概率加密*

作者：S Goldwasser，S Micali

译者：李晓峰, 北京联合大学智慧城市学院†

2023 年 4 月 3 日

摘要

介绍了一种新的数据加密概率模型。对于该模型，在适当的复杂度假设下，证明了对于具有多项式有界计算资源的对手来说，从密码文本中提取任何关于明文的信息平均来说是困难的。该证明适用于具有任何概率分布的任何消息空间。给出了该模型的第一个实现。在二次剩余模复合数因式分解是困难问题的假设下，证明了该实现的安全性。

1 引言

本文提出的加密方案满足以下性质：
在给定密文的情况下，关于明文的任何有效计算，在没有密文的情况下，也是有效计算。

我们的加密方案的安全性是基于复杂性理论的。因此，当我们说对手”不可能” 从密文中计算出关于明文的任何信息时，我们的意思是，这在计算上是不可行的。

相对年轻的复杂性理论领域, 还没有能够证明哪怕是一个自然的 NP 完全问题的非线性下限。同时、尽管付出了巨大的数学努力，数论中的一些问题几个世纪以来一直没有解决。因此，为了具体实施我们的方案，我们假定数论中的一些问题是难以解决的，例如因式分解或决定复合模数的二次剩余。在这种情况下，证明一个问题是困难的意味着要证明它等同于上述问题

*原文：Goldwasser S , Micali S . Probabilistic Encryption[J]. Journal of Computer and System Sciences, 1984, 28(2):270-299.

†译者 email：cy_lxf@163.com，译文来自于译者发起的“信息安全经典翻译”开源项目 https://gitee.com/uisu/InfSecClaT

之一。换句话说，任何对我们的加密方案的具体实现的安全威胁，都会导致一个决定复合整数二次剩余的高效算法。

1.1 确定型加密：陷门函数模型 (Deterministic Encryption: The Trapdoor Function Model)

我们的加密方案得益于 DifIie 和 Hellman[9]、Rivest、Shamir 和 Adleman[21]，以及 Rabin[20] 的思想。

Diffie 和 Hellman[9] 提出了公钥密码系统的概念，它是基于一些难以解决的基础计算问题。直观地说，这个想法是要找到一个加密函数 E，它很容易计算，但很难求逆，除非已知的一些秘密信息，“陷门”。这样的函数被称为” 陷门函数”。为了加密一个信息 m，任何人都可以很容易第计算 E(m)，但只有那些知道陷门信息的人才能从 E(m) 中计算出 m。

与本文最相关和最有启发性的两个陷门函数的实现是 RSA 函数 [21]，Rivest、Shamir 和 Adleman 提出的，以及 Rabin[20] 基于 RSA 提出的一种变种。

1.2 陷门函数模型的主要异议 (Basic Objections to the Trapdoor Function Model)

我们提出这种方法的两个基本缺陷：

(1)f 是一个陷门函数的事实，并不排除当 x 是一个特殊形式时，从 $f(x)$ 计算 x 的可能性。通常情况下，信息不是由随机选择的数字组成，而是拥有更多的结构。这种结构信息可能有助于解码。例如，一个在一般输入上很难反转的函数 f，但在英语句子是 ASCII 表示时，确很容易解码。

(2)f 是一个陷门函数的事实，并不排除从 $f(x)$ 中轻松计算出关于 x 的一些部分信息（甚至是 x 的每一个其他位）的可能性。以确保所有部分信息保密的方式对信息进行加密是密码学的一个重要目标。假设我们想用加密的方式在电话中玩纸牌游戏。如果一张牌的牌型或颜色可能被泄露，那么整个游戏应该是无效的。事实上，Lipton [17] 已经指出，在 Mental Poker [22] 的 SRA 实现中，可以很容易地计算出关于要保持隐藏的牌的一比特信息。

虽然没有人知道如何破解 RSA 或 Rabin 方案，但在这些方案中，没有一个方案被证明，在不对消息空间做任何假设的情况下，解码是困难的。Rabin 表明，在这个方案中，如果可能的消息集具有某种密度特性，那么解

码对对手来说是困难的。我们在第 2 节进一步讨论这个问题。

1.3 概率加密：新模型 (Probabilistic Encryption: The New Model)

在本文中，我们从一个确定性的框架转向一个概率性的框架。这使我们能够处理陷门函数模型中出现的问题，而不需要对我们想要发送的信息施加任何概率结构。

我们用“不可近似的陷门谓词”(unapproximable trapdoor predicate) 的概念取代陷门函数的概念。简而言之，如果任何人都可以选择一个 x，使 $B(x) = 0$ 或选择一个 y，使 $B(y) = 1$，但只有那些知道陷门信息的人可以在给定的 z 下, 计算 $B(z)$ 的值，那么该谓词 B 就是陷门和不可近似的。当陷门信息未知时，具有多项式约束计算资源的对手不能比随机猜测更好地决定 $B(z)$ 的值（正式定义见 Section 3）。

