathsf{Adv}(0) = \mathsf{Adv}(1) = \mathsf{Adv}(2) = \mathsf{negl}(\lambda),$$

由此，定理 3.4 的证明得以完成。 □

3.3 计算安全量子公钥加密

我们的方案假设存在一个量子安全的强存在性不可伪造的一次性签名方案 (SGen,Sign,Ver) 和一个量子安全的伪随机函数 PRF。假设存在任意量子安全的单向函数，即可构造这两种构件。

- SKGen(1^λ):
  - 采样一个密钥 $k \leftarrow \{0,1\}^\lambda$ 并设置 $\mathsf{sk} = k$。
- PKGen(sk):
  - 均匀采样一对 $(r_0, r_1) \leftarrow \{0,1\}^\lambda$ 并计算

$$(\mathsf{sk}_0, \mathsf{vk}_0) \leftarrow \mathsf{SGen}(1^\lambda; \mathsf{PRF}(k, r_0)) \quad \text{and} \quad (\mathsf{sk}_1, \mathsf{vk}_1) \leftarrow \mathsf{SGen}(1^\lambda; \mathsf{PRF}(k, r_1)).$$

  - 计算 $\sigma_0 \leftarrow \mathsf{Sign}(\mathsf{sk}_0, 0)$ 和 $\sigma_1 \leftarrow \mathsf{Sign}(\mathsf{sk}_1, 1)$。
  - 定义该状态

$$|\Psi\rangle = \frac{|0,\sigma_0\rangle + |1,\sigma_1\rangle}{\sqrt{2}}.$$

    该状态可通过制备一个 EPR 对，并根据第一个量子比特的值，将签名的各位受控地通过受控非门复制到一个辅助寄存器中，从而高效计算。
  - 将公钥的量子部分 ρ 设为状态 $|\Psi\rangle$，并将公钥的经典部分和经典私钥设为 $\mathsf{pk} = (\mathsf{vk}_0, \mathsf{vk}_1, r_0, r_1)$。
- Enc(ρ, 公钥 m):
  - 将 ρ 投影到 0和1的有效签名子空间上，分别对应 vk_0 和 vk_1,。更准确地说，令 Σ_0 和 Σ_1 分别表示在 vk_0和 vk_1,下对 0 和 1 的接受签名集合，并考虑投影算子

$$\Pi = \sum_{\sigma \in \Sigma_0} |0,\sigma\rangle\langle 0,\sigma| + \sum_{\sigma \in \Sigma_1} |1,\sigma\rangle\langle 1,\sigma| .$$

    应用投影测量 $\{\Pi, \mathsf{Id} - \Pi\}$，如果测量返回第二个结果，则中止执行（返回 $\perp$）。注意，可以通过相干地运行验证算法，在单独的寄存器上对输出比特应用受控非门，然后对其进行测量来高效地实现该测量。
  - 根据消息 m 进行经典控制，将 Z^m 算子作用于 ρ 的第一个量子比特。

– 将密文 ct 设为残余状态，并附带 (r_0, r_1)。

- Dec(sk, ct):
  – 使用秘密密钥 k 重新计算

$$(\mathsf{sk}_0, \mathsf{vk}_0) \leftarrow \mathsf{SGen}(1^\lambda; \mathsf{PRF}(k, r_0)) \quad \text{and} \quad (\mathsf{sk}_1, \mathsf{vk}_1) \leftarrow \mathsf{SGen}(1^\lambda; \mathsf{PRF}(k, r_1)).$$

  以及 $\sigma_0 \leftarrow \mathsf{Sign}(\mathsf{sk}_0, 0)$ 和 $\sigma_1 \leftarrow \mathsf{Sign}(\mathsf{sk}_1, 1)$。
  – 在该

$$\left\{ \frac{|0, \sigma_0\rangle + |1, \sigma_1\rangle}{\sqrt{2}}, \frac{|0, \sigma_0\rangle - |1, \sigma_1\rangle}{\sqrt{2}} \right\}$$

