概率加密 & 如何在保密所有部分信息的情况下玩心理扑克

Shafi Goldwasser* 和 Silvio Micali** 加州大学伯克利分校计算机科学系

说明：MinerU将原始pdf文献转为markdown文档，用kimi进行全文翻译。

1. 引言

本文提出了一种具有以下性质的加密方案：

一个知道加密算法并获得密文的 adversary （攻击者/敌手），无法获得关于明文的任何信息。

Diffie 和 Hellman 在 [8] 中提出的任何公钥密码系统的实现都应具备这一性质。

我们的加密方案遵循了 Rivest、Shamir 和 Adleman [13] 以及 Rabin [12] 提出的数论实现公钥密码系统的思想。

安全性基于复杂性理论以及数论中某些问题的不可解性，这些问题包括因数分解、指数查找以及判断数字是否是关于合数模的二次剩余。在此上下文中，不可能性意味着计算上的不可行性，而证明一个问题困难则意味着证明它与上述提及的问题之一是等价的。

RSA 方案和 Rabin 方案的关键思想都是选择一个适当的陷门函数：一个易于计算的函数 f，使得除非知道某些额外信息，否则从 $f(x)$ 不容易计算出 x。要加密消息 m，只需计算 $f(m)$。

我们想指出这种方法的两个基本弱点：

1）f 是陷门函数这一事实并不能排除当 x 具有特殊形式时从 $f(x)$ 计算出 x 的可能性。通常消息并非由随机选择的数字组成，而是具有更多的结构。这种结构信息可能有助于解密。例如，一个通常在通用输入上难以求逆的函数 f，有可能在英语句子的 ASCII 表示上容易求逆。

2）f 是陷门函数这一事实并不能排除从 $f(x)$ 容易计算出关于 x 的某些部分信息（甚至 x 的每一位）的可能性。如果 x 是英语句子的 ASCII 表示，其危险性不言而喻。以确保所有部分信息保密的方式加密消息是密码学中极其重要的目标。如果我们要用加密来玩电话扑克游戏，这种观点的重要性尤为明显。如果一张牌的花色或颜色可能被泄露，整个游戏就可能无效。

尽管没人知道如何破解 RSA 或 Rabin 方案，但这些方案中没有任何一个被证明在不对消息空间做出假设的情况下解码是困难的。Rabin 表明，在他的方案中，如果可能消息的集合具有某种密度性质，那么对 adversary 来说解码是困难的。

我们贡献的新颖之处在于：

1. 陷门函数的概念被概率加密所取代。为了加密每条消息，我们使用一枚公平的硬币。每条消息的编码将依赖于消息本身加上一系列抛硬币的结果。因此，每条消息都有许多可能的编码。然而，消息总是可以被唯一解码！
2. 对消息的合法接收者来说解码容易，但对 adversary 来说可证明是困难的。因此保留了陷门函数的精神。此外，在我们的方案中，无需对消息空间施加任何限制，我们就能证明解码等价于判断合数模下的二次剩余性。
3. adversary 无法获得关于加密消息的任何部分信息。假设消息空间具有相关联的概率分布，并且在此分布下，一个易于计算的谓词 P（例如"消息中所有位的异或为 1"）为真的概率为 p。不失一般性，设 $p \geq 0.5$。那么，无需任何特殊能力，一个 adversary 在已知密文的情况下，总可以猜测明文满足谓词 P，并且正确的概率为 p。

基于判断合数模二次剩余性是困难的这一假设，我们证明，adversary 无法从密文中以 $p + \varepsilon$ 的概率正确猜测明文是否满足谓词 P，其中 ε 是一个不可忽略的正实数。

概率加密对于解决心理扑克问题很有用。Robert Floyd 提出了是否可以玩"公平"的心理扑克游戏的问题。Shamir、Rivest 和 Adleman 在 [14] 中提出了使用交换加密函数的优雅解决方案，但他们无法证明部分信息不会在他们的方案中被泄露。事实上，Lipton 在 [10] 中指出了他们方案实现中的几个问题。

我们提出了一种心理扑克的解决方案，基于因数分解和判断合数模二次剩余性是困难的假设，我们能够证明关于一张应该隐藏的牌，其任何一位信息都无法被发现。我们的解决方案不使用交换加密函数。

2. 公钥密码系统的安全性

本节使用的所有数论符号将在第 3.1 节定义。

2.1 什么是公钥密码系统？

Diffie 和 Hellman 在他们富有独创性的论文 [8] 中引入了公钥密码系统的概念。设 M 是一个有限消息空间，$A, B, \ldots$ 是用户，$m \in M$ 表示一条消息。设 $E_A : M \to M$ 是 A 的加密函数，理想情况下是双射，D_A 是 A 的解密函数，使得对所有 $m \in M$ 都有 $D_A(E_A(m)) = m$。在公钥密码系统中，E_A 被放置在公共文件中，用户 A 保密 D_A。仅知道 E_A 时，D_A 应该难以计算。要向 A 发送消息 m，B 从公共文件中取出 E_A，计算 $E_A(m)$ 并将其发送给 A。A 可以轻松计算 $D_A(E_A(m))$ 以获得 m。

2.2 RSA 方案和 Rabin 方案

与本文最相关且最具启发性的两个公钥密码系统实现是 RSA 方案 [13]（由 Rivest、Shamir 和 Adleman 提出）以及 Rabin [12] 提出的特例。

RSA 方案和 Rabin 方案的关键思想都是选择一个适当的数论陷门函数。在 RSA 方案中，用户 A 选择两个大素数 p_1 和 p_2 的乘积 N，以及一个与 $\varphi(N)$ 互素的数 s，其中 φ 是欧拉函数。A 将 N 和 s 放在公共文件中，并保密 N 的因数分解。令 $Z_N^* = \{x \mid 1 \leq x \leq N-1 \text{ 且 } x \text{ 和 } N \text{ 互素}\}$。对于每条消息 $m \in Z_N^*$，$E_A(m) = m^s \mod N$。显然，能够计算模 N 的 s

次根意味着能够解码。知道 N 的因数分解的 A 可以轻松计算模 N 的 s 次根。当不知道 N 的因数分解时，尚不知道计算模 N 的 s 次根的有效方法。

关于 RSA 方案，Rabin 指出，就我们所知，求函数 $\boldsymbol{x}^s \mod N$ 的逆可能是一个一般性的难题，但对大部分 $\boldsymbol{x}$ 来说却很容易。

他建议通过选择 $s = 2$ 来修改 RSA 方案。因此，对所有用户 A，$E_A(x) = x^2 \mod N$。注意 E_A 是一个 4 对 1 的函数，因为我们的 N 是两个素数的乘积。事实上，模 N 的每个二次剩余 q（即存在某个 $x \in Z_N^*$ 使得 $q \equiv x^2 \mod N$）在模 N 下有四个平方根：
$\pm x \mod N$ 和 $\pm y \mod N$。知道 N 的因数分解的 A 在收到加密消息 $m^2 \mod N$ 后，可以计算其四个平方根并获得消息 m。解码中的歧义可以通过例如额外发送 m 的前 20 位来消除。这样的额外信息不能有效帮助解码：我们总可以猜测 m 的前 20 位。

以下定理展示了 Rabin 函数 $x^2 \mod N$ 的求逆难度。

定理（Rabin）：如果对于模 N 的二次剩余 q 中的 1%，能够找到 $\boldsymbol{q}$ 的一个平方根，那么就可以在随机多项式时间内分解 N。

该定理源于以下我们不予证明的引理。

引理 1：给定满足 $\boldsymbol{x}^2 \equiv \boldsymbol{y}^2 \mod N$ 且 $\boldsymbol{x} \neq \pm \boldsymbol{y} \mod N$ 的 $\boldsymbol{x}, \boldsymbol{y} \in Z_N^*$，存在一个多项式时间算法来分解 N。（事实上，N 和 $\boldsymbol{x} \pm \boldsymbol{y}$ 的最大公约数是 N 的一个因子）。

Rabin 定理的非正式证明：假设我们有一个魔法盒子 B，给定模 N 的二次剩余 q，对于 1% 的 q 能输出 q 模 N 的一个平方根。那么我们可以通过迭代以下步骤来分解 N：

在 Z_N^* 中随机选取 i 并计算 $\mathfrak{q} = i^2 \mod N$。将 $\mathfrak{q}$ 喂给魔法盒子 B。如果 B 输出一个不同于 i 或 $-i \mod N$ 的平方根，则（根据上述引理）分解 N。

