密码学的新方向

特邀论文

WHITFIELD DIFFIE 与 MARTIN E. HELLMAN，IEEE 会员

摘要 — 本文审视了密码学中两类当代发展。远程信息处理应用的扩大催生了对新型密码系统的需求，这些系统应能最大限度地减少对安全密钥分发通道的依赖，并提供等同于手写签名的功能。本文提出了解决这些当前开放性问题的方法，并讨论了通信与计算理论如何开始为解决长期存在的密码学问题提供工具。

I. 引言

我们正站在密码学革命的边缘。廉价数字硬件的发展使其摆脱了机械计算的设计限制，并将高级密码设备的成本降至可用于远程取款机和计算机终端等商业应用的水平。反过来，这些应用产生了对新型密码系统的需求，这些系统应能最大限度地减少对安全密钥分发通道的需求，并提供等同于手写签名的功能。与此同时，信息论和计算机科学的理论发展有望提供可证明安全的密码系统，将这门古老的艺术转变为一门科学。

由计算机控制的通信网络的发展，有望实现世界两端的人员或计算机之间轻松且廉价的联系，从而通过远程通信取代大部分邮件和许多出行。对于许多应用，必须保护这些联系免受窃听和非法消息注入的侵害。然而，目前安全问题的解决远远落后于通信技术的其他领域。当代密码学无法满足这些要求，因为它的使用会给系统用户带来严重不便，以至于抵消了远程处理的许多好处。

最著名的密码学问题是保密性问题：防止从未经授权的通信中提取信息。然而，为了使用密码学来确保隐私，目前通信双方必须共享一个密钥，且该密钥不为他人所知。这通常通过提前通过某些安全通道（如私人信使或挂号邮件）发送密钥来实现。然而，在商业中，两个素不相识的人进行私人对话是很常见的，期望初始商业联系被推迟足够长的时间以便通过某种物理方式传输密钥是不现实的。由这个密钥分发问题带来的成本和延迟，是商业通信向大型远程处理网络转移的主要障碍。

第三节提出了两种通过公共（即不安全）信道传输密钥信息而不损害系统安全的方法。在公钥密码系统中，加密和解密由不同的密钥 E 和 D 控制，使得从 E 计算 D 在计算上是不可行的（例如，需要 10^{100} 条指令）。因此，加密密钥 E 可以公开披露而不泄露解密密钥 D 。这样，网络的每个用户都可以将其加密密钥放在公共目录中。这使得系统的任何用户都能向任何其他用户发送消息，该消息以只有预期接收者才能解密的方式进行加密。因此，公钥密码系统是一种多址密码。这样，任何两个个体之间都可以进行私人对话，无论他们以前是否曾通信过。每个人都使用接收者的公共加密密钥对发送给另一方的消息进行加密，并使用自己的秘密解密密钥解密接收到的消息。

我们提出了一些开发公钥密码系统的技术，但这个问题在很大程度上仍然是开放的。

公钥分发系统提供了一种不同的方法来消除对安全密钥分发通道的需求。在这样的系统中，希望交换密钥的两个用户来回通信，直到他们得到一个共同的密钥。窃听此交换过程的第三方必须发现，从窃听到的信息中计算密钥在计算上是不可行的。第三节给出了公钥分发问题的一个可能解决方案，而 Merkle [1] 则有另一种形式的部分解决方案。

阻碍用远程处理系统取代当代商业通信的第二个问题，是**认证**问题，它同样适用于密码学解决方案。在当前的商业中，合同的有效性由签名保证。签名的合同作为协议的法律证据，必要时持有者可以在法庭上出示。然而，签名的使用需要传输和存储书面合同。为了拥有这种纸质工具的纯数字替代品，每个用户必须能够生成一条消息，其真实性可以被任何人验证，但除了发送者本人外，任何其他人（甚至接收者）都无法生成。由于只有一个人可以发起消息，但许多人可以接收消息，这可以被视为一种广播密码。当前的电子认证技术无法满足这一需求。

第四节讨论了提供真实的、数字的、依赖于消息的签名的问题。基于那里提出的原因，我们将其称为**单向认证问题**。我们给出了一些部分解决方案，并展示了任何公钥密码系统如何能够转换为单向认证系统。

第五节将考虑各种密码学问题之间的相互关系，并引入更困难的**陷门**问题。

与此同时，在通信和计算引发新的密码学问题的同时，它们的产物——信息论和计算理论——已经开始为古典密码学中重要问题的解决提供工具。

寻找不可破译的密码是密码学研究最古老的主题之一，但直到本世纪，所有提出的系统最终都被破解了。然而，在二十世纪二十年代，“一次一密”被发明出来，并被证明是不可破译的[2, pp. 398-400]。支撑这一系统及相关系统的理论基础在四分之一世纪后由信息论奠定了坚实的基础[3]。一次一密需要极长的密钥，因此在大多数应用中成本高得令人望而却步。

相比之下，大多数密码系统的安全性在于，密码分析者在不知道密钥的情况下发现明文的计算难度。这个问题属于计算复杂性和算法分析两个近期学科的范畴，它们研究解决计算问题的难度。利用这些理论的结果，在可预见的将来，有可能将安全性证明扩展到更有用的系统类别。第六节探讨了这种可能性。

在继续讨论新发展之前，我们将在下一节介绍术语并定义威胁环境。

II. 传统密码学

密码学是研究用于解决两类安全问题的“数学”系统：**保密**和**认证**。保密系统防止未经授权方从通过公共信道传输的消息中提取信息，从而向消息发送者保证其消息仅被预期接收者阅读。认证系统防止未经授权的消息注入公共信道，从而向消息接收者保证其发送者的合法性。

如果一个信道的安全性不足以满足其用户的需求，则被视为公共信道。因此，像电话线这样的信道可能被某些用户视为私有的，而被另一些用户视为公共的。任何信道都可能面临窃听或注入的威胁，这取决于其用途。在电话通信中，注入的威胁是首要的，因为接听方无法确定是哪个电话在呼叫。窃听需要使用窃听器，技术上更困难，法律上也更有风险。相比之下，在无线电通信中，情况正好相反。窃听是被动的，不涉及法律风险，而注入则使非法发射者面临被发现和起诉的风险。

将我们的问题分为保密和认证问题之后，我们有时会进一步将认证细分为**消息认证**（即上述定义的问题）和**用户认证**，在后一种情况下，系统的唯一任务是验证个人是否是其声称的身份。例如，必须验证出示信用卡的个人的身份，但他没有要传输的消息。尽管在用户认证中似乎没有消息，但这两个问题在很大程度上是等价的。在用户认证中，存在一条隐含的消息“我是用户 X”，而消息认证只是验证发送消息方的身份。然而，这两个子问题在威胁环境和其他方面的差异，有时使得区分它们更为方便。

