密码学新方向

WHITFIELD DIFFIE AND MARTIN E. HELLMAN,

翻译：李晓峰 (cy_lxf@163.com)[‡]

V1.0

2023 年 5 月 6 日

摘要

本文讨论了密码学现代发展的两个方面。远程处理的广泛应用促使开发新型密码系统，这些系统最大限度地减少了对安全密钥分发通道的需求，提供了等同于书面签名的功能。本文提出了解决这些当前未解决问题的方法。同时，本文也讨论了通信和计算理论开始提供解决长期存在的密码学问题的工具。

I 引言

我们今天站在密码学革命的边缘。廉价数字设备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提款机和计算机终端等商业应用。相应地，这些应用程序为新型密码系统的需求创造了条件，这种系统最大程度地减少了安全密钥分发通道的必要性，并提供了等同于书面签名的功能。与此同时，信息理论和计算机科学的理论进展表明，可能提供可证明安全的加密系统，这将把这门古老的艺术变成一门科学。

计算机控制的通信网络的发展为世界两端的人或计算机之间提供了轻松、廉价的联系方式，取代了大部分的邮件和许多短途通信旅行活动 (many excursions with telecommunications)。对于许多应用而言，这些联系必须安全可靠，不能被窃听和注入非法信息。然而，目前安全问题的解决在通信技

*译者目前为北京联合大学智慧城市学院信息安全老师。

†译文来自于经典文献翻译项目 https://gitee.com/uisu/InfSecClaT, 欢迎大家加入经典翻译项目，为更多的人能够获取这些经典文献所传递信息做一点贡献。

术的其他领域中依然相对滞后。当代的密码学无法满足要求，因为其使用会给系统用户带来如此严重的不便，以至于会消除远程处理的许多好处。

最著名的密码问题是隐私问题：防止未经授权从不安全信道上的通信中提取信息。然而，为了使用密码学来确保隐私，目前通信各方必须共享一个其他人不知道的密钥。这是通过一些安全通道（如私人快递或挂号信）提前发送密钥来完成的。私人谈话然，在商业中，两个素不相识的人之间是很常见的，这是不现实的。期望最初的业务联系被推迟足够长的时间，以便通过某种物理手段传输密钥。这种密钥分配问题所带来的成本和延迟是将商业通信转移到大型远程处理网络的主要障碍。

第三节提出了两种在公共（即不安全）信道上传输密钥信息而不损害系统安全性的方法。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 可以在不泄露解密密钥 D 的情况下公开。因此，网络的每个用户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能够以只有预期的接收者才能破译的方式向任何其他用户发送消息。因此，公钥密码系统是多路访问密码。因此，任何两个人之间都可以进行私人谈话，无论他们以前是否交流过。每一方向另一方发送消息，用接收方的公开加密密钥加密，并用自己的秘密解密密钥解密自己收到的消息。

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公开的。

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信道的需要。在这样的系统中，希望交换密钥的两个用户来回通信，直到他们得到共同的密钥。窃听该交换的第三方必须发现从偷听到的信息计算密钥在计算上是不可行的。第三节给出了公钥分配问题的一种可能的解决方案，Merkle[1]给出了不同形式的部分解。

第二个问题是身份验证，该问题可以通过密码解决，它阻碍了远程处理系统取代当代商业通信。在目前的商业中，合同的有效性是通过签字来保证的。签署的合同作为协议的法律证据，持有人可在必要时在法庭上出示。然而，使用签名需要传输和存储书面合同。为了有一个纯粹的数字替代这种纸质仪器，每个用户必须能够产生一个信息，其真实性可以由任何人检查。由于只有一个人可以发出消息，但许多人可以接收消息，因此这可以被视为广播密码。目前的电子认证技术不能满足这一需要。

第四节讨论了提供真实的、数字的、依赖电文的签名的问题。由于这里

提出的原因，我们将其称为单向身份验证问题。给出了一些部分解决方案，并说明了如何将任何公钥密码系统转换为单向认证系统。

第五节将考虑各种密码问题的相互关系，并介绍更困难的陷门问题。

在通信和计算产生了新的密码学问题的同时，它们的衍生 (their offspring)，信息论和计算理论已经开始为解决经典密码学中的重要问题提供工具。

寻找无法破解的密码是密码学研究中最古老的主题之一，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”(ont time pad) 被提出来，并被证明是牢不可破的 [2，pp。398-400]. 四分之一世纪后，信息论 [3] 为这一系统和相关系统的理论基础奠定了坚实的基础。“一次一密”需要极长的密钥，因此在大多数应用中都非常昂贵。

相反，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是计算困难的。这个问题属于计算复杂性和算法分析领域，这两个最近的学科研究解决计算问题的难度。使用这些理论的结果，在可预见的未来，有可能将安全性的证明扩展到更有用的系统类别。第六节探讨了这种可能性。

在论文继续阐述之前，我们先在下一节中介绍术语并定义威胁环境。

II 传统密码体系

密码学是对“数学”系统的研究，用于解决两种安全问题：隐私和认证。保密系统防止未经授权的各方从通过公共信道传输的消息中提取信息，从而向消息的发送者保证该消息仅由预期的接收者读取。认证系统可防止未经授权将消息注入公共信道，从而向消息的接收者保证其发送者的合法性。

如果信道的安全性不足以满足用户的需求，则该信道被视为公共信道。因此，诸如电话线之类的信道可能被一些用户认为是私有的，而被其他用户认为是公共的。任何信道都可能受到窃听或注入的威胁，或者两者兼而有之，具体取决于其使用情况。在电话通信中，注入的威胁是最重要的，因为被叫方无法确定正在呼叫哪个电话。窃听需要使用窃听器，在技术上更困难，在法律上也更危险。相比之下，在无线电领域，情况正好相反。窃听是被动的，不涉及法律风险，而注入会使非法发射器被发现和起诉。

将我们的问题分为隐私和认证，我们有时会进一步将认证细分为消息认证和用户认证，上面说的认证问题是消息认证，对于用户认证，系统的唯一

任务是验证个人是否是他所声称的。例如，必须验证出示信用卡的个人的身份，但没有他希望发送的消息。尽管用户身份验证中明显没有消息，但这两个问题在很大程度上是等价的。在用户认证中，有一个隐含的消息“我是用户 X”，而消息认证只是验证消息发送方的身份。然而，这两个子问题在威胁环境和其他方面的差异有时使区分它们变得容易。