期望的迭代次数很低，因为每一步我们都有 0.5% 的机会分解 N。

2.3 对基于陷门函数的密码系统的异议

用手帕遮住脸当然有助于隐藏个人身份。然而：

1）它不会向我隐藏某个特殊人群的识别：我的母亲、我的姐妹、亲密的朋友。

2）我可以收集很多关于我无法识别的人的信息：他们的身高、头发颜色等等。

本质上，同样的问题可能出现在 RSA 方案和 Rabin 方案中，更一般地说，出现在任何基于陷门函数的公钥密码系统中：

1）f 是陷门函数这一事实并不能排除当 x 具有特殊形式时从 $f(x)$ 计算出 x 的可能性。

2）f 是陷门函数这一事实并不能排除从 $f(x)$ 容易计算出关于 x 的某些部分信息的可能性。

2.4 对异议 1 的讨论

有人可能会认为 Rabin 的公钥密码系统与因数分解一样难以破解，即：任何能从加密消息 $m^2 \mod N$ 中获取消息 m 的人（在时间上的 1%），实际上实现了 Rabin 定理中的魔法盒子，因此可以有效地分解 n。

我们想指出以下事实。

声明：如果 M，消息集合，在 Z_N^* 中是"稀疏"的，那么解码 1% 的所有消息的能力不会产生用于分解的随机多项式时间算法。

"稀疏"的意思是，对于一个随机选择的 $\boldsymbol{x} \in Z_N^*$，$\mathbf{x}$ 是消息的概率实际上为 0。

设 $f(x) = x^2 \mod N$。假设我们只能对 $f(M)$ 求逆函数 f，那么我们将有一个魔法盒子 MB，喂给它 $m^2 \mod N$ 时会输出 m，每当 $m \in M$；喂给它 q 时，只要 $q \notin \{m^2 \mod N | m \in M\}$，就输出 nothing，最多对可忽略的 q 部分例外。使用这样的魔法盒子我们可以解码，但不能有效地分解 N。使用这样的 MB，让我们看看上述 Rabin 定理的非正式证明。如果我们选择 $m \in M$ 并将 $m^2 \mod N$ 喂给 MB，那么我们得到 m 并且无法分解。如果我们选择 $i \notin M$ 并将 $i^2 \mod N$ 喂给 MB，那么 $i^2 \mod N$ 的一个不同于 i 的平方根属于 M 的概率实际上为 0，我们得不到答案。

2.5 对异议 2 的讨论

我们希望定义一个公钥密码系统是安全的，如果 adversary 在获得密文后无法获得关于明文的任何部分信息。后一概念需要形式化：

设 P 是定义在消息空间 M 上的任何易于计算的、非常量的布尔谓词。设 $m \in M$。如果给定 m 的加密，adversary 能有效地计算出 $P(m)$ 的值，那么部分信息就可以从 m 的加密中获得。

注意，根据上述定义，没有任何基于陷门函数的公钥密码系统是安全的。事实上，如果 E_A 是陷门函数，那么在明上定义的以下谓词 P 可以容易地从密文计算：$P(x)$ 为真当且仅当 $E_A(x)$ 是偶数。我们可以使用概率加密来避免此类问题。

我们知道某些决策问题可能对特定输入难以解决，但对大多数输入容易解决。鉴于密码学的特殊目的，获取部分信息应该是困难的要求需要加强。

假设消息空间具有相关联的概率分布，并且在此分布下，谓词 P 为真的概率为 p。不失一般性，设 $p \geq 0.5$。

定义：如果 adversary 能够以对密文相关概率大于 $p + \varepsilon$ 的概率正确猜测明文上 P 的值，则该 adversary 在评估谓词 P 时具有 ε 优势。

我们现在能够重新表述前述部分信息定义。

定义：如果不存在 adversary 在评估密文相关的任何易于计算的谓词时具有 ε 优势，则称一个公钥密码系统是 ε 安全的。

基于判断合数模二次剩余性是困难的这一假设，我们为每个不可忽略的、正的实数 ε 引入了一个 ε 安全的公钥密码系统。让我们首先处理在公钥密码系统中安全发送单个比特的问题。这个问题与部分信息的安全性密切相关，由 Brassard 在 [7] 中提出。

2.6 在基于陷门函数的公钥密码系统中安全发送单个比特的尝试

假设用户 B 想向用户 A 发送一条单比特消息，且要求极高的保密性。该比特为 0 或 1 的可能性相等。B 不希望任何 adversary 在猜测他的消息时具有 1% 的优势。B 知道 E_A 难以求逆，并试图利用这一事实。

想法 1：系统中所有用户就整数 i 达成一致。用户 B 随机选择 $r \in M$，除了 r 的第 i 位作为他的消息外，其余位随机选择。B 将 $E_A(r)$ 发送给 A。

A 可以解码并获得所需的比特。但 adversary 能做什么呢？

危险：设 $\mathbf{y} = E_A(\mathbf{x})$，其中 E_A 是单向函数。那么，给定 $\mathbf{y}$，计算 $\mathbf{x}$ 可能困难，但计算 $\mathbf{x}$ 的特定位可能并不困难。

示例：设 $\boldsymbol{p}$ 是一个大素数，使得 $p-1$ 至少有一个大素因子。设 g 是 Z_{p^*} 的生成元。那么 $y \equiv g^x \mod p$ 是一个众所周知的单向函数。但是，尽管从 $g^x \mod p$ 计算 x 困难（指数查找问题），获得 x 的最后一位却很容易。事实上，x 以 0 结尾当且仅当 y 是模 p 的二次剩余。对于素数 p，我们有快速的随机多项式时间算法来测试二次剩余性，参见 [10]。

Donald Johnson 提出了以下想法。

想法 2：B 随机选择 $8 \leq i \leq 100$，并将 x 的第 i 位设置为他想要通信的比特。x 的其余 93 位随机选择，除了 x 的前 7 位指定位置 i 外。B 向 A 发送 $E_A(x)$。

危险：如果给定 $E_A(x)$，我们可以容易地计算 x 的前 7 位和 x 的最后 93 位中的一位，那么我们可以以 $1/93$ 的优势猜测 B 的消息。

总结：单比特可以"嵌入"二进制数 $\mathbf{x}$ 的方式有很多。取 $\mathbf{x}$ 所有数字的"异或"只是另一个例子。然而，给定 $\mathbf{y} = E_A(\mathbf{x})$，能够发现嵌入在 $\mathbf{x}$ 中的某些特定位，与计算 $\mathbf{x}$ 困难这一事实并不矛盾。那么，安全发送单个比特的方法是什么？这个问题的答案将在下一节讨论。

3. 判断二次剩余性在平均情况下是困难的

符号 $(\boldsymbol{x}, N)$ 将表示 $\boldsymbol{x}$ 和 N 的最大公约数。我们使用 $\Pr(X)$ 表示事件 X 的概率。我们令 $Z_N^* = \{\boldsymbol{x} \mid 1 \leq \boldsymbol{x} \leq N-1 \text{ 且 } (\boldsymbol{x}, N) = 1\}$。

3.1 背景和记号

给定 $q \in Z_N^*$，$q \equiv x^2 \mod N$ 是否可解？如果 N 是素数，那么这个问题的答案可以容易地计算。如果解存在，则称 q 是模 N 的二次剩余。否则称 q 是模 N 的二次非剩余。从现在开始，设 p_1 和 p_2 是奇素数且互不相同，$N = p_1 p_2$。那么，$q \equiv x^2 \mod N$ 可解当且仅当 $q \equiv x^2 \mod p_1$ 和 $q \equiv x^2 \mod p_2$ 都可解。在这种情况下，q 被称为模 N 的二次剩余，否则 q 被称为模 N 的二次非剩余。我们将判断元素 $q \in Z_N^*$ 是否为二次剩余的问题称为二次剩余问题。

设 $\boldsymbol{p}$ 为奇素数且 $q \in Z_{p^*}$，则 Jacobi 符号 (q/p) 在 q 是模 $\boldsymbol{p}$ 的二次剩余时等于 1，否则为 -1。Jacobi 符号 (q/N) 定义为 $(q/N) = (q/p_1)(q/p_2)$。尽管 Jacobi 符号 (q/N) 是通过 N 的因数分解定义的，但即使不知道 N 的因数分解，(q/N) 也可以在多项式时间内计算！

从上述定义容易看出，如果 $(q/N) = -1$，那么 q 必须是模 N 的二次非剩余。事实上，q 必须是模 p_1 或模 p_2 的二次非剩余。然而，如果 $(q/N) = +1$，那么 q 要么是模 N 的二次剩余，要么对 N 的两个素因子都是二次非剩余。