我们用单比特的概率加密取代确定性的分组加密，其中”1 ” 有许多不同的编码，”0 ” 有许多不同的编码。为了加密每条信息，我们使用了一枚公平的硬币。因此，每个消息的编码将取决于该消息和一连串抛硬币的结果。更具体地说，二进制消息将被逐比特加密如下：”0” 是通过随机选择一个 x，使 B(x)=0 来编码的，”1 ” 是通过随机选择一个 x，使 B(x)=1 来编码的[1]。因此，每个信息有许多可能的编码。然而，信息总是唯一可解码的。

新模型有两个属性：

(1) 对于知道陷门信息的合法信息接收者来说，解码是很容易的，但对于敌方来说，可以证明是困难的，因此，陷门函数的精神得以保持。此外，在我们的方案中，我们没有对信息空间施加任何限制。对于属于任何概率分布的消息空间的消息，该方案的安全性被证明。

(2) 对手无法获得关于加密信息的任何信息。

假设消息空间 M 有某种概率分布，让 g $M \to V$ 是一个非常数函数 m。因此，让 $p_v = prob\left(g\left(m\right) = v | m \in M\right)$ ，对于每个 $v \in V$ ，并让 $\overline{v} \in V$ 是这样的：$p_{\overline{v}} = max_{v \in V} p_v$。那么，在没有任何特殊能力的情况下，给定加密文本的敌手总是可以猜 g 在明文上的值，并且正确概率为 $p_{\overline{v}}$。我们证明，对于一个概率加密方案，敌手在给定密文的情况下，不能以优于 $p_{\overline{v}}$ 的概率猜出明文中 g 的值。请注意，g 不需要是可多项式计算的，甚至可以是递归

[1]译者注：x 就是对应“0”或“1”的编码，或者密文。

的。因此，我们的加密模型通过了香农的完美保密定义的多项式约束版本；见 7.3 小节。

这一特性使 Goldwasser 和 Micali[11] 为心理扑克设计了一个方案，在二次剩余假设下，不容易计算出应该保持隐藏的牌的部分信息。

1.4 新模型的具体实现 (Concrete Implementation of the New Model)

我们引入了因式分解未知的复合整数的二次剩余（精确定义见第 6 节），作为不可近似的陷门谓词的第一个例子。因此，我们引入了一个新的概率性公钥密码系统，当且仅当决定复合模的二次剩余是困难的（见第 4 节），该系统在一个非常强的概率意义上是安全的。这个公钥密码系统提供的安全性延伸到所有关于加密信息的部分信息，延伸到所有可能的信息空间和所有可能的信息空间的概率分布（关于安全性的正式定义，见第 5 节）。

这种谓词的另一个例子，已经出现在 Goldwasser, Micah, and Tong [12] 和 Goldwasser [13] 中。他们提出的谓词是不可近似的，当且仅当复合数的因式分解是困难的。使用第 4 节的构造，我们可以在他们提出的谓词的基础上建立一个公钥密码系统。同样，对这个公钥密码系统安全性的任何威胁，将导致一个有效的因式分解算法。

在 [26] 中，Yao 表明，如果存在一对一的陷门函数，则存在不可近似的陷门谓词。

1.5 相关工作 (Related Work)

Blum 和 Micali 在 [5] 中展示了第一个非陷门的不可近似谓词的例子。当且仅当离散对数问题是困难的，他们的谓词是不可近似的。

二次剩余谓词不仅是一个不可近似的陷门谓词的例子，而且拥有其他的特性，使它对协议设计特别有吸引力。自从我们在 [10] 中首次提出它以来，它已被广泛使用。第一个使用该谓词的协议是由 Goldwasser 和 Micali 在 [11] 中提出。他们为两个玩家设计了一个通过电话玩心理扑克的协议，这样就没有玩家可以获得任何关于不在他手中的牌的部分信息。其他证明该谓词有用的作品有：Blum, Blum 和 Shub 的实现 [4]，一个具有密码学强度的伪随机比特发生器 [5]，Brassard 的 [7] 认证标签的实现，Luby, Micali 和 Rackoff 的 [19]，同时交换一个秘密比特的方法，以及 Vazirani 和 Vazirani

的 [25] 一个比特披露的实现。

2 SURVEY OF PUBLIC KEY CRYPTOSYSTEMS BASED ON TRAPDOOR FUNCTIONS

2.1 What Is a Public Key Cryptosystem?

2.2 The RSA Scheme and the Rabin Scheme

2.3 Objections to Cryptosystems Based on Trapdoor Functions

3 UNAPPROXIMABLE TRAPDOOR PREDICATES

3.1 Quadratic Residuosity as a UTP

4 PUBLIC KEY CRYPTOSYSTEMS AND PROBABILISTIC PUBLIC KEY CRYPTOSYSTEMS

致谢

参考文献