图1说明了传统密码系统用于保密通信时的信息流动情况。有三方：发射机、接收机和窃听器。发送器生成要通过不安全信道传送到合法接收器的明文或未加密消息 P。为了防止窃听者获知 P，发射机对 P 进行可逆变换 S_K，以产生密文 (ciphertext) 或密码 (cryptgram)$C = S_K(P)$。密钥 K 通过安全通道在线传输到合法接收器，如图 1 中屏蔽路径所示。由于合法接收者知道 K，他可以通过 S_K^{-1} 操作来解密 C，以获得原始明文消息 $S_K^{-1}(C) = S_K^{-1}(S_K(P)) = P$。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，安全通道可能是每周快递，而不安全通道则是电话线。

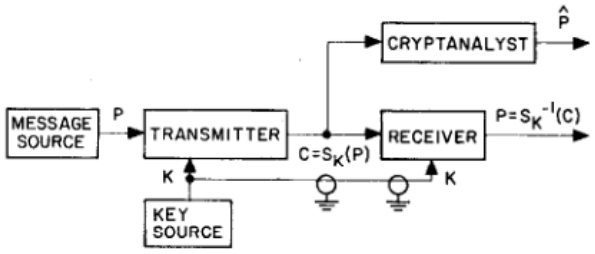

Fig. 1. Flow of information in conventional cryptographic system.

图 1: 传统加密系统中的信息流

一个密码系统是一个有可逆变换的单参数族

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

是从消息明文空间 $\{P\}$ 到密文空间 $\{C\}$ 的一个变换。参数 K 被称为密钥 (key)，是从有限集合 $\{K\}$ 中选择的，这个有限集合 $\{K\}$ 称为密钥空间，如果 $\{P\}$ 和 $\{C\}$ 相等，我们将其记为 $\{M\}$，当讨论某一个加密变换 S_K 时，我们有时将省略对系统的提及，而仅提及变换 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，但确保任何成功的密码分析操作都过于复杂而不经济。解决这个问题有两种方法。一种是由于密码分析的计算成本 (过高) 而安全，这种系统称为计算安全的 (computationally secure)，但会屈服于无限计算的攻击；而一个无论允许多

少计算量都能抵抗任何密码分析攻击的系统被称为无条件安全的 (unconditionally secure.)。在 [3] 和 [4] 中讨论了无条件安全系统，它属于信息论的一部分，称为香农理论，该理论涉及可通过无限计算获得的最优性能。

无条件安全源于一个密文存在多个有意义的解。例如，由英语文本产生的简单替换密码 XMD 可以表示明文消息：NOW、AND、THE 等。相反，计算安全的密文包含足够的信息来唯一地确定明文和密钥，它的安全性完全取决于计算它们的成本。

通常使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相同长度的密钥相结合。虽然这样的系统可证明是安全的，但所需的大量密钥使其对于大多数应用来说是不切实际的。除非另有说明，本文讨论计算安全系统，因为这些系统更普遍适用。当我们谈到需要开发可证明安全的密码系统时，我们排除了那些难以使用的密码系统，例如“一次一密”。相反，我们认为系统只使用几百位密钥，并且可以在少量数字电路或几百行软件中实现。

如果通过使用的内存量或运行时间来衡量的成本是有限的，但大得不可思议，则我们称该任务在计算上是不可行的 (computationally infeasible)。

就像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。流密码以小块（位或字符）的形式处理明文，通常产生位的伪随机序列，该序列以模 2 的形式添加到明文的比特位上。分组密码以纯组合的方式作用于大的文本块，以这样一种方式，输入块中的小变化产生结果输出中的大变化[1]。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是有价值的。

在认证系统中，使用密码学来保证消息的真实性。不仅必须防止干扰者将全新的、看似真实的消息注入到信道中，还必须防止他通过组合、复制过去的旧消息，仅仅重复已有的消息来制造看似真实的消息。一个旨在保障私密性的密码系统通常不会防止这种后一种的恶意行为。

[1]译者注：这就是密码学中的通常所说的变换具有的雪崩效应，密码中的雪崩效应是指，当密码中的一位或几位发生变化时，导致整个密码的值都会发生显著变化。也就是说，小的密码变化会引发大的密码值变化。这种现象是密码学中的一种重要特性，因为它可以确保密码的安全性。如果密码中的某一位或几位被修改，即使只有一小部分的变化，也会导致整个密码的值发生了巨大的变化，从而使攻击者难以推断密码的原始值。S 盒通常具有雪崩效应。S 盒是在 DES（数据加密标准）和 AES（高级加密标准）这样的对称加密算法中使用的一个重要的密码学组件。S 盒的作用是把一些输入位映射到一些不同的输出位，从而增强加密算法的安全性。在 S 盒的设计中，通常需要确保任何一个输入位的变化都能够产生尽可能多的输出位的变化。这样，当输入发生变化时，输出也会发生明显的变化，从而产生雪崩效应。这一特性可以使攻击者难以通过修改输入密码的几位来得出原始密码的值，从而大大增强了密码体系的安全性。

为了保证消息的真实性，需要添加信息，这些信息不仅是消息和密钥的函数，还包括日期和时间。例如，可以将日期和时间附加到每个消息并对整个序列进行加密。这可以确保只有拥有密钥的人才能生成解密后包含正确日期和时间的消息。然而，需要注意使用一个系统，在该系统中，密文中的小变化会导致明文大的变化。这种故意的误差扩散确保，如果有意注入通道上的噪声将一个消息如“删除文件 7”更改为另一个消息如“删除文件 8”，它也会破坏身份验证信息。消息将被拒绝认为是不真实的。

评估密码系统的充分性的第一步是对其所面临的威胁进行分类。用于隐私或认证的加密系统可能会受到以下威胁。

仅密文攻击 (ciphertext only attack) 是密码分析者仅拥有密文的密码分析攻击。

已知明文攻击 (known plaintext attack) 是密码分析攻击，其中密码分析者拥有大量相应的明文和密文。

选择明文攻击 (chosen plaintext attack) 是一种密码分析攻击，其中密码分析者可以提交他自己选择的无限数量的明文消息，并检查得到的密码。

在所有情况下，假设对手知道所使用的一般系统 $\{S_K\}$，因为该信息可以通过研究密码设备来获得。虽然密码学的许多用户试图对他们的设备保密，但许多商业应用不仅要求通用系统是公开的，而且要求它是标准的。