让我们统计一下，在 $(q/N) = 1$ 的 q 中，有多少个实际上是二次剩余。

定理：设 $\boldsymbol{p}$ 为奇素数。则 Z_p^* 是一个循环群。

定理：设 g 是 Z_{p^*} 的生成元，则 $g^{\mathbf{s}} \mod p$ 是二次剩余当且仅当 s 是偶数。

推论：Z_p^* 中一半的数字是二次剩余，另一半是二次非剩余。

定理：设 $N = p_1 p_2$，其中 p_1 和 p_2 是不同的奇素数。那么 Z_N^* 中一半的数字的 Jacobi 符号等于 -1，因此是二次非剩余。其余数字的 Jacobi 符号为 1。这些后者中恰好一半是二次剩余。

3.2 数论中的一个困难问题

如果不知道 $\mathbf{N}$ 的因数分解且 $(\mathbf{q}/\mathbf{N}) = 1$，那么没有已知的方法来判断 $\mathbf{q}$ 是否为模 $\mathbf{N}$ 的二次剩余。这个决策问题众所周知在数论中是困难的。它是 Gauss 在其《算术研究》（1801）中讨论的四个主要算法问题之一。对它的多项式解法将意味着数论中其他开放问题的多项式解法，例如判断其因数分解未知的合数 $\boldsymbol{n}$ 是两个还是三个素数的乘积，参见 Adleman [3] 中的开放问题 9 和 15。

最近，Adleman [1] 表明二次剩余的一个推广与因数分解等价。在协议中使用这个推广概念，我们可以将我们密码系统的安全性建立在因数分解上。目前，我们正在等待 Adleman 论文的最终版本。

假设：设 $0 < \varepsilon < 1$。对每个正整数 k，令 $C_{k,\varepsilon}$ 为电路 C 的最小尺寸，这些电路能正确判断 k 位整数 n 中比例为 ε 的数的二次剩余性。那么，对每个 $0 < \varepsilon < 1$ 和每个多项式 Q，存在 $\delta_{\varepsilon,Q}$，使得 $k > \delta_{\varepsilon,Q}$ 意味着 $C_{\varepsilon,k} > Q(k)$。

3.4 一个数论结果

我们想证明，判断 $\mathbf{q}$ 是否为模 $\mathbf{N}$ 的二次剩余，在某些特殊情况下并不困难，但在平均意义上以非常强的意义是困难的。为此，让我们回顾弱大数定律：

如果 $y_1, y_2, \ldots, y_k$ 是 k 个独立的伯努利变量，使得 $y_i = 1$ 的概率为 p，且 $S_k = y_1 + \ldots + y_k$，则对于实数 $\psi, \delta > 0$，$k \geq \frac{1}{4\delta\psi^2}$ 意味着

$$\Pr\left(\left|\frac{S_k}{k} - p\right| > \psi\right) < \delta.$$

注意 $\mathbf{k}$ 在 ψ^{-1} 和 δ^{-1} 中是多项式有界的。

$$\mathrm{Let}\, A_N^* = \{x \mid x \in Z_N^* \mathrm{and}(x/N) = 1\}.$$

定义：对于合数 N，以及对实数 $0 < \varepsilon \leq \frac{1}{2}$，如果我们在多项式 $(|N|)$ 时间内，能对 A_N^* 中至少 $\frac{1}{2} + \varepsilon$ 的元素正确猜测其模 N 的二次剩余性，则称我们能在 A_N^* 中随机选取 q 时以 ε 优势猜测其是否为模 N 的二次剩余。

定理 1：设 $0 < \varepsilon \leq \frac{1}{2}$，$0 < \delta \leq 1$ 为不可忽略数。假设我们能以 ε 优势猜测从 A_N^* 中随机抽取的 q 是否为模 N 的二次剩余。那么我们就可以以概率 $1 - \delta$ 判断任意整数模 N 的二次剩余性，方法是使用多项式（在 $|N|$、ε^{-1} 和 δ^{-1} 中）时间概率算法。

证明：反之，假设我们有一个多项式时间的魔法盒子 MB，它能正确猜测模 N 的 $q \in A_N^*$ 是否为二次剩余，对 A_N^* 中 $\frac{1}{2} + \varepsilon$ 的元素有效。令

$\alpha = \Pr(\mathbf{MB}$ 回答"q 是二次剩余" | q 是模 n 的二次剩余)

$\beta = \Pr(\mathrm{MB}$ 回答 ”q 是二次剩余" | q 是模 N 的二次非剩余，$q \in A_N^*$)。

MB 在 A_N^* 上正确的比例等于 $\frac{1}{2}\alpha + \frac{1}{2}(1 - \beta)$。为了使 MB 具有 ε 优势，必须有 $\alpha - \beta \geq 2\varepsilon$。然而，$\alpha$ 不一定等于 $\varepsilon + \frac{1}{2}$。我们现在将展示如何获得 α 的良好估计。

构造一个从 Z_N^* 中随机选择的 $\mathbf{k}$ 个二次剩余的样本（$\mathbf{k}$ 的值将在后面定义）。这可以通过在 Z_N^* 中随机选取 $s_1, \ldots, s_k$ 并将它们模 $\mathbb{N}$ 平方来轻松完成。

初始化两个计数器 R 和 NR 为 0。

将每个 s_i^2 喂给 MB。每次 MB 回答"二次剩余"时，递增 R 计数器。每次 MB 回答"二次非剩余"时，递增 NR 计数器。

令 $\psi = \frac{2\varepsilon}{4}$。如果选择足够大的 k，$k \geq \frac{1}{\delta\psi^2}$，弱大数定律保证

$$Pr(\left|\alpha - \frac{R}{k}\right| > \psi) < \frac{\delta}{4};$$

即 R/k 是 MB 仅在输入为二次剩余时猜测能力的非常好的近似。

我们现在准备确定 A_N^* 中元素的二次剩余性。

令 q 是我们要测试二次剩余性的 A_N^* 中的元素。随机生成 k 个二次剩余 $x_1, \ldots, x_k$，Z_N^* 中的元素，并计算 $y_i \equiv qx_i \mod N$，其中 $i = 1, \ldots, k$。注意

a) 如果 $\mathbf{q}$ 是二次剩余，则 y_i 是 Z_N 中的随机二次剩余。

b) 如果 $\mathbf{q}$ 是 A_N^* 中的二次非剩余，则 y_i 是 A_N^* 中的随机二次非剩余。

让我们推迟 (a) 和 (b) 的证明，暂时假设它们是正确的。

初始化两个计数器 R^* 和 NR^* 为 0。将样本 $\{y_i\}$ 输入 MB。每次 MB 回答"二次剩余"时递增 R^*，每次 MB 回答"二次非剩余"时递增 NR^*。我们知道，如果 q 是二次剩余，则 $Pr(|\frac{R^*}{k} - \frac{R}{k}| \leq 2\psi) \geq (1 - \frac{\delta}{4})^2$，如果 q 是二次非剩余，则 $Pr(|\frac{R^*}{k} - \frac{R}{k}| \leq 2\psi) < 1 - (1 - \frac{\delta}{4})^2$。因此，如果 $|\frac{R^*}{k} - \frac{R}{k}| \leq 2\psi$，则以大于 $1 - \delta$ 的概率，q 是模 N 的二次剩余，否则，同样以大于 $1 - \delta$ 的概率，q 是二次非剩余。

我们仍需要证明 (a) 和 (b)。我们仅证明 (a)，因为 (b) 的证明类似。只需证明，给定任意二次剩余 q，Z_N^* 中任何其他二次剩余 y 都可以唯一地写成 $y = qx$ 的形式，其中 x 是模 N 的二次剩余。一个众所周知的代数定理是 $Z_N^* = Z_{p_1}^* \times Z_{p_2}^*$。因此设 a 和 b 分别是 $Z_{p_1}^*$ 和 $Z_{p_2}^*$ 的生成元，使得 $(a, p_2) = 1$ 且 $(b, p_1) = 1$。那么 Z_N^* 中的任何元素都可以唯一地写成 $a^i b^j$ 的形式，其中 $1 \leq i \leq p_1 - 1$ 且 $1 \leq j \leq p_2 - 1$。此外，q 是模 N 的二次剩余当且仅当它可以写成 $q = a^{2t} b^{2j}$ 的形式，其中 $1 \leq 2i \leq p_1 - 1$ 且 $1 \leq 2j \leq p_2 - 1$。因此如果 $y = a^{2s} b^{2t}$ 是任意二次剩余且 $x = a^{2(s-i)} b^{2(t-j)}$，则 $y = qx$，部分 (a) 得证。

定理 2：设 $r \in A_N^*$ 是一个公开的模 N 的二次非剩余。设 $0 < \varepsilon \leq \frac{1}{2}$，$0 < \delta \leq 1$ 为不可忽略数。假设我们能以 ε 优势猜测从 A_N^* 中随机抽取的 q 是否为模 N 的二次剩余。那么我们就可以以概率 $1 - \delta$ 判断任意整数模 N 的二次剩余性，方法是使用多项式（在 $|N|, \varepsilon^{-1}$ 和 δ^{-1} 中）时间概率算法。