图 1 说明了用于通信保密的传统密码系统中的信息流。涉及三方：发送者、接收者和窃听者。发送者生成明文或未加密消息 P，通过不安全信道传送给合法接收者。为了防止窃听者获知 P，发送者使用可逆变换 S_K 对 P 进行操作，生成密文或密码 $C = S_K(P)$。密钥 K 仅通过安全信道（在图 1 中以屏蔽路径表示）传输给合法接收者。由于合法接收者知道 K，他可以通过操作 S_K^{-1} 来解密 C，得到 $S_K^{-1}(C) = S_K^{-1}(S_K(P)) = P$，即原始明文消息。由于容量或延迟的原因，安全信道不能用于传输 P 本身。例如，安全信道可能是每周一次的信使，而不安全信道可能是电话线。

密码系统是一个单参数族 $\{S_K\}_{K\in \{K\}}$ 的可逆变换

$$S_K : \{P\} \rightarrow \{C\} \tag{1}$$

从明文消息空间 $\{P\}$ 到密文消息空间 $\{C\}$。参数 K 称为密钥，是从称为密钥空间的有限集合 $\{K\}$ 中选择的。如果消息空间 $\{P\}$ 和 $\{C\}$ 相等，我们将它们都表示为 $\{M\}$。在讨论单个密码变换 S_{K} 时，我们有时会省略对系统的提及，而仅称变换 K。

设计密码系统 $\{S_K\}$ 的目标是使加密和解密操作成本低廉，但要确保任何成功的密码分析操作都过于复杂而不经济。有两种方法来解决这个问题。一个系统如果由于密码分析的计算成本而安全，但会屈服于拥有无限计算的攻击，则称为**计算上安全的**；而一个能够抵抗任何密码分析攻击（无论允许多少计算）的系统，则称为**无条件安全的**。无条件安全系统在[3]和[4]中讨论，属于信息论中称为香农理论的部分，该部分关注在无限计算情况下可获得的最佳性能。

无条件安全性源于密码存在多个有意义的解。例如，由英文文本产生的简单替换密码 XMD 可以代表明文消息：now、and、the 等。相比之下，计算上安全的密码包含足够的信息来唯一确定明文和密钥。其安全性完全在于计算它们的成本。

常用的唯一无条件安全系统是**一次一密**，其中明文与随机选择的等长密钥组合。虽然这样的系统被证明是安全的，但所需的大量密钥使其在大多数应用中不切实际。除非另有说明，本文讨论的是计算上安全的系统，因为这些系统应用更广泛。当我们谈到需要开发可证明安全的密码系统时，我们排除了那些使用不便的系统，例如一次一密。相反，我们考虑的是仅使用几百比特密钥、并且可以用少量数字硬件或几百行软件实现的系统。

我们将一个任务称为**计算上不可行的**，如果其以所用内存量或运行时间衡量的成本是有限但极其巨大的。

正如纠错码分为卷积码和分组码一样，密码系统也可以分为两大类：**流密码**和**分组密码**。流密码以小数据块（比特或字符）处理明文，通常产生一个伪随机比特序列，该序列与明文的比特进行模 2 加。分组密码以纯组合方式对大块文本进行操作，使得输入块中的微小变化会在输出中产生重大变化。本文主要讨论分组密码，因为这种错误传播特性在许多认证应用中很有价值。

在认证系统中，密码学用于向接收者保证消息的真实性。不仅要防止篡改者向信道中注入全新的、看起来真实的
消息，还要防止他通过组合或仅仅是重复过去复制的旧消息来创建看似真实的消息。旨在保证隐私的密码系统通常无法防止后一种形式的恶作剧。

为了保证消息的真实性，添加的信息不仅是消息和秘密密钥的函数，还是日期和时间的函数；例如，通过将日期和时间附加到每条消息并对整个序列进行加密。这确保了只有拥有密钥的人才能生成一条消息，该消息在解密后将包含正确的日期和时间。然而，必须注意使用一个密文的微小变化会导致解密的明文发生巨大变化的系统。这种有意的错误传播确保了，如果故意在信道上注入噪声将消息如“删除文件 7”更改为不同的消息如“删除文件 8”，它也会破坏认证信息。然后该消息将被视为不真实而被拒绝。

评估密码系统充分性的第一步是分类它们将面临的威胁。以下威胁可能发生在用于保密或认证的密码系统中。

唯密文攻击是一种密码分析攻击，其中密码分析者仅拥有密文。

已知明文攻击是一种密码分析攻击，其中密码分析者拥有大量对应的明文和密文。

选择明文攻击是一种密码分析攻击，其中密码分析者可以提交任意数量的自己选择的明文消息并检查产生的密码。

在所有情况下，都假设对手知道正在使用的一般系统 $\{S_K\}$，因为通过研究密码设备可以获得此信息。虽然许多密码学用户试图对其设备保密，但许多商业应用不仅要求一般系统公开，而且要求其标准化。

唯密文攻击在实践中经常发生。密码分析者仅使用所用语言的统计特性知识（例如，在英语中，字母 e 出现 13% 的时间）和某些“可能”词汇的知识（例如，信件可能以“Dear Sir:”开头）。这是系统可能面临的最弱威胁，任何屈服于此的系统都被认为是完全不安全的。

能够抵抗已知明文攻击的系统使用户无需对过去的消息保密，或在解密前对其进行改述。这对系统用户来说是一个不合理的负担，特别是在商业环境中，产品公告或新闻稿可能以加密形式发送，以便日后公开披露。在外交通信中的类似情况导致了许多本应安全的系统被破解。虽然已知明文攻击并不总是可行的，但其发生频率足以让无法抵抗它的系统被视为不安全。

选择明文攻击在实践中很难实现，但可以近似。例如，向竞争对手提交提案可能导致他将其加密传输到总部。因此，能够抵抗选择明文攻击的密码使其用户无需担心对手是否能在其系统中植入消息。

为了认证系统的安全性，考虑更强大的密码分析威胁是合适的，因为这些不仅为密码系统的工作环境提供了更真实的模型，而且使评估系统强度更容易。许多在唯密文攻击下难以分析的系统，在已知明文或选择明文攻击下可以立即被排除。

从这些定义可以清楚地看出，密码分析是一个系统辨识问题。已知明文和选择明文攻击分别对应于被动和主动系统辨识问题。与许多考虑系统辨识的学科（如自动故障诊断）不同，密码学的目标是构建难以而非易于辨识的系统。