仅密文攻击在实践中经常发生。密码分析员仅使用所使用的语言的统计特性的知识（例如，在英语中，字母 E 出现的频率为 13%）和某些“可能”单词的知识（例如，字母可能以“Dear Sir:”开头）。它是系统所能承受的最弱的威胁，任何抵挡不住 (succumbs) 它的系统都被认为是完全不安全的。

一个安全系统应能够抵御已知明文攻击，使其用户不必为保守过去的消息而感到负担，或在解密之前对这些消息进行复述。这对于系统的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，以供以后公开披露。类似的情况在外交信函中也已经出现，这导致了许多被认为是安全的系统遭到破解。虽然已知明文攻击并非总是可行的，但其发生频率足以使未能抵御此类攻击的系统被认为不安全。

实践中很难实现选择明文攻击，但可以近似实现。例如，向竞争对手提交一个提案，可能会导致他将其加密后传输到总部。一个安全的密码系统应能够抵御选择明文攻击，以避免用户担心其对手在系统中执行消息注入攻

击。

为了证明系统是安全的，考虑更强大的密码分析威胁是适当的，因为这些不仅给出了密码系统工作环境的更真实的模型，而且使系统强度的评估更容易。许多系统使用仅密文攻击是困难的，但是在已知明文或者选择明文攻击下就立即被淘汰了。

从这些定义中可以看出，密码分析是一个系统识别问题。已知明文攻击和选择明文攻击分别对应被动和主动系统识别问题。与许多其他被认为是系统识别的学科（例如自动故障诊断）不同，密码学的目标是构建难以识别的系统，而不是易于识别的系统。

选择明文攻击通常被称为敌我识别攻击，这一术语起源于第二次世界大战后，密码“敌我识别”系统的发展。敌我识别系统使军用雷达能够自动区分友机和敌机。雷达向飞机发送时变询问，飞机接收该询问，在适当的密钥下对其进行加密，并将其发送回雷达。通过将该响应与正确加密的挑战版本进行比较，雷达可以识别友机。当飞机在敌方领土上空时，敌方密码分析员可以发送挑战并检查加密响应，以试图确定正在使用的认证密钥，从而对系统进行选择明文攻击。在实践中，这种威胁是通过限制挑战的形式来应对的，挑战不需要是不可预测的，而只需要是不重复的。

认证系统还面临着传统密码学无法解决的其他威胁，这些威胁需要求助于本文介绍的新思想和新技术。在多用户网络中，接收方通常是系统本身，因此接收方的密码表 (password tables) 和其他认证数据比发送方（个人用户）的密码表和其他认证数据更容易被窃取。如后面所示，一些用于防止这种威胁的技术也可以防止争议的威胁 (threat of dispute.), 即，消息可以被发送，但随后被发送方或接收方否认。或者，任何一方都可能声称发送了一条消息，而事实上根本没有发送。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的订单来掩盖未经授权的买卖，以谋取私利，或者客户发现该订单会造成损失, 从而否认他实际授权的订单。我们将介绍一些概念，这些概念允许接收者验证消息的真实性，但防止他生成认证消息，从而防止接收者的认证数据泄露威胁和争议威胁。

III 公钥密码体系

如图 1 所示，密码学已经成为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, 将安全性扩展到具有更高带宽或更小延

迟的其他信道。其效果是将密码学的使用限制在事先为密码安全做好准备的人之间的通信中。

为了发展大型、安全的电信系统，必须改变这一点。大量的用户 n, 导致更大数量，$(n^2-n)/2$，的签字密钥对，这些用户可能希望与所有其他人私下通信。假设先前不认识的一对用户将能够等待通过某种安全物理手段发送的密钥，或者可以预先安排所有 $(n^2-n)/2$ 对的密钥，这是不现实的。在另一篇论文 [5] 中，作者考虑了一种保守的方法，该方法不需要密码学本身的新发展，但这会降低安全性，带来不便，并将网络限制为与初始连接协议相关的星形配置。

我们提出，可以开发图 2 所示类型的系统，其中仅通过公共信道通信并且仅使用公开技术就可以创建两方安全连接。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。第一个功能更强大，有助于解决下一节中讨论的认证问题，而第二个则更接近于实现。

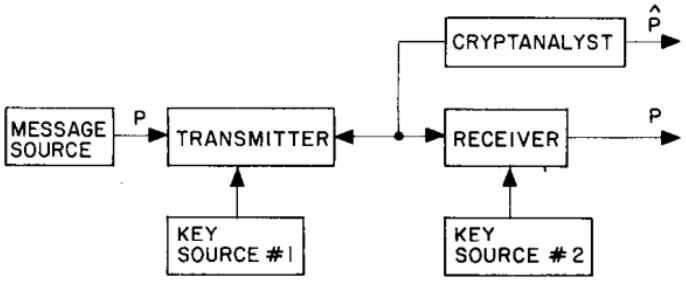

Fig. 2. Flow of information in public key system.

图 2: 公钥系统中的信息流

一个公钥密码系统 (public key cryptosystem) 是一对在有限消息空间 $\{M\}$ 上的算法族，$\{E_K\}_{K\in\{K\}}$ 和 $\{D_K\}_{K\in\{K\}}$，代表可逆变换，

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

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

并且满足：

- 对于每一个 $K \in \{K\}$,E_K 是 D_K 的逆；
- 对于每一个 $K \in \{K\}$ 和 $M \in \{M\}$，算法 E_K 和 D_K 是容易计算的；

- 对于几乎每一个 $K \in \{K\}$，等效于 D_K 的每个容易计算的算法, 从 E_K 推导出来这些算法在计算上不可行;
- 对于每一个 $K \in \{K\}$，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 可以公开而不损害其秘密解密密钥 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，这样，给定一族的成员，不可能找到另一族的相应成员。

第四个性质保证，当加密或解密变换不受约束时，有一种可行的方法来计算相应的逆变换对。在实践中，加密设备必须包含一个真正的随机数生成器（例如，有噪声的二极管）来生成 K，以及用于从其输出生成 $E_K - D_K$ 对的算法。

给定这样一个系统，密钥分配问题就大大简化了。每个用户在其终端生成一对逆变换，即 E 和 D。解密变换 D 必须保密，但不需要通过任何渠道进行通信。加密密钥 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被公开。然后，任何人都可以加密消息并将其发送给用户 Bob，但没有其他人可以破译为 Bob 提供的消息[2]。因此，公钥密码系统可以被视多用户共享密码 (multiple access ciphers.)。