证明：

首先假设，给定任意二次非剩余 $r \in A_N^*$，某人可以构建一个多项式时间魔法盒子 MB_r，它在判断二次剩余和非剩余方面具有 ε 优势。我们将证明，即使不给出这样的 r，二次剩余性仍然可以被判断。

构造一个由从 $A_N^\bullet$ 中随机选择的 20 个元素组成的集合 T。以概率 $1 - (1/2)^{20}$，T 中的一个元素将是模 N 的二次非剩余。对每个 $\boldsymbol{x} \in T$ 执行以下操作：

如定理 1 中所述选择 $\mathbf{k}$。构造 $MB_{\mathbf{x}}$，并在 $\mathbf{k}$ 个随机二次剩余 $S = \{s_1, \ldots, s_k\}$ 上测试其性能，如我们在定理 1 中所做的那样。同时从 A_N^* 中随机选取 $y_1, \ldots, y_{20}$。同样，以很高的概率，至少有一个 y_i 是二次非剩余。现在构造样本 $H_i = \{y_i s \mid s \in S\}$，并将它们输入 MB_x。

a) 如果 MB_x 在所有 H_i 上的表现与其在 S 上的表现相同，则转到 T 中的下一个元素。如果 T 中的所有元素都已使用，则停止。

b) 如果 $MB_{\boldsymbol{x}}$ 在比如说 H_i 上的表现与在 S 上"显著"不同，则停止。

如果情况 (b) 发生，则 y_i 是一个二次非剩余，最重要的是，我们获得了一个魔法盒子 MB_x，它可以在随机多项式时间内区分二次剩余和非剩余。

情况 (b) 发生在存在 $\boldsymbol{x} \in T$ 是模 N 的二次非剩余，并且至少有一个对应的 y_i 是模 N 的二次非剩余时。因此情况 (b) 以概率 $\left[1 - \frac{1}{2}^{20}\right]^2$ 发生。这与我们判断二次剩余性是困难的假设相矛盾。

在上面的证明中，我们假设给定任何二次非剩余 $r \in A_N^*$，都可以构造一个具有判断二次剩余性 ε 优势的魔法盒子 MB_r，并由此导出矛盾。

假设某人只能对 1% 的二次非剩余 $r \in A_N^*$ 构建具有 ε 优势的 MB_r。那么上述证明中唯一需要改变的就是集合 T 的大小，使得 T 包含一个合适的 r。

4. 如何在公钥密码系统中以可证明安全的方式发送消息

系统中每个用户公布一个大的合数 $\mathbf{N}$，其因数分解 $\mathbf{N} = \boldsymbol{p}_1\boldsymbol{p}_2$ 只有他自己知道，以及 $\boldsymbol{y} \in A_N^*$ 使得 $\boldsymbol{y}$ 是模 $\mathbf{N}$ 的二次非剩余。

设 N 是用户 A 的公钥。假设用户 B 想向 A 发送一个二进制消息 $m = (m_1, \ldots, m_k)$。那么，对每个 m_i，B 随机选取 $\boldsymbol{x}_i \in Z_N^*$ 并设置

$$e_i \leftarrow \begin{cases} x_i^2 \mod N \mathrm{if} m_i \mathrm{is\ a\ 0} \\ y x_i^2 \mod N \mathrm{if} m_i \mathrm{is\ a\ 1} \end{cases}.$$

B 将 $(e_1, \ldots, e_k)$ 发送给 A。

为了解码 $\boldsymbol{m}$，知道 N 的因数分解的用户 A 通过以下方式重建 $\boldsymbol{m}$：

$$m_i \leftarrow \begin{cases} 1 \mathrm{if} e_i \mathrm{is\ a\ quadratic\ residue\ mod\ N} \\ 0 \mathrm{if} e_i \mathrm{a\ is\ quadratic\ nonresidue\ mod\ N} \end{cases}$$

当已知 N 的因数分解时，测试 $\boldsymbol{q} \in A_N^*$ 是否为模 $\mathbf{N}$ 的二次剩余很容易，由以下引理证明。

引理 2：如果已知 N 的因数分解，我们可以在多项式时间内测试是否存在 x 使得 $q \equiv x^2 \mod N$。

证明：q 是模 N 的二次剩余当且仅当 q 是模 p_1 的二次剩余 AND 模 p_2 的二次剩余。对于素数 p，q 是模 p 的二次剩余当且仅当 $q^{(p-1)/2} = 1 \mod p$。因此，要测试 q 是否为模 N 的二次剩余，我们只需计算 $q^{(p_1-1)/2} \mod p_1$ 和 $q^{(p_2-1)/2} \mod p_2$。

我们现在处理新提出的公钥密码系统的安全性问题。令 $E(\boldsymbol{x})$ 表示我们的新加密函数，令 M 是所有可能消息的集合。

公钥密码系统中安全性的定义非常困难。它取决于对 adversary 可能行为的模型的假设。目前，我们假设 adversary 可能拦截 $E(m)$ 并试图提取关于 m 的信息。他只能使用计算机、密文和对消息空间 M 的先验知识。对 M 不做任何限制。

注意，在我们的方案中，与 RSA 不同，adversary 在获得 $E(m)$ 后可能很幸运地正确猜测 m，但仍无法证明其猜测的正确性。然而，理解消息的可能性，而无法证明它是什么，对公钥密码系统的安全性仍然是危险的。

我们证明，给定 $m \in M$ 的 $E(m)$，如果 adversary 能比随机猜测 m 做得更好，那么判断任意整数模 N 的二次剩余性就很容易。

回顾 $A_N^* = \{\boldsymbol{x} \in Z_N^* \mid (\boldsymbol{x}/N) = 1\}$

定义：设 $\boldsymbol{x} \in A_N^*$。$\boldsymbol{x}$ 的签名 $\sigma_N(\boldsymbol{x})$ 定义为

$$\sigma_N(\boldsymbol{x}) \leftarrow \begin{cases} 1 \mathrm{if} \boldsymbol{x} \mathrm{is\ a\ quadratic\ residue\ mod\ N} \\ 0 \mathrm{if} \boldsymbol{x} \mathrm{a\ is\ quadratic\ nonresidue\ mod\ N} \end{cases}$$

令 S_N^n 为所有从 A_N^* 中选取的 n 个元素组成的序列的集合。

定义：设 $s = (x_1, \ldots, x_n) \in S_N^n$。$s$ 的 n-签名 $\Sigma_N(s)$ 定义为字符串 $\Sigma_N(s) = \sigma_N(x_1)\sigma_N(x_2)\cdots\sigma_N(x_n)$。

定义：决策函数是函数 $d : S_N^n \to \{0, 1\}$。

设 $\boldsymbol{a} = (a_1, \ldots, a_n)$ 和 $b = (b_1, \ldots, b_n)$ 为 n-签名。

定义：$\boldsymbol{a}$ 和 $\boldsymbol{b}$ 之间的距离定义为 $\boldsymbol{a}$ 和 $\boldsymbol{b}$ 不同的位置数。如果它们之间的距离为 1，则称 $\boldsymbol{a}$ 和 $\boldsymbol{b}$ 相邻。

对于任何决策函数 $\boldsymbol{d}$ 和 $\boldsymbol{n}$-签名 l，令 $P_{\boldsymbol{d}}(l) : \{0,1\}^n \to [0,1]$ 定义为

$$P_{\boldsymbol{d}}(l) = \Pr(\boldsymbol{d}(\boldsymbol{x}) = 1 \mid \Sigma_N(\boldsymbol{x}) = l \mathrm{f\,o\,r} \boldsymbol{x} \in S_N^n)$$

定理 3：设 $0 < \varepsilon \leq \frac{1}{2}$ 和 $0 < \delta \leq 1$ 为不可忽略数。如果存在一个易于计算的决策函数 d，并且找到了两个 n-签名 u 和 v，使得 $|P_d(u) - P_d(v)| > \varepsilon$，那么我们可以通过多项式（在 $|N|$、ε^{-1} 和 δ^{-1} 中）时间概率算法以概率 $1-\delta$ 判断任意整数模 N 的二次剩余性。