选择明文攻击通常称为 IFF 攻击，该术语源于二战后密码学“敌我识别”系统开发中的起源。IFF 系统使军用雷达能够自动区分友方和敌方飞机。雷达向飞机发送一个时变询问，飞机接收询问，在适当的密钥下加密，然后将其发送回雷达。通过将此响应与正确加密的询问版本进行比较，雷达可以识别友方飞机。当飞机在敌方领土上空时，敌方密码分析者可以发送询问并检查加密响应，试图确定正在使用的认证密钥，从而对系统发起选择明文攻击。在实践中，通过限制询问的形式来应对这种威胁，询问不必是不可预测的，只需不重复即可。

认证系统还存在其他威胁，传统密码学无法处理，需要借助本文介绍的新思想和技术。**接收方认证数据泄露**的威胁源于多用户网络中的情况，其中接收方通常是系统本身。接收方的密码表和其他认证数据比发送方（单个用户）的数据更容易被盗。如下文所示，一些针对此威胁的保护技术也同时防范**争议**威胁。即，一条消息可能被发送，但后来被发送方或接收方否认。或者，任何一方可能声称发送了一条消息，而实际上没有发送。需要不可伪造的数字签名和收据。例如，不诚实的股票经纪人可能试图通过伪造客户订单来掩盖为个人利益进行的未经授权的买卖，或者客户可能声称一条实际由他授权但后来发现会导致损失的订单。我们将引入一些概念，允许接收方验证消息的真实性，但防止他生成看似真实的消息，从而保护免受接收方认证数据泄露和争议的威胁。

III. 公钥密码学

如图 1 所示，密码学一直是一种衍生的安全措施。一旦存在可以传输密钥的安全信道，就可以通过加密在其上发送的消息，将安全性扩展到带宽更高或延迟更低的其他信道。其效果是限制了密码学在已经为密码安全做了事先准备的人们之间的通信中使用。

为了开发大型、安全的电信系统，必须改变这种情况。大量的用户 n 导致更大的潜在对数 $(n^2 - n) / 2$，他们可能希望私下通信，不受所有其他人干扰。假设两个素不相识的用户能够等待通过某种安全的物理方式发送密钥，或者提前安排所有 $(n^2 - n) / 2$ 对的密钥，都是不现实的。在另一篇论文[5]中，作者考虑了一种保守的方法，不需要密码学本身有新的发展，但这涉及安全性降低、不便以及网络在初始连接协议方面局限于星形配置。

我们提出，可以开发如图 2 所示的系统，其中两方仅通过公共信道并使用仅公开已知的技术即可建立安全连接。我们研究了解决这个问题的两种方法，分别称为**公钥密码系统**和**公钥分发系统**。前者功能更强大，适用于解决下一节讨论的认证问题，而后者则更容易实现。

公钥密码系统是两族算法 $\{E_K\}_{K\in \{K\}}$ 和 $\{D_K\}_{K\in \{K\}}$，表示有限消息空间 $\{M\}$ 上的可逆变换，

$$E_K : \{M\} \rightarrow \{M\} \tag{2}$$

$$D_K : \{M\} \rightarrow \{M\} \tag{3}$$

使得

1) 对于每个 $K \in \{K\}$，E_K 是 D_K 的逆，

2) 对于每个 $K \in \{K\}$ 和 $M \in \{M\}$，算法 E_K 和 D_K 易于计算，

3) 对于几乎所有 $K \in \{K\}$，任何等价于 D_K 的易于计算的算法都难以从 E_K 推导出来。

4) 对于每个 $K \in \{K\}$，从 K 计算逆对 E_K 和 D_K 是可行的。

由于第三个特性，用户的加密密钥 E_K 可以公开，而不会泄露其秘密解密密钥 D_K 的安全性。因此，密码系统被分成两个部分：一族加密变换和一族解密变换，使得给定其中一个族的成员，要找到另一个族的对应成员是不可行的。

第四个特性保证了，当对加密或解密变换的内容不加限制时，存在一种可行的方法来计算相应的逆变换对。在实践中，密码设备必须包含一个真正的随机数生成器（例如，噪声二极管）来生成 K，以及一个从其输出生成 $E_K - D_K$ 对的算法。

有了这种系统，密钥分发问题就大大简化了。每个用户在其终端生成一对逆变换 E 和 D。解密变换 D 必须保密，但永远不需要在任何信道上传输。解密密钥 E 可以通过将其与用户的姓名和地址一起放在公共目录中而公开。然后任何人都可以加密消息并将其发送给该用户，但其他任何人都无法解密发送给他的消息。因此，公钥密码系统可以被视为多址密码。

至关重要的是，必须保护加密密钥的公共文件免受未经授权的修改。这个任务由于文件的公共性质而变得更容易。读取保护是不必要的，并且由于文件很少被修改，可以经济地采用精细的写入保护机制。

一个具有启发性但不幸无用的公钥密码系统示例是：将表示为二进制 n 向量 $\mathbf{m}$ 的明文，乘以一个可逆的二进制 $n \times n$ 矩阵 E 来加密。因此，密文等于 $E \mathbf{m}$。令 $D = E^{-1}$，我们有 $\mathbf{m} = D \mathbf{c}$。因此，加密和解密都需要大约 n^2 次运算。然而，从 E 计算 D 涉及矩阵求逆，这是一个更难的问题。并且，获得任意一对逆矩阵至少在概念上比求给定矩阵的逆更简单。从单位矩阵 I 开始，进行初等行和列运算以获得任意可逆矩阵 E。然后从 I 开始，按相反顺序进行这些相同初等运算的逆运算以获得 $D = E^{-1}$。初等运算的序列可以很容易地从随机比特串确定。

不幸的是，矩阵求逆仅需大约 n^3 次运算。因此，“密码分析”时间（即从 E 计算 D）与加密或解密时间的比率最多为 n，需要巨大的分组大小才能获得 10^6 或更高的比率。此外，似乎了解用于从 I 获得 E 的初等运算并不会大大减少计算 D 的时间。而且，由于二进制算术中没有舍入误差，数值稳定性在矩阵求逆中并不重要。尽管缺乏实际效用，这个矩阵例子对于阐明公钥密码系统中必要的关系仍然是有用的。

寻找一对易于计算的逆算法 E 和 D（使得从 E 推断 D 很困难）的更实用方法利用了分析低级语言程序的难度。任何曾尝试确定别人的机器语言程序完成什么操作的人都知道，从 E 的算法推断 E 本身（即 E 做什么）可能很困难。如果通过添加不需要的变量和语句使程序故意混乱，那么确定逆算法可能会变得非常困难。当然，E 必须足够复杂，以防止从输入-输出对中识别它。