保护加密密钥的公共文件不受未经授权的修改是至关重要的。由于文件的公共性质，这项任务变得更加容易。读取保护是不必要的，而且由于文件很少被修改，因此可以经济地使用精心设计的写入保护机制。

公钥密码系统的一个提示性的例子，尽管不幸的是没有用，是通过将明文乘以可逆的二进制 $n \times n$ 矩阵 E 来加密明文，明文表示为二进制 n 维向量 m。因此，密码等于 Em。设 $D = E^{-1}$，我们有 $m = DC$。因此，加密和解密都需要大约 n^2 次操作。然而，从 E 计算 D 涉及矩阵求逆，这是一个更困难的问题。并且至少在概念上，获得任意一对逆矩阵比对给定矩阵求逆更简单。从单位矩阵 I 开始，进行初等行、列运算，得到任意可逆矩阵 E。然后从 I 开始，以相反的顺序做这些相同的初等运算的逆运算，得到 $D = E^{-1}$。基本操作的序列可以很容易地从随机位串中确定。

不幸的是，矩阵求逆只需要 n^3 个运算。“密码分析”时间（即从 E 计算 D）与加密或解密时间的比率最大为 n，并且需要巨大的块大小才能获得 10^6 或更大的比率。此外，用于从 I 获得 E 的基本运算的知识似乎并不能大

[2]译者注：原文 Anyone can then encrypt messages and send them to the user, but no one else can decipher messages intended for him. 根据上下文意思“the user”和”him” 是指同一人，为了便于准确翻译和理解，我们称其为 Bob。

大减少计算 D 的时间。并且，由于在二进制算术中没有舍入误差，因此在矩阵求逆中数值稳定性并不重要。尽管缺乏实用性，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。

一种更实用的方法是找到一对易于计算的逆算法 E 和 D，使得从 E 中推导出 D 很困难，这利用了用低级语言分析程序的困难。任何试图确定别人的机器语言程序实现了什么操作的人，都知道 E 本身（即 E 所做的事情），但很难从 E 的算法中推导出来。如果通过添加不必要的变量和语句使程序有意混淆，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，才能防止从输入输出对中识别出它。

从本质上讲，所需要的是一个单向编译程序：它把用高级语言编写的容易理解的程序翻译成用某种机器语言编写的难以理解的程序。编译器是单向的，因为它必须能够进行编译，但不能反向编译。由于在该应用中，程序大小和运行时间的效率不是至关重要的，因此如果机器语言的结构可以被优化以帮助混淆，则这样的编译器是可能的。

Merkle [1] 独立地研究了在不安全信道上分配密钥的问题。该方法不同于上面建议的公钥密码系统的方法，并且将被称为公钥分发系统 (public key distribution system)。目标是让两个用户 A 和 B 通过不安全的信道安全地交换密钥。然后，该密钥由正常密码系统中的两个用户用于加密和解密。Merkle 提出了一种解决方案，其密码分析成本增长为 n^2，其中 n 是合法用户的成本。不幸的是，系统的合法用户的成本在传输时间上与在计算上一样多，因为 Merkle 的协议需要在决定一个密钥之前传输 n 个潜在密钥。Merkle 指出，这种高传输开销妨碍了该系统在实践中非常有用。如果在建立协议的开销上设置 1 兆比特的限制，则该技术可以实现大约 10000 比 1 的成本比，这对于大多数应用来说太小了。如果廉价的高带宽数据链路变得可用，则可以实现百万分之一或更大的比率，并且该系统将具有相当大的实用价值。

我们现在提出一种新的公钥分配系统，它具有几个优点。首先，它只需要交换一把“钥匙”。其次，在合法用户的努力中，密码分析的努力似乎呈指数增长。第三，它的使用可以绑定到用户信息的公共文件，该公共文件用于向用户 B 认证用户 A，反之亦然。通过使公共文件本质上成为只读存储器，一次个人出现允许用户向许多用户多次认证其身份。Merkle 的技术要求 A 和 B 通过其他手段验证对方的身份。

新技术利用了在具有素数 q 个元素的有限域 GF(q) 上计算对数明显是

困难的这一结论。设

$$Y = \alpha^X \pmod{q} \quad , for\ 1 \leq X \leq q-1 \tag{4}$$

此处 α 是 GF(q) 中固定的素元素，X 是以 α 为基 Y 的对数，模 q：

$$X = log_\alpha Y \pmod{q} \quad , for\ 1 \leq Y \leq q-1 \tag{5}$$

从 X 计算 Y 是容易的，进行 $2 \times log_2 q$ 次乘法运算 [6,pp.398-422]。例如，X=18,

$$Y = \alpha^{18} = (((\alpha^2)^2)^2)^2 \times \alpha^2 \tag{6}$$

另一方面，从 Y 计算 X 很困难，对于一些仔细选择的 q，在使用最好的算法情况下 [7,pp.9,575-576,[8]]，需要 $q^{1/2}$ 个顺序运算。

我们技术的安全性关键取决于计算模 q 对数的困难程度，如果有一种算法其复杂性随 $log_2 q$ 增加，那么我们的系统就被破解了。虽然问题陈述的简单性可能会导致出现这样简单的算法，但它也可能会证明问题的困难性。目前我们假定计算模 q 对数的最佳已知算法确实接近于最优的，因此对于经过适当选择的 q，$q^{1/2}$ 是该问题复杂度的好度量标准。

每个用户产生一个独立随机数 X_i, 均匀地从整数集合 $\{1, 2, \ldots, q-1\}$ 中选择，每一个用于保持 X_i 的机密，但是将 Y_i 与自己的名字和地址一起放在公共文件

$$Y_i = \alpha^{X_i} \pmod{q} \tag{7}$$

当用户 i 和 j 准备私密通信时，他们使用

$$K_{i,j} = \alpha^{X_i X_j} \pmod{q} \tag{8}$$

作为他们的密钥，用户 i 通过从公共文件中获得 Y_j，从而获得 K_{ij}

$$K_{ij} = Y_j^{X_i} \pmod{q} \tag{9}$$

$$= (\alpha^{X_j})^{X_i} \pmod{q} \tag{10}$$

$$= \alpha^{X_j X_i} = \alpha^{X_i X_j} \pmod{q} \tag{11}$$

用户 j 用相似的方式获得 K_{ij}

$$K_{ij} = Y_i^{X_j} \pmod{q} \tag{12}$$

其他用户必须从 Y_i 和 Y_j 计算 K_{ij}，例如，计算

$$K_{ij} = Y_i^{(log_\alpha Y_j)} \pmod{q} \tag{13}$$

从而我们可以看到，如果模 q 的对数很容易计算，那么系统就可以破解。虽然我们目前没有证明相反的结论（即，如果计算模 q 的对数是困难，则系统是安全的），但我们也没有发现任何不先获得 X_i 或 X_j 即可从 Y_i 和 Y_j 计算出 K_{ij} 的方法。