  基下对 ct 的量子态进行测量，并返回相应的结果。

分析。 为说明该方案满足正确性，首先注意到，PKGen算法中定义的状态 $|\Psi\rangle$位于投影算子 Π的像空间中。因此，投影测量{Π,Id $-\ \Pi$} 在 $|\Psi\rangle$上充当恒等操作。然后，加密算法输出的状态对应于

$$(\mathsf{Z}^m \otimes \mathsf{Id}) \frac{|0, \sigma_0\rangle + |1, \sigma_1\rangle}{\sqrt{2}} = \frac{|0, \sigma_0\rangle + (-1)^m |1, \sigma_1\rangle}{\sqrt{2}}.$$

因此，解密算法的输出必然等于 m。接下来，我们证明该方案在计算意义上是安全的。

定理 3.7 （计算安全性）。 如果量子安全单向函数存在，那么 QPKE (SKGen,PKGen,Enc,Dec) 满足计算安全性。

证明。我们首先定义一系列混合实验，并证明从任何量子多项式时间算法的角度来看，它们是不可区分的。

- $\mathsf{Hyb}_0^{\mathcal{A}_\lambda}(1^\lambda, b)$：这是定义3.3中定义的原始实验 $\mathsf{Exp}^{\mathcal{A}_\lambda}(1^\lambda, b, n)$。

- $\mathsf{Hyb}_1^{\mathcal{A}_\lambda}(1^\lambda, b)$: 在此实验中，我们通过惰性采样来模拟伪随机函数的输出，即每次调用 PKGen算法时，实验都会均匀采样一个元组 $(r_0, r_1, \tilde{r}_0, \tilde{r}_1)$，并将后两项用作一次性签名方案的随机数。为保持一致，实验会维护所有此类元组的列表。

注意，这两个混合实验之间的唯一差异在于 OTS 的随机硬币采样方式。因此，根据 PRF 的伪随机性，这两个混合实验在计算上不可区分。注意，在第二个混合实验中，公钥的不同副本现在彼此独立。

- $\mathsf{Hyb}_2^{\mathcal{A}_\lambda}(1^\lambda, b)$：在此实验中，我们进一步修改 PKGen 算法的首次调用，按如下方式采样状态 ρ 。抛掷一枚随机硬币 $c \leftarrow \{0, 1\}$。如果 $c = 0$ ，则返回 $|0, \sigma_0\rangle\langle 0, \sigma_0|$；否则返回 $|1, \sigma_1\rangle\langle 1, \sigma_1|$。

注意到　　t 由修改后的PKGen算法返回的状态 ρ 是经典混合　　re

$$\rho = \frac{|0,\sigma_0\rangle\langle 0,\sigma_0| + |1,\sigma_1\rangle\langle 1,\sigma_1|}{2}.$$

通过直接应用引理 2.7，我们可以得出结论：这两个混合实验在计算上不可区分。此时，我们可以援引主张 3.5（在定理3.4的证明中），从而证明对手在安全实验中返回的状态 ρ^* 与某个基态之间的迹距离必然是可忽略的。最后，只需注意到：如果算法以任意基态作为输入，则0 的加密和 1 的加密的分布除相差一个全局相位外完全相同，即可完成证明。

□

4 双消息量子密钥分发

下面我们概述如何使用 QPKE方案（SKGen、PKGen、Enc、Dec）构造一种仅需两轮交互的量子密钥分发协议，正如引言中所述。

4.1 定义

我们给出永久安全场景下量子密钥分发的形式化定义，即要求攻击者仅在协议执行期间受到计算能力限制。为方便起见，我们采用针对双消息协议的特定语法，但这些定义可以自然地扩展到更一般的交互式场景。

定义 4.1（双消息量子密钥分发）。量子密钥分发（QKD）方案定义为由以下算法组成的元组（QKDFirst、QKDSecond、QKDDecode）：

- （msg μ，st） $\leftarrow$ QKDFirst（1^λ）：一种量子多项式时间算法，其输入安全参数 1^λ 后，输出一条消息，包括一个经典分量 msg、一个（可能为混合态的）量子态 μ 以及一个内部状态 st。

- $\{$（resp η，k） $\perp\}$ $\leftarrow$ QKDSecond（msg μ）：一种量子多项式时间算法，其输入第一条消息（msg μ）后，输出一个响应，包括一个经典分量 resp、一个（可能为混合态的）量子态 η，以及一个密钥 $k \in \{0,1\}^\lambda$；或者输出一个表示拒绝的特殊符号 $\perp$。