本质上需要的是一个**单向编译器**：一个将用高级语言编写的易于理解的程序翻译成某种机器语言中难以理解的程序的编译器。编译器是单向的，因为编译必须是可行的，而逆转这个过程是不可行的。由于在此应用中程序大小和运行时间的效率并不关键，如果机器语言的结构可以优化以帮助混淆，这样的编译器也许是可能的。

Merkle [1] 独立研究了通过不安全信道分发密钥的问题。他的方法不同于上面提出的公钥密码系统，将被称为**公钥分发系统**。目标是让两个用户 A 和 B 通过不安全信道安全地交换密钥。然后该密钥由两个用户在正常的密码系统中用于加密和解密。Merkle 有一个解决方案，其密码分析成本以 n^2 增长，其中 n 是合法用户的成本。不幸的是，合法用户的系统成本在传输时间和计算时间上都很高，因为 Merkle 的协议在决定一个密钥之前需要传输 n 个潜在密钥。Merkle 指出，这种高传输开销使得该系统在实践中不太有用。如果对设置协议的开销施加一兆比特的限制，他的技术可以实现大约 10,000 比 1 的成本比率，这对于大多数应用来说太小了。如果廉价、高带宽的数据链路变得可用，则可以实现一百万比一或更高的比率，该系统将具有重要的实用价值。

我们现在提出一个新的公钥分发系统，它具有几个优点。首先，它只需要交换一个“密钥”。其次，密码分析的工作量似乎相对于合法用户的工作量呈指数增长。第三，它的使用可以与用户信息的公共文件联系起来，该文件用于向用户 B 认证用户 A，反之亦然。通过使公共文件基本上成为只读存储器，一次亲自露面允许用户多次向多个用户认证其身份。Merkle 的技术要求 A 和 B 通过其他方式验证彼此的身份。

新技术利用了在具有素数 q 个元素的有限域 $GF(q)$ 上计算对数的明显困难。令

其中 α 是 $GF(q)$ 的一个固定本原元，则 X 被称为 Y 以 α 为底的**对数**，模 q：

从 X 计算 Y 很容易，最多需要 $2 \times \log_2 q$ 次乘法[6, pp. 398-422]。例如，对于 $X = 18$，

另一方面，从 Y 计算 X 可能要困难得多，并且对于某些精心选择的 q 值，使用已知的最佳算法[7, pp. 9, 575-576], [8] 需要大约 $q^{1/2}$ 次运算。

我们技术的安全性关键取决于计算模 q 对数的难度，如果找到一个复杂度按 $\log_2 q$ 增长的算法，我们的系统就会被攻破。虽然问题陈述的简单性可能允许这种简单算法，但它也可能允许证明问题的难度。目前我们假设，计算模 q 对数的最佳已知算法实际上接近最优，因此对于适当选择的 q，$q^{1/2}$ 是问题复杂性的良好度量。

每个用户生成一个独立的随机数 X_{i}，该数从整数集 $\{1,2,\dots ,q - 1\}$ 中均匀选择。每个人保密 X_{i}，但将

与他的姓名和地址一起放在公共文件中。当用户 i 和 j 希望私下通信时，他们使用

作为他们的密钥。用户 i 通过从公共文件获取 Y_{j} 并令

来获得 K_{ij}。用户 j 以类似方式获得 K_{ij}

另一个用户必须从 Y_{i} 和 Y_{j} 计算 K_{ij}，例如，通过计算

因此我们看到，如果模 q 对数易于计算，系统就会被攻破。虽然我们目前没有反证的证明（即，如果模 q 对数难以计算，则系统是安全的），我们也没有看到任何在不首先获得 X_i 或 X_j 的情况下从 Y_i 和 Y_j 计算 K_{ij} 的方法。

如果 q 是一个略小于 2^b 的素数，那么所有量都可以表示为 b 比特数。指数运算最多需要 $2b$ 次模 q 乘法，而根据假设，取对数需要 $q^{1/2} = 2^{b/2}$ 次运算。因此，密码分析的工作量相对于合法工作量呈指数增长。如果 $b = 200$，则最多需要 400 次乘法从 X_i 计算 Y_i，或从 Y_i 和 X_j 计算 K_{ij}，但计算模 q 对数需要 2^{100} 或大约 10^{30} 次运算。

IV. 单向认证

认证问题可能比密钥分发问题更严重地阻碍电信在商业交易中的普遍采用。认证是任何涉及合同和计费的系统的核心。没有它，业务就无法运作。当前的电子认证系统无法满足对纯数字的、不可伪造的、依赖于消息的签名的需求。它们提供针对第三方伪造的保护，但不保护发送方和接收方之间的争议。

为了开发一个能够用某种纯电子形式的通信取代当前书面合同的系统，我们必须发现一种具有与手写签名相同属性的数字现象。它必须让任何人都容易识别签名是真实的，但除了合法的签署者外，任何人都无法产生它。我们将任何此类技术称为**单向认证**。由于任何数字信号都可以精确复制，真正的数字签名必须在未被知晓的情况下即可被识别。

考虑多用户计算机系统中的“登录”问题。用户在设置其账户时选择一个密码，该密码被输入到系统的密码目录中。每次他登录时，系统会再次要求他提供密码。通过将此密码对所有其他用户保密，可以防止伪造登录。然而，这使得保护密码目录的安全变得至关重要，因为它包含的信息将允许完美地冒充任何用户。如果系统操作员有合法理由访问该目录，问题会进一步复杂化。允许此类合法访问，但防止所有其他访问，几乎是不可能的。

这导致了对新登录程序的看似不可能的要求：能够在不实际知道密码的情况下判断密码的真实性。虽然这看起来是逻辑上的不可能，但这个提议很容易满足。当用户第一次输入其密码 PW 时，计算机自动且透明地计算一个函数 $f(PW)$ 并存储这个值，而不是 PW，到密码目录中。在每次后续登录时，计算机计算 $f(X)$，其中 X 是提供的密码，并将 $f(X)$ 与存储的值 $f(PW)$ 进行比较。当且仅当它们相等时，用户才被接受为真实的。由于函数 f 必须每次登录计算一次，其计算时间必须很小。一百万条指令（在两百周年纪念价格下成本约为 0.10 美元）似乎是此计算的合理限制。然而，如果我们能确保计算 f^{-1} 需要 10^{30} 条或更多指令，那么破坏系统以获得密码目录的人将无法在实践中从 $f(PW)$ 获得 PW，因此无法执行未经授权的登录。请注意，$f(PW)$ 不被登录程序接受为密码，因为它会自动计算 $f(f(PW))$，这将与密码目录中的条目 $f(PW)$ 不匹配。