证明：假设存在一个决策函数 $\boldsymbol{d}$ 和两个 n-签名 $\boldsymbol{u}$ 和 $\boldsymbol{v}$，使得 $|P_{\boldsymbol{d}}(\boldsymbol{u}) - P_{\boldsymbol{d}}(\boldsymbol{v})| > \varepsilon$。令 $\boldsymbol{\Delta}$ 为 $\boldsymbol{u}$ 和 $\boldsymbol{v}$ 之间的距离。令 $\boldsymbol{a}_0, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{\Delta}$ 是一个 n-签名序列，使得 $\boldsymbol{a}_0 = \boldsymbol{u}$，$\boldsymbol{a}_{\Delta} = \boldsymbol{v}$，且 $\boldsymbol{a}_i$ 与 $\boldsymbol{a}_{i+1}$ 相邻，其中 $0 \leq i < m$。由于 $|P_{\boldsymbol{d}}(\boldsymbol{u}) - P_{\boldsymbol{d}}(\boldsymbol{v})| > \varepsilon$，必然存在 $i, 0 \leq i \leq \Delta - 1$，使得 $|P_{\boldsymbol{d}}(a_i) - P_{\boldsymbol{d}}(a_{i+1})| \geq \varepsilon / n$。为方便起见，令 $s = a_i$ 且 $t = a_{i+1}$。

让我们选择 $\psi = \frac{\varepsilon}{4n}$。同时，令 $k \geq \frac{1}{\delta \psi^2}$。从 $\Omega_s = \{x \in S_N^n \mid \Sigma_N(x) = s\}$ 中随机选择 k 个元素 $x_1, \ldots, x_k$，并从 $\Omega_t = \{x \in S_N^n \mid \Sigma_N(x) = t\}$ 中随机选择 k 个元素 $y_1, \ldots, y_k$。然后，根据弱大数定律，

$$Pr(|P_d(s) - \frac{d(x_1) + \cdots + d(x_k)}{k}| > \psi) < \frac{\delta}{4}$$

和

$$Pr\left(\left|P_d(t) - \frac{d\left(y_1\right) + \cdots + d\left(y_k\right)}{k}\right| > \psi\right) < \frac{\delta}{4}.$$

设

$$\alpha = \frac{d(x_1) + \cdots + d(x_k)}{k}, \beta = \frac{d(y_1) + \cdots + d(y_k)}{k}$$

由于 $s = (s_1, \ldots, s_n)$ 和 $t = (t_1, \ldots, t_n)$ 相邻，它们恰好在一个位置上不同。称此位置为 r。不失一般性，假设 $s_r = 1$ 且 $t_r = 0$。

我们现在将证明，我们以大于 $1-\delta$ 的概率判断二次剩余性模 N。设 $\boldsymbol{q}$ 是我们要测试剩余性的 A_N^* 中的元素。选择 $\boldsymbol{k}$ 个在 A_N^* 中的随机二次剩余：$x_1^2, \ldots, x_k^2$，并计算
$\mathbf{y}_j = q \cdot x_j^2 \mod N$，其中 $1 \leq j \leq k$。根据定理 1，如果

$\boldsymbol{q}$ 是二次剩余，则 $\mathbf{y}_j$ 都是二次剩余，否则都是 A_N^* 中的二次非剩余。

在定理 2 中我们表明，知道 A_N^* 中的非剩余无助于判断二次剩余性。因此我们可以假设这样的非剩余 h 是已知的。这使我们能够从 A_N^* 中随机选取二次非剩余（通过计算 hx^2）。

我们现在准备判断 $\mathbf{q}$ 是否为二次剩余。

(* 构造一个 $\boldsymbol{k}$ 个元素 $(y_{1,1}, \ldots, y_{1,n}), \ldots, (y_{k,1}, \ldots, y_{k,n}) \in S_N^n$ 的随机样本

使得对所有

$1 \leq i \leq n, i \neq r, 1 \leq j \leq k, \sigma_N(y_{j,i}) = s_i$ 且

对所有 $1 \leq j \leq k$，$y_{j,r} = y_j$ 。

对 $i = 1, \ldots, r-1, r+1, \ldots n$ 执行 begin

对 $j = 1, \ldots, k$ 执行
从 A_N^* 中随机抽取 $\boldsymbol{x}$。
如果 $s_i = 1$ 则 $y_{j,i} := x^2 \mod N$。
否则如果 $s_i = 0$ 则 $y_{j,i} := hx^2 \mod N$ 。

end.

(* 评估决策函数 $\boldsymbol{d}$ 在样本每个成员上的值 *)

对 $j = 1, \ldots, k$ 执行

$$X_j = d\left(y_{j,1}, \ldots, y_{j,r-1}, y_j, y_{j,r+1}, \ldots, y_{j,n}\right)$$

注意整个样本 $\{y_{j,1}, \ldots, y_{j,r-1}, \mathbf{y}_j, y_{j,r+1}, \ldots, y_{j,n} | 1 \leq j \leq k\}$ 要么是 Ω_s 的子集，要么是 Ω_t 的子集。因此以大于 $1 - \delta$ 的概率，以下两个互斥事件之一将发生：

(1) $\left| \frac{(X_1 + \ldots + X_k)}{k} - \alpha \right| < \frac{\varepsilon}{2n}$

或

(2) $\left| \frac{(X_1 + \ldots + X_k)}{k} - \beta \right| < \frac{\varepsilon}{2n}$.

如果情况 (1) 发生，我们以大于 $1 - \delta$ 的概率得出结论，q 是二次剩余。否则，我们再次以大于 $1 - \delta$ 的概率得出结论，q 是二次非剩余。

决策函数的概念立即推广为判别函数。这是可以取多于 2 个值的决策函数。对任何非空集合 Ω，令 $D : S_N^n \to \Omega$。设 $\boldsymbol{a} \in \Omega$，则 $P_{D,\boldsymbol{a}}(l) = Pr(D(\boldsymbol{x}) = \boldsymbol{a} \mid \Sigma_N(\boldsymbol{x}) = l$ 对于 $\boldsymbol{x} \in S_N^n$ 成立。以下定理是定理 3 的简单扩展，我们将不予证明地陈述它。

定理 4：设 $0 < \varepsilon \leq \frac{1}{2}$ 和 $0 < \delta \leq 1$ 为不可忽略数。如果存在一个易于计算的判别函数 $D : S_N^n \to A$，并且找到了两个 n-签名 u 和 v，使得 $|P_{D,\boldsymbol{a}}(u) - P_{D,\boldsymbol{a}}(v)| > \varepsilon$，那么我们可以通过多项式（在 $|N|$、ε^{-1} 和 δ^{-1} 中）时间概率算法以概率 $1 - \delta$ 判断任意整数模 N 的二次剩余性。

让我们引入更多记号。设 $M^n = \{m_1, m_2, \ldots\}$ 是长度为 n 的消息集合，其中 n 被 $|N|$ 的多项式函数所限制。令 $k = |M^n|$。设 M_i 是使用本节开头描述的方案对消息 $m_i \in M^n$ 的所有可能编码的集合。显然，$M_i \subset S_N^n$ 且对所有 i 和 j，$|M_i| = |M_j|$。令 $\chi = |M_i|$。

4.1 部分信息的安全性

在本文的当前版本中，我们假设 M^n 中的所有消息都是等可能的。设 P 是一个易于计算的谓词，定义在 M^n 上。设 p 是随机 $\boldsymbol{x} \in M^n$ 上 $P(\boldsymbol{x})$ 为真的概率。由于 M^n 是均匀分布的，且 $|M^n| = k$，P 必须在 M^n 中的 pk 条消息上计算为 1。

令 MB 是一个魔法盒子，接收作为输入的密文 $E(m) \in S_N^n$，其中 $m \in M^n$，并输出 0 或 1，作为对 $P(m)$ 值的猜测。设 0_j 是 MB 在 m_j 的编码上猜测为 0 的数量，1_j 是猜测为 1 的数量。显然，$0_j + 1_j = \chi$。令

$$C_j = \begin{cases} 1_j & \text{if } P(m_j) = 1 \\ 0_j & \text{if } P(m_j) = 0. \end{cases}$$

C_j 表示 MB 正确猜测 $P(m_j)$ 值的 m_j 的编码数量。

定理 5：设 $0 < \delta < 1$ 为不可忽略实数。如果 $\frac{1}{k\chi}\sum_{j=1}^{k} C_j \geq p + \varepsilon$，对某个不可忽略实数 $\varepsilon > 0$ 成立，那么我们可以通过多项式（在 $|N|$、ε^{-1} 和 δ^{-1} 中）时间概率算法以概率 $1-\delta$ 判断任意整数模 N 的二次剩余性。

证明：让我们将 M^n 划分为 $10/\varepsilon$ 个桶，$M^n = \bigcup_{i=1}^{10/\varepsilon} B_i$，使得 $m \in B_i$ 当且仅当

(i-1) $\frac{\varepsilon}{10} \leq \frac{1_m}{\chi} < i\frac{\varepsilon}{10}$。我们证明存在两个不相邻的桶，每个都包含不可忽略比例的消息。更正式地，我们证明存在 g, h，其中 $1 < h+1 < g \leq 10/\varepsilon$，使得 $|B_g|, |B_h| > \frac{1}{(10\varepsilon^{-1})^2}k$。说 B_i 是大的，如果