- $\{k, \perp\}$ $\leftarrow$ QKDDecode（st，resp η）：一种量子多项式时间算法，其输入内部状态 st 和响应（resp η）后，返回一个密钥 $k \in \{0,1\}^\lambda$，或者返回一个表示拒绝的特殊符号 $\perp$。

我们称量子密钥分发方案 (QKDFirst, QKDSecond, QKDDecode) 满足正确性，如果对所有$\lambda \in \mathbb{N}$，均有：

$$\Pr\left[\perp = \mathsf{QKDSecond}(\mathsf{msg}, \mu) : (\mathsf{msg}, \mu, \mathsf{st}) \leftarrow \mathsf{QKDFirst}(1^\lambda)\right] = 0$$

and

$$\Pr\left[k = \mathsf{QKDDecode}(\mathsf{st}, \mathsf{resp}, \eta) : \begin{array}{l}(\mathsf{msg}, \mu, \mathsf{st}) \leftarrow \mathsf{QKDFirst}(1^\lambda); \\ (\mathsf{resp}, \eta, k) \leftarrow \mathsf{QKDSecond}(\mathsf{msg}, \mu)\end{array}\right] = 1.$$

永久安全性。 接下来，我们定义量子密钥分发的永久安全性这一安全概念，它包含两项性质。隐私性要求密钥 k 在协议执行期间面对计算有界对手时仍无条件保密。此外，与量子密钥分发的标准做法一致，我们假设存在一个经过认证的经典信道，并通过禁止对手篡改经典消息来对其建模。另一方面，可验证性要求任何计算有界对手都无法在不被 Alice 和 Bob 任一方察觉的情况下，使双方对密钥产生分歧。

定义 4.2（永久安全性）。 对于一组QPT 算法 $\{\mathcal{A}_\lambda\}_{\lambda\in\mathbb{N}}$，我们将实验 $\mathsf{QKDSec}^{\mathcal{A}_\lambda}(1^\lambda)$ 定义如下：

1. 示例（msg, μ,st) $\leftarrow$ 量子密钥分发First(1^λ) 并将对应的第一条消息 (msg μ) 发送给 $\mathcal{A}_\lambda$.

2. $\mathcal{A}_\lambda$ 返回两个量子寄存器。第一个寄存器被解析为修改后的第一条消息，而第二个寄存器是任意的，称为对手的内部寄存器。

3.计算 {(resp η, k_0) $\perp$}，通过将由量子密钥分发Second(msg $\cdot$)定义的映射应用于对手在上一轮返回的经修改的第一条消息寄存器。

(a) 如果上述消息为 $\perp$，则令 (k_0, k_1) $=(\perp,\perp)$ 并结束实验。(b) 否则，将 (resp η) 连同其内部状态一并返回给对手。

4. $\mathcal{A}_\lambda$ 再次返回两个量子寄存器。第一个寄存器被解析为修改后的响应，而第二个寄存器是对手的内部寄存器。

5. 通过将 QKDDecode(st, resp $\cdot$) 定义的映射应用于对手在上一轮返回的经过修改的响应寄存器，计算 $\{k_1, \perp\}$。如果结果为 $\perp$，则设置 $k_1 = \perp$。

6. 实验的输出定义为对手的内部寄存器。

然后，如果以下性质成立，我们称一个量子密钥分发方案 (QKDFirst,QKDSecond,QKDDecode) 满足永久安全性。

- (隐私)存在一个可忽略函数negl，使得对于所有 $\lambda \in \mathbb{N}$ 以及所有量子多项式时间 $\mathcal{A}_\lambda$ ，都有

$$\mathsf{Td}\left(\left\{\mathsf{QKDSec}^{\mathcal{A}_\lambda}(1^\lambda), k_0, k_1\right\}, \left\{\mathsf{QKDSec}^{\mathcal{A}_\lambda}(1^\lambda), \tilde{k}_0, \tilde{k}_1\right\}\right) = \mathsf{negl}(\lambda)$$

~其中变量 k_0 和 k_1 在实验中定义，而对于 $b \in \{0,1\}$， k_b 定义为

$$\begin{cases} \tilde{k}_b = \perp & \text{if } k_b = \perp \\ \tilde{k}_b \leftarrow \{0,1\}^\lambda & \text{otherwise.} \end{cases}$$