如果 q 是略小于 2^b 的素数，则所有量都可表示为 b 比特数。然后，取幂最多需要 2b 次模 q 乘法，而假设取对数需要 $q^{1/2} = 2^{b/2}$ 次运算。因此，密码分析工作相对于合法工作呈指数增长。如果 $b = 200$，则从 X_i 计算 Y_i 或从 Y_i 和 X_j 计算 K_{ij} 最多需要 400 次乘法，而取模 q 的对数需要 2^{100} 或大约 10^{30} 次运算。

IV 单向认证

与密钥分发问题相比，认证问题可能是普遍采用电子通信进行商业交易的更严重障碍。身份验证是任何涉及合同和计费的系统的核心。没有它，企业就无法运转。目前的电子认证系统不能满足对纯数字的、不可伪造的、依赖电文的签名的需要。它们提供了防止第三方伪造的保护，但不能防止发送方和接收方之间的争议。

为了开发一种能够用某种纯粹的电子通信形式代替当前书面合同的系统，我们必须发现一种具有与书面签名相同属性的数字现象。任何人都必须很容易地将签名识别为真实的，但合法签名人以外的任何人都不可能制作它。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，因此真正的数字签名必须在不知道的情况下被识别 (Since any digital signal can be copied precisely, a true digit,al signature must be recognizable without being known.)。

考虑多用户计算机系统中的“登录”问题。在设置帐户时，用户会选择一个密码，该密码会输入到系统的密码目录中。每次登录时，都会再次要求用户提供密码。通过对所有其他用户保密此密码，可以防止伪造登录。然而，这使得保护密码目录的安全性变得至关重要，因为它所包含的信息将允许完美地模拟任何用户。如果系统操作员具有访问目录的合法理由，则该问题会变得更加复杂。允许这种合法访问，但阻止所有其他访问，几乎是不可能的。

这导致一个明显不可能的需求，要求新的登录程序能够在不实际知道密码的情况下判断密码的真实性。虽然在逻辑上似乎是不可能的，但这一建

议很容易得到满足。当用户首次输入其密码 PW 时，计算机自动且透明地计算函数 $f(PW)$, 并将其存储在密码目录中, 而不是将 PW 存储起来。在每次连续登录时，计算机计算 $f(X)$，其中 X 是提供的密码，并将 $f(X)$ 与存储的 $f(PW)$ 进行比较，当且仅当它们相等时，用户才被认为是可信的。由于函数 f 必须在每次登录时计算一次，因此其计算时间必须很短。一百万条指令（按二百万条指令成本约为 0.10 美元）似乎是这一计算的合理限制。然而，如果我们能够确保 f^{-1} 的计算需要 10^{30} 或更多的指令，则破坏系统以获得密码目录的人实际上不能从 $f(PW)$ 获得 PW，因此不能执行未经授权的登录。请注意，登录程序不接受 $f(PW)$ 作为密码，因为它将自动计算 $f(f(PW))$，该值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，因此它不是使 f^{-1} 的计算变得困难的未知函数。这样的函数称为单向函数，最早由 R.M.Needham[9，p.91] 用于登录过程。在最近的两篇论文 [10]、[11] 中也讨论了它们，这两篇论文对单向函数的设计提出了有趣的方法。

更准确地说，函数 f 是单向函数，如果，对于 f 定义域中的变量 x，很容易计算出相应的值 $f(x)$，但是，对于 f 值域中的几乎所有 y，对于任何合适的参数 x，求解方程 $y = f(x)$ 在计算上是不可行的。

值得注意的是，从计算的角度来看，我们定义的函数是不可逆的，但其不可逆性与数学中通常遇到的不可逆性完全不同。当点 y 的逆函数不唯一时，函数 f 通常称为“不可逆”(例如，存在不同的点 x_1 和 x_2，使得 $f(x_1) = y = f(x_2)$)。我们强调，这不是所需要的那种反演困难。更确切地说，在给定 y 值和 f 的知识的情况下，计算具有 $f(x) = y$ 性质的任何 x 肯定是极其困难的。事实上，如果 f 在通常意义上是不可逆的，它可能会使寻找逆像的任务变得更容易。在极端情况下，如果对于域中的所有 x，$f(x) = y_0$，那么 f 的范围是 $\{y_0\}$，并且我们可以将任何 x 取为 $f^{-1}(y_0)$。因此，f 不能太退化是必要的。小程度的退化是可以容忍的，并且正如后面所讨论的，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。找到多项式方程 $p(x) = y$ 的根 x_0 比在 $x = x_0$ 处计算多项式 $p(x)$ 要难得多。Purdy[11] 建议在有限域上使用非常高次数的稀疏多项式，其似乎具有非常高的解与求值时间的比率[3]。第 VI 节详细讨论了单向函数的理论基础。如第 V 节所示，单向函数在实践中很容易设计。

[3]译者注：这句话的意思就是需要很长时间来计算。

单向函数登录协议只能解决多用户系统中出现的部分问题。它可以在不使用时防止系统身份验证数据泄露，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对窃听的保护，而对争议威胁的保护也不存在。

公钥密码系统可以用来产生一个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，他会用私钥运算 $D_A(M)$ 发送给 B。当用户 B 收到它时，他可以阅读它，并通过使用用户 A 的公钥进行解密操作 E_A, 确保其真实性。B 还保存 $D_A(M)$ 作为消息来自 A 的证明。任何人都可以通过在 $D_A(M)$ 上运行公共已知的 E_A 操作来恢复 M, 从而检查是否是 A 的声称。由于只有 A 可以生成消息 $D_A(M)$，因此公钥密码系统自然衍生出单向认证方案。