我们假设函数 f 是公共信息，因此不是对 f 的无知使得计算 f^{-1} 变得困难。此类函数被称为**单向函数**，由 R. M. Needham [9, p. 91] 首次用于登录程序。它们也在两篇最近的论文[10], [11]中讨论，这些论文提出了设计单向函数的有趣方法。

更精确地说，函数 f 是单向函数，如果对于 f 定义域中的任何参数 x，容易计算对应的值 $f(x)$，然而，对于 f 值域中的几乎所有 y，解方程 $y = f(x)$ 以得到任何合适的参数 x 在计算上是不可行的。

重要的是要注意，我们定义的是一个从计算角度不可逆的函数，但其不可逆性与数学中通常遇到的完全不同。函数 f 通常在其逆不唯一时被称为“不可逆”（即，存在不同的点 x_{1} 和 x_{2} 使得 $f(x_{1}) = y = f(x_{2})$）。我们强调，这不是所需的那种求逆困难。相反，给定一个值 y 和 f 的知识，计算任何满足 $f(x) = y$ 的 x 必须是极其困难的。实际上，如果 f 在通常意义上是不可逆的，可能会使寻找逆像的任务更容易。在极端情况下，如果对于定义域中的所有 x 有 $f(x) \equiv y_{0}$，那么 f 的值域是 $\{y_{0}\}$，我们可以取任何 x 作为 $f^{-1}(y_{0})$。因此，f 不能过于退化是必要的。小程度的退化是可以容忍的，并且如后面所讨论的，可能存在于最有希望的一类单向函数中。

多项式提供了单向函数的一个基本例子。寻找多项式方程 $p(x) = y$ 的根 x_0 比在 $x = x_0$ 处求多项式 $p(x)$ 的值要困难得多。Purdy [11] 建议使用有限域上的稀疏高次多项式，它们似乎具有非常高的求解时间与求值时间的比率。单向函数的理论基础在第六节有更详细的讨论。并且，如第五节所示，在实践中很容易设计单向函数。

单向函数登录协议只解决了多用户系统中出现的一些问题。它保护系统认证数据在未使用时不被泄露，但仍要求用户向系统发送真实密码。必须通过额外的加密来提供针对窃听的保护，而针对争议威胁的保护则完全不存在。

公钥密码系统可用于产生真正的单向认证系统，如下所示。如果用户 A 希望向用户 B 发送消息 M，他用自己的秘密解密密钥对其进行“解密”并发送 $D_A(M)$。当用户 B 收到它时，他可以阅读它，并通过用用户 A 的公共加密密钥 E_A 对其进行“加密”来确信其真实性。B 还将 $D_A(M)$ 保存为消息来自 A 的证据。任何人都可以通过用公开已知的操作 E_A 对 $D_A(M)$ 进行操作以恢复 M 来验证这一声明。由于只有 A 才能生成具有此属性的消息，单向认证问题的解决方案将随着公钥密码系统的发展而立即出现。

单向消息认证有一个部分解决方案，由马萨诸塞州计算机联合公司的 Leslie Lamport 向作者建议。该技术采用一个单向函数 f，将 k 维二进制空间映射到自身，k 大约为 100。如果发送者希望发送一条 N 比特消息，他生成 $2N$ 个随机选择的 k 维二进制向量 $x_{1}, X_{1}, x_{2}, X_{2}, \dots, x_{N}, X_{N}$ 并保密。接收者获得它们在 f 下的对应像，即 $y_{1}, Y_{1}, y_{2}, Y_{2}, \dots, y_{N}, Y_{N}$。后来，当要发送消息 $m = (m_{1}, m_{2}, \dots, m_{N})$ 时，发送者根据 $m_{1} = 0$ 或 1 发送 x_{1} 或 X_{1}。他根据 $m_{2} = 0$ 或 1 发送 x_{2} 或 X_{2}，依此类推。接收者对第一个接收到的块使用 f 操作，看它产生 y_{1} 还是 Y_{1} 作为其像，从而了解它是 x_{1} 还是 X_{1}，以及 $m_{1} = 0$ 还是 1。以类似的方式，接收者能够确定 $m_{2}, m_{3}, \dots, m_{N}$。但是接收者无法伪造 m 中即使一个比特的改变。

这只是部分解决方案，因为它需要大约 100 倍的数据扩展。然而，当 N 大约为一兆比特或更多时，存在一种修改可以消除扩展问题。令 g 为从二进制 N 空间到二进制 n 空间的单向映射，其中 n 大约为 50。取 N 比特消息 m 并用 g 操作得到 n 比特向量 $\pmb{m}^{\prime}$。然后使用先前的方案发送 $\pmb{m}^{\prime}$。如果 $N = 10^{6}$，$n = 50$，且 $k = 100$，这向消息添加了 $kn = 5000$ 个认证比特。因此，在传输过程中仅产生 5% 的数据扩展（如果包括初始交换的 $y_{1}, Y_{1}, \dots, y_{N}, Y_{N}$，则为 15%）。尽管平均有大量其他消息（ $2^{N - n}$ 条）具有相同的认证序列，但 g 的单向性使得它们在计算上难以找到，从而难以伪造。实际上，g 必须比普通的单向函数稍强一些，因为对手不仅拥有 $\pmb{m}^{\prime}$，还拥有它的一个逆像 $\pmb{m}$。即使给定 $\pmb{m}$，也必须难以找到 $\pmb{m}^{\prime}$ 的不同逆像。寻找这样的函数似乎没什么问题（见第五节）。

单向用户认证问题还有另一个部分解决方案。用户生成一个密码 X 并保密。他向系统提供 $f^{T}(X)$，其中 f 是单向函数。在时间 t，适当的认证符是 $f^{T - t}(X)$，系统可以通过应用 $f^{t}(X)$ 来检查。由于 f 的单向性，过去的响应对于伪造新响应没有价值。这个解决方案的问题在于，合法的登录可能需要相当多的计算（尽管比伪造少许多数量级）。例如，如果 t 每秒递增一次，并且系统每个密码必须工作一个月，那么 $T = 260$ 万。用户和系统每次登录平均必须迭代 f 130 万次。虽然并非不可克服，但这个问题显然限制了该技术的使用。如果能够找到一种简单的方法来计算 $f^{(2\uparrow n)}$，对于 $n = 1,2,\dots$，就像 $X^{8} = ((X^{2})^{2})^{2}$ 那样，那么这个问题可能会被克服。因为这样，$T - t$ 和 t 的二进制分解将允许快速计算 $f^{T - t}$ 和 f^{t}。然而，快速计算 f^{n} 可能会妨碍 f 成为单向函数。