- (可验证性)存在一个可忽略函数negl，使得对于所有 $\lambda \in \mathbb{N}$ 以及所有量子多项式时间 $\mathcal{A}_\lambda$，均有

$$\Pr[k_0 \neq k_1 \text{ and } k_1 \neq \perp] = \mathsf{negl}(\lambda)$$

其中， k_0 和 k_1 在实验中定义。

请注意，对于双消息协议，上述可验证性的定义是紧的：攻击者可以在第一轮什么也不做并阻断第二条消息，从而轻易导致两个密钥不一致。在这种情况下，根据正确性，k_0 会是一个有效密钥，而由于第二条消息从未送达，k_1 会被设置为 $\perp$。

4.2 基于量子公钥加密的双消息量子密钥分发

现在我们可以描述我们的量子密钥分发协议了。所需组件包括一个 QPKE 方案 (SKGen, PKGen, Enc, Dec) 和一个一次性签名方案 (SGen, Sign, Ver)，二者都可以由单向函数构造。此外，我们还将使用一个通用哈希函数族

$$\mathsf{Hash} : \{0,1\}^{4\lambda} \to \{0,1\}^{\lambda}$$

它无条件存在。为方便起见，我们用 $s(\lambda)$ 表示对大小为 λ 的消息进行签名所得签名的大小。下面给出该协议。

- 量子密钥分发第一步(1^{λ}):
  - 对于所有 $i = 1, \ldots, 4\lambda + s(4\lambda)$，生成一个量子公钥加密密钥对

$$\mathsf{sk}_i \leftarrow \mathsf{SKGen}(1^{\lambda}) \quad \text{and} \quad (\rho_i, \mathsf{pk}_i) \leftarrow \mathsf{PKGen}(\mathsf{sk}_i).$$

  - 将第一条消息设为 $\mathsf{msg} = (\mathsf{pk}_1, \ldots, \mathsf{pk}_{4\lambda+s(4\lambda)})$ 和 $\mu = \rho_1 \otimes \cdots \otimes \rho_{4\lambda+s(4\lambda)}$。
- 第二消息量子密钥分发(msg μ):
  - 采样一个 OTS 密钥对(vk,zk) $\leftarrow$ SGen(1^{λ})、一个密钥 $k \leftarrow \{0,1\}^{4\lambda}$ 和一个通用哈希函数 Hash。– 计算 $\sigma \leftarrow \mathsf{Sign}(\mathsf{zk}\ k)$。– 对于所有 $i = 1, \ldots, 4\lambda + s(4\lambda)$ 计算

$$\{\mathsf{ct}_i \leftarrow \mathsf{Enc}(\rho_i, \mathsf{pk}_i, k_i)\}_{i \le 4\lambda} \quad \text{and} \quad \{\mathsf{ct}_i \leftarrow \mathsf{Enc}(\rho_i, \mathsf{pk}_i, \sigma_i)\}_{i > 4\lambda}$$

    其中，$k = (k_1, \ldots, k_{4\lambda})$ 和 $\sigma = (\sigma_1, \ldots, \sigma_{s(4\lambda)})$。
  - 如果任何加密过程失败，则返回 $\perp$。
  - 否则，将响应设为 $\mathsf{resp} = (\mathsf{Hash}, \mathsf{vk}, \mathsf{ct}_1, \ldots, \mathsf{ct}_{4\lambda+s(4\lambda)})$，不存在量子态。
  - 将密钥设置为 $K =$哈希(k)。
- QKD解码(st, resp):
  - For all $i = 1, \ldots, 4\lambda + s(4\lambda)$ compute

$$\{k_i \leftarrow \mathsf{Dec}(\mathsf{sk}_i, \mathsf{ct}_i)\}_{i \le 4\lambda} \quad \text{and} \quad \{\sigma_i \leftarrow \mathsf{Dec}(\mathsf{sk}_{\lambda+i}, \mathsf{ct}_{\lambda+i})\}_{i > 4\lambda}\,.$$

  - If $\mathsf{Ver}(\mathsf{vk}, k, \sigma) \neq 1$ return $\perp$.
  - Else, return $K = \mathsf{Hash}(k)$.