马萨诸塞州计算机协会的莱斯利 • 兰波特（Leslie Lamport）向作者建议了单向消息身份验证的部分解决方案。该技术使用单向函数 f 将 k 维二元空间映射到其自身，其中 k 的数量级为 100。如果发射机希望发送 N 比特消息，则他生成 2N 个随机选择的 k 维二进制向量 $x_1, X_1, x_2, X_2, \ldots, x_N, X_N$，并对其保密。接收器被给予 f 下的相应的像，即 $y_1, Y_1, y_2, Y_2, \ldots, y_N, Y_N$。稍后，当要发送消息 $m = (m_1, m_2, \ldots, m_N)$ 时，发射机根据 $m1 = 0$ 还是 1 来发送 x_1 或 X_1。他根据 $m_2 = 0$ 还是 1 来发送 x_2 或 X_2，等等。接收机用 f 对第一个接收到的块进行操作，并查看它是否产生 y_1 或 Y_1 作为其像，从而知道它是 x_1 还是 X_1，以及 $m_1 = 0$ 还是 1。以类似的方式，接收机能够确定 $m_2, m_3, \ldots, m_N$。但是接收器不能伪造 M 的哪怕一个比特的变化。

这只是部分解决方案，因为需要大约 100 倍的数据扩展。然而，当 N 大约是兆比特或更大时，有一种修改可以消除扩展问题。设 g 是从二进制 N 空间到二进制 N 空间的单向映射，其中 N 大约为 50。取 N 位消息 m，并用 g 对其进行运算，以获得 n 位向量 m'。然后使用前面的方案发送 m'。如果 $N = 10^6$，$n = 50$，$k = 100$，则向消息添加 $kn = 5000$ 个认证位。因此，在传输期间仅需要 5% 的数据扩展（或者如果包括 $y_1, Y_1, \ldots, y_N, Y_N$ 的初始交换，则为 15%）。即使存在大量具有相同认证序列的其他消息（平均 2^{N-n}），g 的单向性也使得它们在计算上不可能被找到并因此被伪造。实际上，g 必须比正常的单向函数强一些，因为对手不仅有 m'，而且还有它的一个逆像 m。即使给定 m，也很难找到 m 的另一个逆像 m'。找到这样的函数似乎并不困难（见第 V 节）。

对于单向用户身份验证问题，还有另一种部分解决方案。用户生成密码 X，并对其保密。他给出了系统 $f^T(X)$，其中 f 是单向函数。在时间 t，适

当的验证器是 $f^{T-t}(X)$，其可以由系统通过应用 $f^t(X)$ 来检查。由于 f 的单向性，过去的响应对形成新的响应没有价值。这种解决方案的问题在于，对于合法的登录，它可能需要相当多的计算（虽然比伪造要少很多个数量级）。例如，如果每秒增加一次 t，而系统必须在每个密码上工作一个月，那么 T=260 万次。然后，用户和系统必须平均迭代 f 130 万次才能登录。虽然这个问题不是不可克服的，但显然限制了这种技术的使用。如果能够找到一种简单的方法来计算 $f^{2\uparrow n}$，对于 $n = 1, 2, \ldots$，类似于 $X^8 = ((X^2)^2)^2$，那么就可以解决这个问题。因为 T-t 和 t 的二进制分解将允许快速计算出 f^{T-t} 和 f^t。然而，快速计算 f^n 可能排除了 f 是单向函数的可能性。

V 问题的相互关系和陷门

在本节中，我们将展示到目前为止提出的一些密码问题可以简化为其他问题，从而根据难度定义一个不精确的排序 (a loose ordering)。我们还介绍了更困难的陷门问题。

在第二节中，我们展示了旨在保护隐私的密码系统也可以用于提供针对第三方伪造的认证服务。这样的系统也可以用于创建其他密码学目标。

对于已知明文攻击是安全的密码系统可以用来产生单向函数。

如图3所示，密码系统 $\{S_K : \{P\} \to \{C\}_{K\in\{K\}}\}$ 对于已知明文攻击是安全的，取 $P = P_0$，考虑以下映射

$$f : \{K\} \to \{C\} \tag{14}$$

定义

$$f(x) = S_X(P_0) \tag{15}$$

这个函数是单向的，因为给定 $f(x)$ 求解 x 等价于密码分析问题，也就是已知一个明文密文对要去找到密钥。f 是公开信息，等同于 $\{S_K\}$j 和 P_0 公开信息。

虽然此结果的逆向并不一定成立，但是在寻找单向函数时找到的函数可能会产生一个良好的加密系统。这实际上就发生在第三节 [8] 中讨论的离散指数函数中。

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（称为密钥流）与以二进制形式表示的消息进行模 2 加法，以仿效一次一密。密钥用作确定伪随机密钥流序列的“种子”。因此已

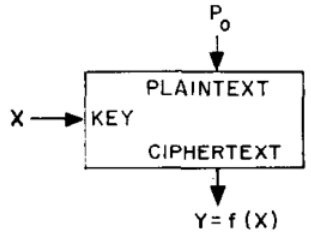

Fig. 3. Secure cryptosystem used as one-way function.

图 3: 用作单向函数的安全加密系统

知明文攻击归结为从密钥流中确定密钥的问题。为了保证系统安全，从密钥流计算密钥必须是计算上的不可行的。同时，为了使用系统，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就是一个单向函数的定义。

将任一类型的加密系统用作单向函数会遇到一个小问题。如前所述，如果函数 f 不是唯一可逆的，则不需要（也不可能）找到实际使用的 X 的实际值。任何具有相同像的 X 都足够了。而且，尽管加密系统中的每个映射 S_K 都必须是双射的，但是上面定义的密钥到密文的函数 f 没有这样的限制。的确，保证一个加密系统具有这种属性似乎非常困难。在一个良好的加密系统中，映射 f 可以预期具有随机选择映射的特征（即 $f(X_i)$ 在所有可能的 Y 中均匀选择，并且连续的选择是独立的）。在这种情况下，如果 X 被均匀选择，并且有相同数量的密钥和消息（X 和 Y），那么结果 Y 具有 $k+1$ 个逆元素的概率大约为 $e^{-}1/k!$，其中 $k = 0, 1, 2, 3...$。这是一个平均值 $\lambda = 1$ 的泊松分布，向右移动 1 个单位。在这种情况下，期望的逆的数目仅为 2。虽然 f 可以更加退化，但是一个良好的加密系统不会退化太多，否则密钥就没有被很好地使用。在最坏的情况下，如果对于某个 Y_0 有 $f(X) = Y_0$，我们有 $S_K(P_0) = C_0$，P_0 加密不会根本依赖于密钥！