V. 问题相互关系和陷门

在本节中，我们将展示迄今为止提出的一些密码学问题可以归约为其他问题，从而根据难度定义一个松散的顺序。我们还引入了更困难的陷门问题。

在第二节中，我们展示了用于保密的密码系统也可以用于提供针对第三方伪造的认证。这样的系统也可以用于创建其他密码学对象。

能够抵抗已知明文攻击的密码系统可用于产生单向函数。

如图 3 所示，取能够抵抗已知明文攻击的密码系统 $\{S_K: \{P\} \to \{C\}\}_{K \in \{K\}}$，固定 $P = P_0$，并考虑映射

定义为

这个函数是单向的，因为根据 $f(X)$ 求解 X 等价于从单个已知明文-密文对找到密钥的密码分析问题。现在公开 f 的知识等价于公开 $\{S_K\}$ 和 P_0 的知识。

虽然这个结果的逆不一定成立，但在寻找单向函数的过程中最初发现的函数有可能产生一个好的密码系统。这实际上发生在第三节讨论的离散指数函数上[8]。

单向函数是分组密码和密钥生成器的基础。密钥生成器是一种伪随机比特生成器，其输出（密钥流）与以二进制形式表示的消息进行模 2 加，模仿一次一密。密钥用作“种子”，决定伪随机密钥流序列。因此，已知明文攻击就简化为从密钥流确定密钥的问题。为了使系统安全，从密钥流计算密钥必须是计算上不可行的。同时，为了使系统可用，从密钥计算密钥流必须是计算上简单的。因此，一个好的密钥生成器几乎根据定义就是单向函数。

使用任何一种密码系统作为单向函数都存在一个小问题。如前所述，如果函数 f 不是唯一可逆的，则不一定（或不可能）找到实际使用的 X 值。相反，任何具有相同像的 X 就足够了。并且，虽然密码系统中的每个映射 S_{K} 必须是双射的，但上述从密钥到密文的函数 f 没有这样的限制。实际上，保证密码系统具有此属性似乎相当困难。在一个好的密码系统中，映射 f 可以预期具有随机选择的映射的特征（即，$f(X_{i})$ 从所有可能的 Y 中均匀选择，且连续选择是独立的）。在这种情况下，如果 X 被均匀选择，并且密钥和消息数量相等（X 和 Y），则所得 Y 有 $k + 1$ 个逆的概率大约为 $e^{-1} / k!$，其中 $k = 0,1,2,3,\dots$。这是一个均值为 $\lambda = 1$、偏移了 1 个单位的泊松分布。因此，预期的逆的数量仅为 2。虽然 f 可能更退化，但一个好的密码系统不会太退化，否则密钥就没有被充分利用。在最坏的情况下，如果对于某个 Y_{0} 有 $f(X) \equiv Y_{0}$，那么我们就有 $S_{K}(P_{0}) \equiv C_{0}$，并且 P_{0} 的加密将完全不依赖于密钥！

虽然我们通常感兴趣的是定义域和值域大小相当的函数，但也有例外。在上一节中，我们需要一个将长字符串映射到短得多的字符串的单向函数。通过使用密钥长度大于分组大小的分组密码，可以使用上述技术获得此类函数。

Evans 等人[10] 有一种不同的方法从分组密码构造单向函数。他们不是选择一个固定的 P_0 作为输入，而是使用函数

这是一种有吸引力的方法，因为这类方程通常难以求解，即使族 S 相对简单。然而，这种增加的复杂性破坏了系统 S 在已知明文攻击下的安全性与 f 的单向性之间的等价性。

另一种关系已经在第四节中展示。

公钥密码系统可用于生成单向认证系统。

反之似乎不成立，使得构造公钥密码系统成为一个比单向认证严格更困难的问题。类似地，公钥密码系统可以用作公钥分发系统，但反之则不然。

由于在公钥密码系统中，使用 E 和 D 的一般系统必须是公开的，指定 E 就指定了一个将输入消息转换为输出密码的完整算法。因此，公钥系统实际上是一组**陷门单向函数**。这些函数并不是真正的单向函数，因为存在易于计算的逆。但是给定正向函数的算法，要找到一个易于计算的逆在计算上是不可行的。只有通过了解某些陷门信息（例如，产生 $E-D$ 对的随机比特串），才能轻松找到易于计算的逆。

陷门已经在前一段中以陷门单向函数的形式出现，但也存在其他变体。**陷门密码**是一种强烈抵抗任何不拥有密码设计中使用的陷门信息的人进行密码分析的密码。这使得设计者可以在将系统出售给客户后破解它，却仍能虚假地维持其作为安全系统构建者的声誉。重要的是要注意，允许设计者做其他人做不到的事情，并不是因为他更聪明或拥有更多的密码学知识。如果他丢失了陷门信息，他的处境不会比其他人更好。这种情况与密码锁完全类似。任

何知道组合的人都能在几秒钟内完成，即使是熟练的锁匠也需要数小时才能完成的事情。然而，如果他忘记了组合，他就没有任何优势。

陷门密码系统可用于产生公钥分发系统。

为了让 A 和 B 建立一个共同的私有密钥，A 随机选择一个密钥，并向 B 发送一个任意的明文-密文对。B 公开了陷门密码，但保密了陷门信息，他使用明文-密文对来求解密钥。A 和 B 现在有了一个共同的密钥。

目前几乎没有证据表明陷门密码存在。然而，它们是一种明显的可能性，在从可能的对手那里接受密码系统时应牢记[12]。

根据定义，我们将要求陷门问题必须是设计陷门在计算上可行的问题。这为第三类实体留下了空间，我们将为其使用前缀“拟”。例如，**拟单向函数**不是单向的，因为存在易于计算的逆。然而，即使是设计者，要找到这个易于计算的逆在计算上也是不可行的。因此，拟单向函数可以代替单向函数使用，基本上没有安全性损失。

丢失陷门单向函数的陷门信息会使其变成拟单向函数，但也可能存在不是以这种方式获得的单向函数。

拟单向函数被排除在单向函数类别之外完全是定义的问题。人们也可以讨论广义的或严格意义上的单向函数。

类似地，**拟安全密码**是一种即使其设计者也能成功抵抗密码分析，但存在计算高效的密码分析算法（该算法当然是计算上不可行的）的密码。同样，从实际角度来看，安全密码和拟安全密码之间基本上没有区别。

我们已经看到，公钥密码系统意味着陷门单向函数的存在。然而，反之则不成立。对于陷门单向函数可用作公钥密码系统，它必须是可逆的（即，具有唯一的逆）。

VI. 计算复杂性

密码学与所有其他努力领域的不同之处在于，其要求似乎很容易被满足。简单的变换就能将可读的文本转换成看似无意义的混乱。批评者若想声称通过密码分析仍可能恢复其含义，则需进行艰苦的论证才能证明其观点正确。然而，经验表明，很少有系统能够抵抗熟练密码分析师的协同攻击，许多本应安全的系统随后都被破解了。