正确性直接由底层构件的正确性推出。接下来，我们证明该方案具有隐私性和可验证性。

定理 4.3. 如果量子安全单向函数存在，那么 QKD（QKDFirst，QKDSecond，QKDDecode）满足永久安全性（隐私性和可验证性）。

证明。我们首先证明该方案满足隐私性。我们将更改实验的语法，以明确包含对手的视图，即标志 abort $\in \{0,1\}$ ，该标志表示实验是否在步骤 5中中止。然后，只需证明密钥 K_0（如实验步骤 3 中所定义）和 K_1 （如实验步骤 5 中所定义）在给定变量的条件下，与均匀分布在统计上接近即可。

$$\left\{\mathsf{QKDSec}^{\mathcal{A}_\lambda}(1^\lambda), \mathsf{abort}\right\}.$$

作为第一步，我们声称，在上述视图中， k 的最小熵为 $H_\infty(k) \geq 3\lambda$ 。为证明这一点，我们首先考虑一个修改后的分布，其中区分器 未被提供 变量abort。然后，我们将$\mathsf{Hyb}_0^{\mathcal{A}_\lambda}(1^\lambda)$ 定义为原始实验$\mathsf{QKDSec}^{\mathcal{A}_\lambda}(1^\lambda)$ 的输出，其中原始实验如定义 4.2所定义。接着，对于 $i = 1,\ldots,4\lambda + s(4\lambda)$，我们定义混合实验 $\mathsf{Hyb}_i^{\mathcal{A}_\lambda}(1^\lambda)$ 如下。

- $\mathsf{Hyb}_i^{\mathcal{A}_\lambda}(1^\lambda)$：其定义与前一个混合实验相同，区别在于第 i 个密文 ct_i 的计算方式为

$$\mathsf{ct}_i \leftarrow \mathsf{Enc}(\rho_i, \mathsf{pk}_i, 0).$$

相邻输出的统计不可区分性可直接由 QPKE方案的永久安全性推出，即，

$$\mathsf{Td}\left(\mathsf{Hyb}_{i-1}^{\mathcal{A}_\lambda}(1^\lambda), \mathsf{Hyb}_i^{\mathcal{A}_\lambda}(1^\lambda)\right) = \mathsf{negl}(\lambda) \text{ for all } i = 1, \ldots, 4\lambda + s(4\lambda).$$

注意，在最后一个混合实验$\mathsf{Hyb}_{4\lambda+s(4\lambda)}^{\mathcal{A}_\lambda}(1^\lambda)$ 中，攻击者的视图在形式上独立于密钥 k ，因此 k 恰好具有 4λ 比特的熵。应用引理2.4已经表明， K_0 在统计上接近均匀分布，因为其分布独立于中止事件。

然而，对于 K_1而言情况并非如此，因为 $K_1 = \perp$ 是否取决于中止事件。将相同的论证反向应用，我们在 k的熵中仅损失一个可忽略的加项，因此可以得出，在原始实验中， $H_\infty(k) \geq 4\lambda - 1$ 。根据公式 (2.2)（平均情形最小熵的链式法则），在给定中止事件的条件下，有

$$\tilde{H}_\infty(k|\mathsf{abort}) \geq H_\infty(k) - 2 > 3\lambda$$

由于中止 $\in \{0,1\}$。根据引理 2.4， K_1 与均匀分布之间的统计距离上界为 $\varepsilon = 2^{-\lambda}$ ，因为

$$\tilde{H}_\infty(k|\mathsf{abort}) - 2\log\left(\frac{1}{\varepsilon}\right) \geq 3\lambda - 2\lambda = \lambda = \ell.$$

这表明， K_0 和 K_1 都在统计上接近均匀分布，并完成了永久安全性的证明。

关于可验证性，让我们反设存在一个会导致密钥不匹配 $k_0 \neq k_1$ 而不会导致解码算法拒绝的量子多项式时间对手，即 $k_1 \neq \perp$。那么，对手必然能够在 vk下，为消息 $k_1 \neq k_0$生成一个有效的消息-签名对（k_1, σ^*）。由于对手以量子多项式时间运行，这与一次性签名方案的不可伪造性相矛盾，从而得出我们的证明。 □