虽然我们通常对定义域和值域大小相当的函数感兴趣，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这样的函数。

Evans 等人 [10] 对从分组密码构造单向函数的问题有不同的方法。他

们没有选择固定的 P0 作为输入，而是使用函数

$$f(X) = S_X(X). \tag{16}$$

这是一种有吸引力的方法，因为这种形式的方程通常难以求解，即使当族 S 相对简单时也是如此。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单向性之间的等价性。

另一种关系已在第四节中说明。

公钥密码系统可用于生成单向认证系统。

相反的情况似乎并不成立，这使得公钥密码系统的构造成为比单向认证更困难的问题。类似地，公钥密码系统可以用作公钥分配系统，但不能相反。

由于公钥加密系统中使用 E 和 D 的一般系统必须是公开的，因此指定 E 指定了一个完整的算法，将输入消息转换为输出加密文。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，因为存在简单计算逆的函数。但是，在给定正向函数的算法的情况下，计算简单的逆确实是计算上不可行的。只有通过某些陷门信息（例如，产生 E-D 对的随机位串）的知识，才可以轻松找到易于计算的逆。

在前面的段落中，已经看到了以陷门单向函数的形式出现的陷门，但还存在其他变化。陷门密码是一种强烈抵制密码分析的密码，该密码由不拥有在密码设计中使用的陷门信息的任何人进行分析。这使得设计者在将系统出售给客户后可以破坏系统，但却错误地维护了他作为安全系统建设者的声誉。需要注意的是，并不是更聪明或更懂密码学，才能让设计者做别人做不到的事情。如果他失去了陷门信息，他不会比其他人做得更好。这种情况与组合锁完全类似。任何知道这种组合的人都可以在几秒钟内完成，即使是熟练的锁匠也需要数小时才能完成。然而，如果他忘记了组合，他就没有优势了。

陷门密码系统可以用来产生公钥分配系统。

为了使 A 和 B 建立一个共同的私钥，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，但对陷门信息保密，使用该明文-密文对来求解密钥。A 和 B 现在有一把共同的钥匙。

目前几乎没有证据表明陷门密码的存在。然而，它们是一种明显的可能性，并且在接受来自可能对手的密码系统时应该记住 [12]。

按照定义，我们将要求一个陷门问题是陷门计算是可行的。这为第三种实体留下了空间，我们将使用前缀“准”。例如，准单向函数并不是单向函数，因为易于计算的逆函数存在。但是，对于设计者来说，找到易于计算的逆是计算上不可行的。因此，准单向函数可以用来替代单向函数，而基本上不会损失安全性。

将陷阱门信息从陷阱单向函数中去掉，将其变成准单向函数，但也可能存在不能用这种方式获取的单向函数。

准单向函数是否被排除在单向函数的类别之外完全是一个定义问题。我们可以讨论宽义或严格意义上的单向函数。

同样地，准安全密码是一种密码，它将成功抵抗密码分析，即使是由自己的设计者进行的分析，但仍然存在一种计算上高效的密码分析算法（当然，找到这种算法在计算上是不可行的）。同样，从实际的角度来看，安全密码和准安全密码之间基本上没有什么区别。

我们已经看到了公钥加密系统暗示着陷门单向函数的存在。然而反过来并不一定成立。对于一个陷门单向函数被用作公钥加密系统，它必须是可逆的（即具备独特的逆元素）。

VI 计算复杂度

密码学与所有其他领域的不同之处在于，它的要求似乎很容易得到满足。简单的转换将把清晰的文本转换为明显无意义的混乱。批评家声称也许可以通过密码分析恢复消息的意思，但如果他想证明自己的观点是正确的，那么他将面临一场艰巨证明。然而，经验表明，很少有系统能够抵御熟练的密码分析员的协同攻击，许多本应安全的系统随后被攻破。

因此，判断新系统的价值一直是密码学家关注的中心问题。在十六世纪和十七世纪期间，数学论证经常被用来论证密码方法的强度，通常依赖于显示可能的密钥的天文数字的计数方法。虽然这个问题很难用这种简单的方法来解决，但即使是著名的代数学家卡尔达诺 (Cardano) 也掉进了这个陷阱 [2,p.145]. 随着其强度被如此论证的系统被反复破坏，为系统的安全性给出数学证明的概念声名狼借，并被通过密码分析攻击的分析方法所取代。

然而，在本世纪，钟摆开始摆回另一个方向。在一篇与信息论诞生密切相关的论文中，Shannon[3] 指出，自二十年代后期开始使用的一次一密系统提供了“完美保密”（一种无条件安全的形式）。Shannon 研究的可证明安全

系统要么依赖于使用长度随消息长度线性增长的密钥，要么依赖于完美的源编码，但对于大多数用途来说这些都无法实用。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，因为公开信息总是在有限集合的成员中唯一确定秘密信息。因此，在无限计算的情况下，该问题可以通过直接搜索来解决。

在过去的十年里，两个密切相关的学科兴起，它们致力于研究计算的代价：计算复杂性理论和算法分析。前者将已知的计算问题按难度分为几大类，而后者则专注于寻找更好的算法并研究它们所消耗的资源。在简短地介绍了复杂性理论之后，我们将考察它在密码学中的应用，特别是对单向函数的分析。

一个函数被称为属于 P 类复杂度 (多项式复杂度)，如果它可以由确定性的图灵机在一个时间内计算，该时间由其输入长度的某个多项式函数限定。有人可能会认为这是一类容易计算的函数，但更准确地说，不在这一类中的函数至少对于某些输入来说一定很难计算。我们知道这些问题就不是 P 类问题 [13,pp.405-425] .