因此，判断新系统的价值一直是密码学家的核心关切。在十六和十七世纪，经常引用数学论证来论证密码方法的强度，通常依赖于显示可能密钥数量极其庞大的计数方法。尽管这个问题过于复杂，无法用如此简单的方法解决，但即使是著名的代数学家 Cardano 也落入了这个陷阱[2, p. 145]。随着许多如此论证强度的系统被反复破解，通过数学证明来论证系统安全性的观念声名狼藉，并被通过密码分析攻击来认证的方式所取代。

然而，在本世纪，钟摆已经开始向另一个方向摆动。在信息论诞生密切相关的一篇论文中，香农[3]证明了自二十年代后期以来一直在使用的一次一密系统提供了“完美保密性”（一种无条件安全的形式）。香农研究的可证明安全系统依赖于使用密钥长度随消息长度线性增长，或者依赖于完美的信源编码，因此对于大多数用途来说过于笨拙。我们注意到，无论是公钥密码系统还是单向认证系统，都不可能是无条件安全的，因为公共信息总是在有限集合中唯一地确定秘密信息。在无限计算的情况下，问题可以通过直接搜索来解决。

过去十年见证了两门密切相关学科的兴起，它们致力于研究计算的成本：计算复杂性理论和算法分析。前者将计算中的已知问题按其难度分为几大类，而后者则专注于寻找更好的算法并研究它们消耗的资源。在简要介绍复杂性理论之后，我们将探讨其在密码学中的应用，特别是对单向函数的分析。

如果一个函数可以由确定性图灵机在时间上以输入长度的某个多项式函数为上界计算出来，则称其属于复杂性类 $\pmb{P}$（多项式类）。人们可能认为这是易于计算的函数类，但更准确地说，不在这个类中的函数对于至少某些输入必须是难以计算的。存在已知不属于类 $\pmb{P}$ 的问题[13, pp. 405-425]。

工程中有许多问题，除非在具有无限并行度的计算机上运行，否则用任何已知技术都无法在多项式时间内解决。这些问题可能属于也可能不属于类 $\pmb{P}$，但属于类 $\pmb{NP}$（非确定性多项式），即可在“非确定性”计算机（即具有无限并行度的计算机）上在多项式时间内解决的问题。显然，类 $\pmb{NP}$ 包含类 $\pmb{P}$，复杂性理论中的一个重大开放问题是类 $\pmb{NP}$ 是否严格更大。

在已知可在 NP 时间内解决，但不知是否可在 P 时间内解决的问题中，有旅行商问题、命题演算的可满足性问题、背包问题、图着色问题以及许多调度和最小化问题的版本[13, pp. 363-404], [14]。我们看到，并非缺乏兴趣或努力阻碍了人们为这些问题找到 $\pmb{P}$ 时间内的解决方案。因此，人们强烈认为，这些问题中至少有一个一定不在类 $\pmb{P}$ 中，因此类 $\pmb{NP}$ 是严格更大的。

Karp 确定了 NP 问题的一个子类，称为 **NP 完全问题**，其特性是，如果其中任何一个属于 $\pmb{P}$，那么所有 NP 问题都属于 $\pmb{P}$。Karp 列出了 21 个 NP 完全问题，包括上述所有问题[14]。

虽然 NP 完全问题在密码学应用中显示出前景，但目前对其难度的理解仅包括最坏情况分析。出于密码学目的，必须考虑典型的计算成本。然而，如果我们用平均或典型计算时间代替最坏情况计算时间作为我们的复杂性度量，当前关于 NP 完全问题之间等价的证明就不再有效。这表明了几个有趣的研究课题。信息论者熟悉的集合和典型性概念显然可以发挥作用。

我们现在可以确定一般密码分析问题在所有计算问题中的位置。

一个加密和解密操作可在 $\mathbf{P}$ 时间内完成的系统，其密码分析难度不能大于 $\mathbf{NP}$。

要理解这一点，可以观察到任何密码分析问题都可以通过从有限集合中选择一个密钥、逆像等来解决。非确定性地选择密钥，并在 $\pmb{P}$ 时间内验证它是正确的。如果有 M 个可能的密钥可供选择，则必须采用 M 倍并行度。例如，在已知明文攻击中，明文同时在每个密钥下加密，并与密文进行比较。由于根据假设，加密仅需 $\pmb{P}$ 时间，因此密码分析仅需 $\pmb{NP}$ 时间。

我们还观察到，一般的密码分析问题是 NP 完全的。这源于我们对密码学问题定义的广泛性。一个具有 NP 完全逆的单向函数将在下文讨论。

密码学可以直接借鉴 NP 复杂性理论，通过研究如何将 NP 完全问题适应于密码学应用。特别地，有一个被称为**背包问题**的 NP 完全问题，很容易用于构造单向函数。

令 $y = f(x) = \mathbf{a} \cdot \mathbf{x}$，其中 $\mathbf{a}$ 是已知的 n 个整数向量 $(a_{1}, a_{2}, \dots, a_{n})$，$\mathbf{x}$ 是二进制 n 向量。计算 y 很简单，涉及最多 n 个整数的和。反演 f 的问题被称为背包问题，需要找到 $\{a_{i}\}$ 的一个子集，其和为 y。

穷举搜索所有 2^{n} 个子集呈指数增长，对于大于 100 左右的 n 在计算上是不可行的。然而，必须注意选择问题的参数，以确保不可能有捷径。例如，如果 $n = 100$ 且每个 a_{i} 是 32 比特长，则 y 最多是 39 比特长，f 是高度退化的；平均只需要 2^{38} 次尝试就能找到一个解。更微不足道的是，如果 $a_{i} = 2^{i - 1}$，那么反演 f 等价于寻找 y 的二进制分解。

这个例子展示了当代复杂性理论的巨大前景和相当大的缺点。该理论只告诉我们背包问题在最坏情况下可能很难。对于任何特定数组，没有迹象表明其难度。然而，似乎从 $\{0,1,2,\dots ,2^{n - 1}\}$ 中均匀选择 $\{a_i\}$ 会导致一个问题，随着 $n\to \infty$，该问题困难的概率为 1。