致谢

作者谨感谢 Khashayar Barooti 就量子公钥加密展开的诸多讨论，并感谢 Takashi Yamakawa 提出定理 A.1 的证明思路。G.M. 部分经费由德国联邦教育与研究部（BMBF）通过 6GEM 研究中心提供，项目资助编号为 16KISK038；另部分经费由德国研究联合会（DFG，德国研究基金会）通过德国卓越战略资助，项目编号为 EXC 2092 CASA – 390781972。M.W. 感谢欧盟（欧洲研究委员会，SYMOPTIC，101040907）、德国研究联合会（DFG，德国研究基金会）通过德国卓越战略（EXC 2092 CASA – 390781972）、BMBF 通过 QuBRA 项目，以及荷兰研究理事会（NWO 资助编号 OCENW.KLEIN.267）提供的支持。文中所表达的观点和意见仅代表作者本人，并不一定反映欧盟或欧洲研究委员会执行机构的立场。欧盟和资助机构均不对此承担责任。

参考文献

[1]Aaronson, S., Atia, Y., Susskind, L.：关于检测宏观叠加态的困难性。电子计算复杂性研讨会 **TR20-146**(2020)，https://eccc.weizmann.ac.il/report/2020/146

[2]Barooti, K., Grilo, A.B., Huguenin-Dumittan, L., Malavolta,G.,Sattath,O., Vu, Q., Walter, M.：量子密钥公钥加密。CoRR **abs/2306.07698**（2023）。https://doi.org/10.48550/arXiv.2306.07698，https://doi.org/10.48550/arXiv.2306.07698[3] Bartusek, J., Khurana, D.：带认证删除的密码学。CoRR **abs/2207.01754**（2022）。https://doi.org/10.48550/arXiv.2207.01754，https://doi.org/10.48550/arXiv.2207.01754[4] Bennett,C.H., Brassard,G.：量子密码学：公钥分发与抛硬币。在：IEEE 计算机、系统与信号处理国际会议论文集。第 175 页。印度（1984）[5] Diffie, W.,Hellman, M.E.：密码学的新方向。IEEE信息论汇刊**22**（6），644–654（1976）。https://doi.org/10.1109/TIT.1976.1055638[6] Dodis, Y., Ostrovsky,R., Reyzin, L., Smith,A.D.：模糊提取器：如何从生物特征和其他含噪数据中生成强密钥。SIAM计算杂志**38**（1），97–139（2008）。https://doi.org/10.1137/060651380，https://doi.org/10.1137/060651380[7] Dodis,Y., Reyzin, L., Smith, A.D.：模糊提取器：如何从生物特征和其他含噪数据中生成强密钥。在：Cachin, C., Camenisch, J.（编）密码学进展——EUROCRYPT 2004，密码技术理论与应用国际会议，瑞士因特拉肯，2004 年 5 月 2—6 日，论文集。计算机科学讲义，第3027 卷，第 523—540 页。Springer（2004）。https://doi.org/10.1007/978-3-540-24676-3_31，https://doi.org/10.1007/978-3-540-24676-3_31