工程中出现的许多问题不能用任何已知的技术在多项式时间内解决，除非它们在具有无限并行度的计算机上运行。这些问题可能属于也可能不属于 P 类，但属于在“非确定性”计算机（即具有无限并行度的计算机）上可在多项式时间内解决的问题的 NP 类（对于非确定性，多项式）。显然，NP 类包括 P 类，并且复杂性理论中的一个重大公开问题是 NP 类是否严格地比 P 类更大。

在已知在 NP 时间内可解但未知在 P 时间内可解的问题中，有游商问题 (traveling salesman problem,)、命题演算的可满足性问题 (satisfiability problem for propositional calculus,)、背包问题 (knapsack problem)、图着色问题 (graph coloring problem,) 以及许多调度和最小化问题 [13,pp.363-404][14]. 我们看到，并不是缺乏兴趣或努力, 而阻碍了人们在 P 时间内找到这些问题的解决方案。因此，人们强烈认为，这些问题中至少有一个不属于 P 类，因此 NP 类严格地更大。

Karp 已经确定了 NP 问题的一个子类，称为 NP 完全，其性质是如果它们中的任何一个在 P 中，那么所有的 NP 问题都在 P 中。Karp 列出了 21 个 NP 完全的问题，包括上面提到的所有问题 [14]。

虽然 NP 完全问题显示了密码应用的前景，但目前对其难度的理解仅包括最坏情况分析。出于加密目的，必须考虑典型的计算成本。然而，如果

我们用平均或典型的计算时间代替最坏情况的计算时间作为我们的复杂性度量，那么目前对 NP 完全问题之间的等价性的证明就不再有效。这表明几个有趣的研究课题。熟悉集成和典型性概念的信息论家在其中显然扮演着重要的角色。

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以在 P 时间内完成的系统的密码分析难度不可能大于 NP。

要了解这一点，请注意，任何密码分析问题都可以通过从有限集合中找到密钥、逆像等来解决。不确定地选择密钥，并在多项式时间内验证它是否正确。如果有 M 个可能的密钥可供选择，则必须采用 M 重并行。例如，在已知的明文攻击中，在每个密钥下同时加密明文，并将其与密文进行比较。因为，通过假设，加密仅花费 P 时间，所以密码分析仅花费 NP 时间。

我们还观察到一般的密码分析问题是 NP 完全的。这源于我们对密码问题定义的广度。接下来将讨论具有 NP 完全逆的单向函数。

通过检查 NP 完全问题是否适应密码使用的方式，我们可以直接从 NP 复杂性理论中获得加密算法，特别地，有一个称为背包问题的 NP 完全问题，它可以很容易地构造一个单向函数。

设 $y = f(x) = a \cdot x$,此处 a 是一个已知有 n 个整数的向量 $(a_1, a_2, \ldots, a_n)$,x 是一个二进制 n 维向量，计算 y 是简单的，最多计算 n 个整数的加，但是求 f 的逆的问题是已知的背包问题，需要找到 $\{a_i\}$ 的子集，此子集元素和为 y。

所有 2^n 个子集的穷举搜索呈指数增长，并且对于 n 大于 100 左右在计算上是不可行的。然而，在选择问题的参数时必须小心，以确保不可能走捷径。例如，如果 $n = 100$ 并且每个 a_i 是 32 位长，则 y 是至多 39 位长，并且 f 是高度退化的；平均只需要 2^38 就可以找到解决方案。更简单地说，如果 $a_i = 2^{i-1}$，那么对 f 求逆等价于求 y 的二进制分解。

这个例子既证明了当代复杂性理论的巨大前景，也证明了其相当大的缺陷。理论只是告诉我们，在最坏的情况下，背包问题可能是困难的。对于某些特定数组，则不是一个困难问题。然而，似乎从 $\{0, 1, 2, \ldots 2^{n-1}\}$ 中均匀地选择 a_i 会导致一个困难问题，当 $n \to \infty$ 时其概率为 1。

在算法分析中，另一个潜在的单向函数是取模 q 指数函数，它在加州斯坦福大学的 John Gill 教授的建议下引起了作者的兴趣。该函数的单向性已在第 III 节中讨论过。

VII 历史背景/历史观点

虽然本文中提出的公钥系统和单向认证系统起初似乎没有受到过去密码学发展的推动，但可以将其视为数百年前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，人们对什么是保密的感到困惑。密码系统，如凯撒密码（其中每个字母都被后面的第 3 个字母替换，因此 A 替换为 D，B 替换为 E，等等）的安全性依赖于保持整个加密过程的机密性。电报发明后 [2,p191]，通用系统和特定密钥之间的区别是，允许通用系统被破坏，例如通过盗窃密码设备，而不会破坏用新密钥加密的未来消息。这一原则是由 Kerchoffs 提出的 [2,p.235], 他在 1881 年写道，密码系统的泄露不应给通信者带来不便。大约在 1960 年，密码系统投入使用，这些系统被认为足够强大，可以抵抗已知的明文密码分析攻击，从而消除了对旧消息保密的负担。每一项发展都减少了该系统中必须保护公众不知情的部分，消除了在提交外交文书之前转述这些冗长的权宜之计。公钥系统是这种降低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动或使用简单的类似滑尺的设备进行的计算。第一次世界大战刚结束后的一段时期，出现了一种革命趋势，这种趋势现在正在取得成果。为加密而开发专用的机器。然而，在通用数字硬件开发之前，密码学仅限于可以用简单的机电系统执行的操作。数字计算机的发展使其摆脱了齿轮计算的限制，并允许根据纯粹的密码标准寻找更好的加密方法。

通过数学证明来证明密码系统的可靠性的无数尝试的失败, 开启了上个世纪由 Kerchoffs [2,p.234] 提出的密码分析攻击的验证范式。尽管已经开发了一些通用规则来帮助设计者避免明显的弱点，但最终的测试是由熟练的密码分析员在最有利的条件下对系统进行攻击（例如，选择明文攻击）。计算机的发展首次导致了算法的数学理论，该理论可以开始处理估计破译密码系统的计算难度的难题。因此，数学证明的地位可能会回到原点，并被重新确立为最好的证明方法。

在密码学的历史上，我们注意到的最后一个特征是业余密码学家和专业密码学家之间的划分。密码分析的技能一直在很大程度上依赖于专业人员，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 (Thomas Jefferson) 是一位业余密码学家，他发明了一种系统，该系统在第二次世界大战期间仍在使用 [2,pp.192-195]，而二十世纪最著名的密码系统转子机是由四个不同的人同时发明的，他们都是业余爱好

者 [2,pp.415,420,422-424]。我们希望这将激励其他人在这个迷人的领域工作，在这个领域，由于最近几乎完全的政府垄断，参与受到了阻碍。

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. Theorv.

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

l0. 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, “Cryptanalysis 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. 855104.