$|B_i| > \frac{1}{(10\varepsilon^{-1})^2}k$，否则是小的。那么我们要证明存在两个不相邻的大桶。假设矛盾地不成立。那么以下情况之一必然适用：

1) 没有大桶。

2) 只有一个大桶：B_i

3) 恰好有两个相邻的大桶：B_i 和 B_{i-1}

注意情况 1 永远不可能是真的；否则 $k = \sum_{i=1}^{10\varepsilon^{-1}} |B_i| \leq \frac{k}{10\varepsilon^{-1}} < k$。在情况 2 中，当 $i = \frac{\varepsilon}{10}$ 时，$\sum_{m_j \in B_i} C_j$ 达到最大，且如果所有满足 $P(m_j) = 1$ 的消息 m_j 都属于 $B_{\frac{\varepsilon}{10}}$，即当 MB 对所有谓词为真的消息的所有编码都猜测为 1 时。

因此，$p + \varepsilon \leq \frac{1}{k\chi}\sum_{m_j \in M^n} C_j$

$$= \frac{1}{k\chi}\left(\sum_{m_j \in B_i} C_j + \sum_{m_j \in B_k, k \neq i} C_j\right) \leq p + \frac{\varepsilon}{10} < p + \varepsilon$$

在情况 3 中，当 $i = \frac{\varepsilon}{10}$ 时，$\sum_{m_j \in B_i} C_j + \sum_{m_j \in B_{i-1}} C_j$ 达到最大，且所有谓词为真的消息属于 $B_{\frac{\varepsilon}{10}}$，所有谓词为假的消息属于 $B_{\frac{\varepsilon}{10}-1}$。

因此，$p + \varepsilon \leq \frac{1}{k\chi}\sum_{m_j \in M^n} C_j =$

$$\begin{aligned}
&\tfrac{1}{k\chi}\left\{\left(\textstyle\sum_{m_j \in B_i} C_j + \sum_{m_j \in B_{i-1}} C_j\right) + \sum_{m_j \in B_k, k \neq i, i+1} C_j\right\} \\
&\leq \tfrac{1}{k\chi}\left\{\left[pk\chi + (1-p)2\varepsilon 10^{-1}k\chi\right] + k\chi\varepsilon 10^{-1}\right\} \\
&\leq \tfrac{1}{k\chi}\left(pk\chi + 3\varepsilon 10^{-1}k\chi\right) < p + \tfrac{\varepsilon}{2}
\end{aligned}$$

在所有三种情况下我们都得到矛盾。

因此存在两个不相邻的桶 B_g 和 B_h，每个都包含至少 $\frac{\varepsilon}{10}k$ 条消息。通过抽样，我们可以在很小的期望时间内找到两条消息 u 和 v，分别位于 B_g 和 B_h 中。我们将 MB 视为决策函数 $D : S_N^n \to [0,1]$。那么，$P_D(u) - P_D(v) > \frac{\varepsilon}{10}$，且定理 3 适用。□

接下来，我们将看到 adversary 无法解码超过所有消息编码的可忽略部分。

4.2 adversary 无法解码

令 MB 是一个魔法盒子，接收 $m \in M^n$ 的 $E(m)$ 作为输入，并输出 m_i。MB 的输出可解释为 MB 对 m 是什么的猜测。

令 $r_{j,i}$ 表示 MB 回答 m_i 的消息 m_j 的编码数量。显然，$r_{i,j}$ 将表示在所有可能的 m_i 编码上 MB 正确回答的次数。

定理 6：设 $0 < \delta < 1$ 为不可忽略实数。如果 $\sum_{i=1}^{k} \frac{r_{i,i}}{k\chi} > \varepsilon + \frac{1}{k}$ 对某个不可忽略 $\varepsilon < 1 - \frac{1}{k}$ 成立，那么我们可以以概率 $1 - \delta$ 判断二次剩余性模 N，方法是使用多项式（在 $|N|$、ε^{-1} 和 δ^{-1} 中）时间概率算法。

证明：说消息 m_i 被良好解码，如果 $r_{i,i} > \left(\frac{1}{2}\epsilon\right)\chi$。令 W 为良好解码消息的集合，$W' = M^n - W$。

声明 1：至少存在 $\frac{\varepsilon k}{2}$ 条良好解码消息。

证明：

$$\begin{aligned}&\varepsilon k\chi < \varepsilon k + \chi < \sum_{i=1}^{k} r_{i,i} = \sum_{i\in W} r_{i,i} + \sum_{i\in W'} r_{i,i} \\ &\leq \chi|W| + (k - |W|)\tfrac{1}{2}\epsilon\chi = \chi\left[\left(1 - \tfrac{1}{2}\epsilon\right)|W| + k\tfrac{1}{2}\epsilon\right]\end{aligned}$$

因此，$\frac{|W|}{k} > \frac{\varepsilon/2}{(1-\varepsilon/2)} > \frac{\varepsilon}{2}$。（声明 1）

显然，如果我们从 M^n 中随机选择消息，我们期望在 $2\varepsilon^{-1}$ 次试验中找到一条良好解码消息。令 $\Omega \subset W$ 使得 $|\Omega| > 2\varepsilon^{-1}$ 且 $\rho > \frac{1}{2\varepsilon^{-1}(2\varepsilon^{-1}+1)}$。

声明 2：存在两条良好解码消息 $m_i, m_j \in \Omega$，使得 $\left|\frac{r_{i,i}}{\chi} - \frac{r_{j,i}}{\chi}\right| > \rho$。

证明：固定 $m_j \in \Omega$。有多少条消息 $m_i \in \Omega$ 可以满足 $\left|\frac{r_{i,i}}{\chi} - \frac{r_{j,i}}{\chi}\right| \leq \rho$？至多有 $\frac{1}{\left(\frac{1}{2}\varepsilon - \rho\right)} < 2\varepsilon^{-1} + 1$ 条这样的消息。因此存在满足该声明的 $m_i \in \Omega$。（声明 2）

让我们将 MB 转换为判别函数 $D : S_N^n \to M^n \cup \{\gamma\}$。如果 $x \in S_N^n$ 且 MB 在输入 x 时输出 m_j，则设 $D(x) = m_j$。如果 y 不是任何消息的编码，则以下三种情况之一必然发生：

1) MB 输出 m_i，其中 $1 \leq i \leq t$。设 $D(y) = m_i$。

2) MB 输出 m_i，其中 $i < 1$ 或 $i > t$。设 $D(y) = \gamma$。

3) MB 在一定时间限制内没有回答。设 $D(y) = \gamma$。

现在，注意在上面证明的声明 1 和 2 中，我们表明可以快速找到两条良好解码消息 m_i 和 m_j，使得 $|P_{D,m_i}(m_i) - P_{D,m_i}(m_j)| > \rho$。因此定理 4 的假设成立，判断二次剩余性模 N 在 $|N|$、ε^{-1} 和 δ^{-1} 中是多项式的。

定理 6 表明，对加密消息求函数 E 的逆与判断二次剩余性一样困难，且与 M^n 的稀疏性无关。

5. 心理扑克

心理扑克的玩法与普通扑克相同，只是没有纸牌和牌堆。游戏通过电话线或计算机网络进行。由于我们无法通过电话线发送实体牌，发牌和打牌必须通过玩家之间交换消息来模拟。玩家彼此之间的信任程度不超过普通玩家。电话上的公平游戏应确保：

1) 任何玩家都无法获得关于对手手牌或牌堆中牌的任何部分信息。

2) 发给玩家的牌没有重叠，

3) 所有可能的手牌对两位玩家都等概率。

4) 游戏结束时，每位玩家可以验证游戏是按照规则进行的，没有发生作弊。

注意，在心理扑克的公平游戏中，仅仅表明很难获得一张牌的确切值是不够的。我们还必须表明 adversary 无法获得关于该表的任何部分信息。

我们提出了一种使用加密进行两人心理扑克游戏的协议。我们证明，在判断二次剩余性是困难的假设下，没有任何方式让玩家能够获得任何不在其手牌中的单张加密牌或不在其手牌中的任何加密牌子集的信息。

我们的心理扑克实现使用了两个主要工具。一个是通过电话抛硬币的方法 [5]，另一个是本文提出的在公钥密码系统中安全发送单个比特的方法。

Manuel Blum 在 [6] 中独立获得了该心理扑克问题的另一种解决方案。他的解决方案基于因数分解是困难的且完全安全的单向函数存在的假设。

5.1 抛硬币的背景

在井中抛硬币——A 和 B 彼此站得很远。B 站在一口深井旁边。A 从远处将一枚硬币扔进井中。现在 B 知道抛掷的结果（通过往井里看），但无法改变它，而 A 无法知道结果。后来当 B 想向 A 证明他赢了（或输了）时，他让 A 走近并往井里看。