[8] Ekert, A.K.：基于贝尔定理的量子密码学。Physical review letters **67**(6)，661 (1991)[9] Goldreich, O.：《密码学基础——第2卷：基本应用》。剑桥大学出版社 (2004)。https://doi.org/10.1017/CBO9780511721656[10] Goldreich, O., Goldwasser, S., Micali, S.：如何构造随机函数。Journal of the ACM (JACM)**33**(4)，792–807 (1986)[11] Hhan, M.,Morimae,T.,Yamakawa,T.：从检测叠加态的困难性到密码学：量子公钥加密与承诺。IACR Cryptol. ePrint Arch. p. 1375 (2022)，https://eprint.iacr.org/2022/1375[12] Impagliazzo,R.：平均情形复杂度的个人观点。载于：复杂性理论结构论文集。第十届 IEEE 年会。第 134–147 页。IEEE (1995)[13]Impagliazzo,R., Rudich, S.：关于单向置换可证明推论的界限。载于：Johnson,D.S.（编）第21届ACM计算理论年会论文集，1989年5月14–17日，美国华盛顿州西雅图。第 44–61页。ACM (1989)。https://doi.org/10.1145/73007.73012, https://doi.org/10.1145/73007.73012[14] Jouguet,P., Kunz-Jacques, S., Leverrier,A., Grangier, P.,Diamanti, E.：长距离连续变量量子密钥分发的实验演示。Nature Photonics**7**(5)，378–381(2013)[15] Kitagawa, F., Morimae,T.,Nishimaki,R.,Yamakawa, T.：利用单向函数实现具有防篡改公钥的量子公钥加密。CoRR **abs/2304.01800**(2023)。https://doi.org/10.48550/arXiv.2304.01800, https://doi.org/10.48550/arXiv.2304.01800[16] Korzh, B., Lim, C.C.W., Houlmann, R., Gisin, N., Li, M.J.,Nolan, D., Sanguinetti, B.,Thew, R.,Zbinden, H.：在307 km光纤上实现可证明安全且实用的量子密钥分发。Nature Photonics**9**(3)，163–168(2015)[17] Lo, H.K., Chau, H.F.：任意长距离量子密钥分发的无条件安全性。Science **283**(5410)，2050–2056 (1999)[18] Mayers, D.：量子密码学中的无条件安全性。Journal of the ACM (JACM)**48**(3)，351–406(2001)[19]Mayers, D., Yao, A.C.：不完美设备下的量子密码学。载于：第39届计算机科学基础年会，FOCS'98，1998年11月8–11日，美国加利福尼亚州帕洛阿尔托。第 503–509 页。IEEE Computer Society (1998)。https://doi.org/10.1109/SFCS.1998.743501[20] Müller-Quade, J., Unruh, D.：长期安全性与普适可组合性。J. Cryptol.**23**(4)，594–671 (2010)。https://doi.org/10.1007/s00145-010-9068-8 [21] Nielsen, M.A.,Chuang, I.L.：《量子计算与量子信息》（10周年纪念版）。剑桥大学出版社 (2016)

[22] Renner, R.：量子密钥分发的安全性。《国际量子信息杂志》6(01)，1–127（2008）[23] Shor, P.W., Preskill, J.：BB84 量子密钥分发协议安全性的简单证明。《物理评论快报》85(2)，441（2000）[24] Tomamichel, M., Leverrier, A.：量子密钥分发的一份基本自洽且完整的安全性证明。《Quantum》1，14（2017）[25] Yin, J., Cao, Y., Li, Y.H., Liao, S.K., Zhang, L., Ren, J.G., Cai, W.Q., Liu, W.Y., Li, B., Dai, H. 等：基于卫星的纠缠分发，距离达 1200 公里。《科学》356(6343)，1140–1144（2017）

无条件安全量子公钥加密不可能

下面我们将说明一个简单的论证，证明即使对手只能访问公钥的一个副本，不存在无条件安全的量子公钥加密。更具体地说，我们展示一个对手：只要允许它在协议执行过程中也不受计算能力限制，就能攻破任意量子公钥加密的安全性。以下证明由 Takashi Yamakawa 提出，论证应归功于他。

定理 A.1(U nconditional Security). 不存在无条件安全的量子公钥加密 .

证明。 我们描述一个通用攻击者，它运行无限长时间，并以确定的方式赢得定义 3.2 中的实验。攻击者按以下步骤进行。

- 输入一个状态 ρ 和一个比特串公钥 pk 后，进入以下循环：

  – 均匀采样一个秘密密钥 $\mathsf{sk}^* \leftarrow \mathsf{SKGen}(1^\lambda)$。– 运行 $(\rho^*, \mathsf{pk}^*) \leftarrow \mathsf{PKGen}(\mathsf{sk})$。– 如果 $\mathsf{pk}^* = \mathsf{pk}$，则退出循环并返回 $(\rho^*, \mathsf{pk}^*, \mathsf{sk}^*)$。– 否则，重新开始。

- 令$(\rho^*$,公钥*,sk$^*)$ 为上述循环输出的元组。将 ρ^* 返回给挑战者。
- 收到密文后，使用 sk^* 解密消息。

为了证明该攻击总能成功，只需注意到，内部循环最终会返回一个元组 $(\rho^*$,公钥*,sk$^*)$，使得

$$\mathsf{pk}^* = \mathsf{pk} \quad \text{and} \quad (\rho^*, \underbrace{\mathsf{pk}^*}_{=\mathsf{pk}}) = \mathsf{PKGen}(\mathsf{sk}^*)$$

具体而言，这意味着挑战者运行的算法 Enc 的输入是一个有效的对 $(\rho^*$,公钥$)$。因此，根据量子公钥加密的正确性，密钥 sk^* 必定能恢复出正确的消息。

□