另一个潜在的单向函数，在算法分析中很重要，是模 q 的指数运算，这是斯坦福大学的 John Gill 教授向作者建议的。该函数的单向性已在第三节中讨论过。

VII. 历史视角

虽然乍一看，本文提出的公钥系统和单向认证系统似乎与过去的密码学发展毫无关联，但可以将它们视为数百年来密码学趋势的自然产物。

保密是密码学的核心。然而，在早期的密码学中，对于什么应该保密存在混淆。诸如凯撒密码（其中每个字母被替换为向后三位的位置，因此 A 变为 D，B 变为 E，等等）之类的密码系统，其安全性依赖于保持整个加密过程保密。电报发明后[2, p. 191]，一般系统和特定密钥之间的区分允许一般系统被破坏（例如，通过盗窃密码设备），而不损害用新密钥加密的未来消息。这一原则由 Kerchoffs [2, p. 235] 在 1881 年编撰成文，他写道，密码系统的泄露不应给通信双方带来不便。大约在 1960 年，投入使用的密码系统被认为足够强大以抵抗已知明文密码分析攻击，从而消除了对过去消息保密的负担。每一项发展都减少了系统需要保护免受公众知晓的部分，消除了诸如在外交公文提交前进行改述之类的繁琐权宜之计。公钥系统是这种减少保密性趋势的自然延续。

在本世纪之前，密码系统仅限于可以手工或使用简单的类似计算尺的设备进行的计算。第一次世界大战后不久，出现了一个革命性的趋势，现在正开花结果。开发了用于加密的专用机器。然而，在通用数字硬件发展之前，密码学仅限于可以用简单机电系统执行的操作。数字计算机的发展使其摆脱了使用齿轮计算的限制，并允许根据纯粹的密码学标准寻找更好的加密方法。

无数次试图通过数学证明来论证密码系统可靠性的尝试失败后，导致了 Kerchoffs [2, p. 234] 在上个世纪确立的通过密码分析攻击进行认证的范式。虽然已经制定了一些一般规则，帮助设计者避免明显的弱点，但最终的测试是在最有利的条件下（例如，选择明文攻击）由熟练的密码分析师对系统进行攻击。计算机的发展首次催生了算法数学理论，该理论可以开始接近估计破解密码系统计算难度这一困难问题。因此，数学证明的地位可能会完成一个完整的循环，并重新确立为最佳认证方法。

我们在密码学历史中注意到的最后一个特征是业余和专业密码学家之间的区分。生产密码分析的技能总是严重偏向于专业人士，但创新，特别是在新型密码系统的设计方面，主要来自业余爱好者。托马斯·杰斐逊，一位密码学业余爱好者，发明了一个在第二次世界大战中仍在使用系统[2, pp. 192-195]，而二十世纪最著名的密码系统——转子机，则是由四个独立的业余爱好者同时发明的[2, pp. 415, 420, 422-424]。我们希望这将激励其他人从事这个迷人的领域工作，该领域的参与在最近过去几乎完全被政府垄断所阻碍。

参考文献

[1]. R. Merkle, "Secure communication over an insecure channel," submitted to Communications of the ACM.

[2] D. Kahn, The Codebreakers, The Story of Secret Writing. New York: Macmillan, 1967.

[3] C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J., vol. 28, pp. 656-715, Oct. 1949.

[4] M. E. Hellman, “An extension of the Shannon theory approach to cryptography,” submitted to IEEE Trans. Inform. Theory, Sept. 1975.

[5] W. Diffie and M. E. Hellman, “Multiuser cryptographic techniques,” presented at National Computer Conference, New York, June 7–10, 1976.

[6] D. Knuth, The Art of Computer Programming, Vol. 2, Semi-Numerical Algorithms. Reading, MA.: Addison-Wesley, 1969.

[7] ——, The Art of Computer Programming, Vol. 3, Sorting and Searching. Reading, MA.: Addison-Wesley, 1973.

[8] S. Pohlig and M. E. Hellman, "An improved algorithm for computing algorithms in $GF(p)$ and its cryptographic significance," submitted to IEEE Trans. Inform. Theory.

[9] M. V. Wilkes, Time-Sharing Computer Systems. New York: Elsevier, 1972.

[10] A. Evans, Jr., W. Kantrowitz, and E. Weiss, “A user authentication system not requiring secrecy in the computer,” Communications of the ACM, vol. 17, pp. 437-442, Aug. 1974.

[11] G. B. Purdy, “A high security log-in procedure,” Communications of the ACM, vol. 17, pp. 442-445, Aug. 1974.

[12] W. Diffie and M. E. Hellman, “Cryptography of the NBS data encryption standard” submitted to Computer, May 1976.

[13] A. V. Aho, J. E. Hopcroft, and J. D. Ullman, The Design and Analysis of Computer Algorithms. Reading, MA.: Addison-Wesley, 1974.

[14] R. M., Karp, "Reducibility among combinatorial problems," in Complexity of Computer Computations. R. E. Miller and J. W. Thatcher, Eds. New York: Plenum, 1972, pp. 85-104.

专业术语中英文对照表

英文术语	中文翻译
Abstract	摘要
Authentication	认证
Block cipher	分组密码

英文术语	中文翻译
Caesar cipher	凯撒密码
Chosen plaintext attack	选择明文攻击
Ciphertext	密文
Ciphertext only attack	唯密文攻击
Computational complexity	计算复杂性
Computational infeasible	计算上不可行的
Computational security	计算上安全的
Conventional cryptography	传统密码学
Cryptanalysis	密码分析
Cryptogram	密码
Cryptographic system	密码系统
Cryptography	密码学
Deciphering	解密
Discrete exponential function	离散指数函数
Enciphering	加密
Eavesdropping	窃听
Finite field	有限域
IFF (Identification Friend or Foe)	敌我识别
Injection	注入
Insecure channel	不安全信道
Key	密钥
Key distribution	密钥分发
Key generator	密钥生成器
Keyspace	密钥空间
Known plaintext attack	已知明文攻击
Knapsack problem	背包问题
Logarithm	对数
Message authentication	消息认证
Multiple access cipher	多址密码
Noninvertible	不可逆的
NP complete	NP 完全的
One-time pad	一次一密
One-way authentication	单向认证
One-way compiler	单向编译器
One-way function	单向函数
Plaintext	明文
Privacy	保密，隐私
Public channel	公共信道
Public key cryptosystem	公钥密码系统
Public key distribution system	公钥分发系统

英文术语	中文翻译
Quasi secure cipher	拟安全密码
Quasi one-way function	拟单向函数
Receiver	接收者
Secure channel	安全信道
Signature	签名
Stream cipher	流密码
Teleprocessing	远程信息处理，远程处理
Threat	威胁
Transmitter	发送者
Trap door	陷门
Trap-door cipher	陷门密码
Trap-door one-way function	陷门单向函数
Unconditionally secure	无条件安全的
User authentication	用户认证