本质上，如果我们能通过交换消息在电话上模拟井中的抛掷，A 可以向 B 发送一个随机比特，其中 A 不知道他发送的是什么，但 B 可以在必要时向 A 证明该比特是什么。这特别适用于密码学游戏。

Blum 和 Micali 在 [5] 中引入了井中抛硬币的概念，其中基于指数查找是困难的假设，他们展示了如何在电话线上抛硬币。Blum 在 [4] 中找到了另一种基于因数分解困难假设的方法。我们概述第三种方法，基于区分合数模的二次剩余和非剩余的困难性。

A 和 B 想抛硬币。A 随机生成两个大的奇素数 P 和 Q，并设 $N = P^*Q$。A 公布 N 和 $y \in A_N^*$，使得 y 是模 N 的二次非剩余。A 从 A_N^* 中随机选择一个数 q，并询问不知道 N 的因数分解的 B，q 是否为模 N 的二次剩余。B 告诉 A 他的猜测。A 现在知道 B 是赢了（还是输了），并可以在以后通过公开 N 的因数分解向 B 证明他确实赢了（或输了）。

为了避免增加我们已经有的假设之外的假设，我们建议在心理扑克协议中使用后两种抛硬币方法之一。

下一节将列出一些将在协议证明中使用的结果。

5.2 有用的结果

设 p_1, p_2 为奇素数且 $N = p_1 p_2$。

引理 3：如果已知 N 的因数分解，我们可以以随机多项式时间找到 $q \in Z_N^*$，使得 $(q/N) = 1$ 且 q 是二次非剩余。

证明：选取 $\boldsymbol{a} \in Z_{p_1}$ 使得 $(\boldsymbol{a}/p_1) = -1$。这可以在 2 次期望试验内完成。类似地，选取 $\boldsymbol{b} \in Z_{p_2}$ 使得 $(\boldsymbol{b}/p_2) = -1$。使用中国剩余定理计算唯一的 $q \in Z_N^*$，使得 $q \equiv a \pmod{p_1}$ 且 $q \equiv b \pmod{p_2}$。现在，q 是二次非剩余且 $(q/N) = (q/p_1 p_2) =$

$$(q/p_1) \cdot (q/p_2) = (a/p_1) \cdot (b/p_2) = 1.$$

引理 4：设 $N = p_1 p_2$ 使得 $p_1 \equiv p_2 \equiv 3 \mod 4$。对所有 $x, y \in Z_N^*$，如果 $x^2 \equiv y^2 \mod N$ 且 $x \neq \pm y \mod N$，则 $(x/N) = -(y/N)$。

证明：令

$$c \leftarrow \begin{cases} 1(\mathrm{m\ o\ d} p_1) \\ 0(\mathrm{m\ o\ d} p_2) \\ 1(\mathrm{m\ o\ d} p_2) \\ 0(\mathrm{m\ o\ d} p_1) \end{cases}$$

我们可以通过中国剩余定理找到 c 和 d。令 $a^2 \equiv x^2 \pmod{p_1}$ 且 $b^2 \equiv x^2 \pmod{p_2}$。则四个平方根（模 N）由 $ac + db, -ac + db, -(ac + db)$ 和 $(ac - db)$ 给出。令 $x = ac + db$，且 $y = -ac + bd$。由于 $N \equiv 1 \mod 4$ 意味着 $(x/N) = (-x/N)$，我们只需证明 $(+x/N) = -(y/N)$。因此，$(x/N) = (ac + bd/N) = (ac + bd/p_1)(ac + bd/p_2)$。
$= (ac/p_1)(bd/p_2).$
$= (-ac + bd/N) = -(-ac + bd/p_1)(-ac + bd/p_2) =$ 由于 $p_1 = 3 \pmod{4}$，
$= (-ac/p_1)(bd/p_2) = -(-1/p_1)(x/N).$
$(-1/p_1) = -1$ 。

根据 de la Vallee Poussin 的定理 [15]，大约一半给定长度的素数同余于 3 mod 4。因此，形如 $N = p_1 p_2$ 且 $p_1 \equiv p_2 \equiv 3 \mod 4$ 的合数约占给定长度的两个奇素数乘积的所有合数的 $1/4$。因此，因数分解和判断此类特殊 N 的二次剩余性仍然是一个困难问题。另一种不使用特殊合数但增加协议中交换消息数量的方法将出现在最终论文中。

5.3 协议

要用二进制表示 52 张牌，每张牌至少需要 6 位。因此首先 A 和 B 就对应 52 张牌的 52 个不同比特模式达成一致。

从现在开始，当我们说 A 向 B 翻转 $\boldsymbol{k}$ 时，我们的意思是 B 从 A 那里随机接收一个数 $\boldsymbol{k}$，而 A 对 $\boldsymbol{k}$ 没有任何信息。$\boldsymbol{k}$ 实际上是通过一系列井中抛硬币逐位发送的。

5.3.1 算法

第 1 步：B 随机选择 52 对大素数：$(p_1, q_1), (p_2, q_2), (p_3, q_3), \ldots, (p_{52}, q_{52})$，使得对 $1 \leq i \leq 52$ 有 $p_i \equiv q_i \equiv 3 \mod 4$，并生成 52 个他知道其因数分解的大合数，即 $N_1 := p_1 \cdot q_1, N_2 := p_2 \cdot q_2, \ldots, N_{52} := p_{52} \cdot q_{52}$。接下来，她用手洗牌，并将 $N_1, \ldots, N_{52}$ 分配给洗好的牌堆，每张第 i 张牌对应一个 N_i。她公布有序的 52 元组 $< N_1, N_{2,\ldots,N_{52}} >$。

第 2 步：A 做同样的事情。让我们用 $(s_1, t_1), (s_2, t_2), (s_3, t_3), \ldots, (s_{52}, t_{52})$ 表示他选择的素数，使得对 $1 \leq i \leq 52$ 有 $s_i \equiv t_i \equiv 3 \mod 4$，他的 52 个合数表示为 $M_1 := s_1 \cdot t_1$，$M_2 := s_2 \cdot t_2, \ldots, M_{52} := s_{52} \cdot t_{52}$。他洗牌并将 $M_1, \ldots, M_{52}$ 分配给洗好的牌堆，每张第 i 张牌对应一个 M_i。他公布有序的 52 元组 $< M_1, M_2, \ldots, M_{52} >$。

第 3 步：B 公布她的整副牌。牌堆按以下方式加密。对每张牌 C_i（对应公钥 N_i），B 公布 $A^*_{N_i}$ 中有序的 6 个数列表 $(q_1, \ldots, q_6)$，使得对 $1 \leq j \leq 6$，当且仅当 C_i 的第 j 位是 1 时，q_j 是二次剩余。

例如，设 B 牌堆中的第一张牌为 010010。则 B 公布 $(q_1, q_2, q_3, q_4, q_5, q_6)$，其中 q_1, q_3, q_4 和 q_6 是模 N_i 的二次非剩余，且 q_2, q_5 是 Jacobi 符号为 1 的模 N_i 的二次剩余。q_i 在 $A^*_{N_i}$ 中具有所需性质的元素中随机选择。这可以通过引理 3 在随机多项式时间内完成。

注意，根据引理 2，如果 A 能分解 N_i，他也能判断 B 作为牌 C_i 编码位对应的数字是否为二次剩余，从而确定牌是什么。如果 A 不能分解 N_i，他无法判断对应牌编码位的数字是否为二次剩余，因此无法确定剩余的牌是什么。

第 4 步：A 以与 B 完全相同的方式公布他的牌堆。

第 5 步 [B 向 A 发一张牌]：假设 A 决定从 B 的牌堆中挑选第 K 张牌。对 B 的加密牌堆中的每张牌重复以下过程。我们对第 i 张牌进行描述，它对应于 N_i。B 向 A 翻转 $x \in Z^*_{N_i}$。A 计算 $x^2 \mod N_i$ 和 (x/N_i)。此时 A 必须遵循以下两个过程之一：P1 如果 $i = K$，否则 P2。

P1：A 向 B 发送 $x^2 \mod N_i$ 和 $-(x/N_i)$。

P2：A 向 B 发送 $x^2 \mod N_i$ 和 (x/N_i)。

B 计算 $x^2 \mod N_i$ 的平方根。令平方根为 $x, n-x, y$ 和 $n-y$。接下来，B 发送她从 A 收到的 Jacobi 符号对应的根：如果她收到来自 A 的 $-(x/N_i)$，则发送 y，否则发送 x。根据引理 4，(x/N_i) 唯一确定 x，且 $-(x/N_i)$ 唯一确定 y。因此如果 A 遵循 P1，他将收到 $x^2 \mod N_i$ 的 4 个平方根，并根据引理 1 可以分解。如果 A 遵循 P2，他不会获得关于 C_i 值的新信息。B 从她那一方不知道 A 选择了哪张牌。之后，B 可以验证她向 A 翻转的内容，从而验证 B 只发现了一张牌的因数分解。

第 6 步：此时 A 知道 N_K 的因数分解。为了重建实际牌 C_K，A 对 C_K 的加密表示 $(q_1, \ldots, q_6)$ 应用引理 2 的多项式时间测试。接下来，A 必须从加密牌堆中删除 C_K。B 可以看到 A 牌堆中哪个加密元素被擦除，但这并不能使她解密它。

第 7 步 [A 向 B 发一张牌]：显然，执行与第 5 步和第 6 步相同的过程，A 和 B 的角色互换。现在 B 将发现 $M_1, \ldots, M_{52}$ 中某一个的因数分解。

第 8 步：如果游戏中需要发更多牌，则执行类似的协议。每当 A 需要一张牌时，他将从 B 的牌堆中挑选一张牌，遵循第 5 步和第 6 步中的过程。同样，每当 B 需要一张牌时，她将从 A 的牌堆中挑选。

第 9 步 [游戏结束后验证]：游戏结束后，A 可以向 B 证明他所声称的她向他翻转的所有内容确实是由她翻转的，以及翻转的顺序。B 也可以做同样的事情。A 公开每个 M_i 的因数分解（对所有 $1 \leq i \leq 52$），B 公开每个 N_i 的因数分解（对所有 $1 \leq i \leq 52$）。他们都可以向对方证明他们在游戏中的任何主张，例如"N 是两个素数的乘积"、"所有牌始终都在牌堆中"、"这些是你向我翻转的二次剩余"或"我赢了"。

5.3.2 正确性证明：

声明 1：所有手牌都是等概率的。

证明：在第 9 步中，A 和 B 验证两个加密牌堆都包含全部 52 张牌。在第 5 步中，A 自己选择他想从 B 的牌堆中获取的加密值，因此他等可能地获得牌堆中的任何牌。B 的情况同理。

声明 2：没有重叠或重复的手牌。

证明：当 A 被发一张牌时，他从加密牌堆中删除该牌。因此 B 永远不会被发同一张牌。A 知道自己从 B 的牌堆中挑选了哪些牌，因此永远不会两次挑选同一张牌。

声明 3：如果玩家 A 知道 N_i 的因数分解，他可以在 $O(|N|^3)$ 时间内重建 C_i。

证明：我们已知 $N_i = p_1 p_2$ 和 $(q_1, \ldots, q_6)$，使得对所有 j，$q_j \in Z_N$ 且 $(q_j / N_i) = 1$。为了重建 C_i，我们必须测试所有 j 对应的 q_j 是否为模 N_i 的二次剩余。这可以通过引理 2 在 $O(|N|^3)$ 步内完成。

仍需证明，在游戏的任何阶段，任何玩家都无法获得关于不在其手牌中的单张加密牌或不在其手牌中的加密牌子集的任何部分信息。完整证明将出现在最终论文中。这里我们仅限于证明，当两位玩家 A 和 B 公布各自的加密牌堆时，A 和 B 都无法以 1% 的优势快速回答关于对手牌堆中单张牌的单比特问题。此类单比特问题的示例包括：牌堆中第 i 张牌是黑色的吗？第 i 张牌的第 1 位和第 3 位相等吗？第 i 张牌各位的模 2 和是 0 还是 1？

定理 7：如果当 B 公布她的加密牌堆时，A 能在多项式时间内以 1% 的优势回答关于 B 牌堆中单张牌的单比特问题 Q，那么他能以概率 1 判断随机合数 N 的二次剩余性，方法是使用多项式$(|N|)$时间概率算法。

证明：假设 A 能回答关于第 i 张牌的单比特问题 Q，该牌对应于合数 N_i。A 以 1% 优势回答 Q 的能力可视为决策函数 $d : S^6 \to 0, 1$（S^6 = 所有来自 $A^*_{N_i}$ 的 6 长序列）。由于 A 在 100 次中正确回答 Q 51 次，我们可以有效地找到两个 6-签名 u 和 v，使得 $|P_d(u) - P_d(v)| \geq 1/100$。因此我们可以应用定理 3 并在多项式时间内判断模 N_i 的二次剩余性。矛盾！

0

5.3.3 实现细节

为了执行协议，我们必须能够做到以下几点：

1. 生成大素数。这可以使用 Gary Miller 的素性测试 [11] 来完成。

2. 当已知 N 的因数分解时，找到 $x^2 \mod N$ 的平方根。使用 Adleman、Manders 和 Miller 的多项式时间算法 [2] 来寻找平方根。

6. 备注和进一步改进

在本文中，我们表明可以加密消息，使得 adversary 在获得密文后无法提取关于明文的信息。这对于心理扑克等协议或加密私人文件已经足够。adversary 可以读取这些文件但无法理解它们。

我们还表明，概率加密可用于公钥环境。然而，在公钥密码系统中，获取密文并试图理解它是对方案安全性最明显的攻击。

adversary 可以作为用户尝试通过通信来破解方案。

他可以尝试通过拦截其他用户的消息并更改它们来破解方案。

最后，他可能尝试利用解码设备来破解方案！

本文提出的公钥密码系统无法抵御这些可能的攻击。然而，通过强制用户遵循特定的消息交换协议，我们构建了一个可证明能抵御上述攻击的公钥密码系统。这些结果将出现在未来的论文中。

致谢

我们最诚挚的感谢献给 Richard Karp，他指导了这项研究，感谢他的贡献、鼓励和极大的耐心，以及 Manuel Blum，他讲授了一门精彩的数论课程，进行了许多富有洞察力的讨论，并找到了减少协议中交换消息数量的方法。

我们特别感谢 Faith Fich、Mike Luby、Jeff Shallit 和 Po Tong。没有他们慷慨的帮助，这篇论文永远不会写成。

Andrew Yao 向我们指出了交换加密函数出现的一些普遍困难。第 2.4 节中的声明是与 Vijay Vazirani 一起获得的。我们感谢他们两人。

我们感谢 Ron Rivest 和 Mike Sipser 的一次非常鼓舞人心的讨论。它极大地改进了这篇论文。

参考文献

[1] Adleman, L., Private Communication, 1981。

[2] Adleman, L., Manders K. and Miller G., On Taking Roots In Finite Fields, Proceedings of the 18th Annual IEEE Symposium on Foundations of Computer Science (FOCS), 1977, 175-177。

[3] Adleman, L., On Distinguishing Prime Numbers from Composite Numbers, Proceedings of the 21st IEEE Symposium on the Foundations of Computer Science (FOCS), Syracuse, N.Y., 1980, 387-408。

[4] Blum, M., Three Applications of The Oblivious Transfer, to appear, 1981。

[5] Blum, M., and Micali, S., How to Flip A Coin Through the Telephone, to appear, 1982。

[6] Blum, M., Mental Poker, to appear, 1982。

[7] Brassard, G., Relativized Cryptography, Proceedings of the 20st IEEE Symposium on the Foundations of Computer Science (FOCS), San Juan, Puerto Rico, 1979, 383-391。

[8] Diffie, W., and M. E. Hellman, New Direction in Cryptography, IEEE Trans. on Inform. Th. IT-22, 6 (1976), 644-654。

[9] Goldwasser S., and Micali S., A Bit by Bit Secure Public Key Cryptosystem, Memorandum NO. UCB/ERL M81/88, University of California, Berkeley, December 1981。

[10] Lipton, R., How to Cheat at Mental Poker, Proceeding of the AMS short course on Cryptology, January 1981。

[11] Miller, G., Riemann's Hypothesis and Tests for Primality, Ph.D. Thesis, U.C. Berkeley, 1975。

[12] Rabin, M., Digitalized Signatures and Public-Key Functions As Intractable As Factorization, MIT/LCS/TR-212, Technical Memo MIT, 1979。

[13] Rivest, R., Shamir, A., Adleman, L., A Method for Obtaining Digital Signatures and Public Key Cryptosystems, Communications of the ACM, February 1978。

[14] Shamir, Rivest, and Adleman, Mental Poker, MIT Technical Report, 1978。

[15] Shanks, D., Solved and Unsolved Problems in Number Theory, Chelsea Publishing Co. (1978)。

校对时补充：

---

[16] Chaum, D. L., Untraceable Electronic Mail, Return Addresses, and Digital Pseudonymus, Communications of the ACM, 24,2 (1981) 84-88。