**密码学的新方向**

*特邀论文*

WHITFIELD DIFFIE AND MARTIN E. HELLMAN,IEEE会员

摘要：本文考察了两种当代密码学的发展。远程处理的广泛应用引起了对新型密码系统的需求，该系统最大限度地减少了对安全密钥分发通道的需求，并提供了书面签名的等价物。本文提出了解决这些目前尚未解决的问题的方法。它还讨论了通信和计算理论如何开始为解决长期存在的密码问题提供工具。

1. 介绍

我们今天站在一场革命的边缘。密码学。廉价数码的发展

W

硬件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低到可用于远程自动提款机和计算机终端等商业应用的水平。反过来，这样的应用产生了对新型密码系统的需求，该系统最大限度地减少了安全密钥分发通道的必要性，并提供了书面签名的等价物。与此同时，信息论和计算机科学的理论发展表明，有希望提供可证明安全的密码系统，将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促进了TJ（即世界）两端的人或计算机之间的轻松和廉价的联系，用电信取代了大多数邮件和许多短途旅行。对于许多应用程序，必须确保这些联系人的安全，以防止窃听和非法消息的注入。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。当代的密码术不能满足这些要求，因为它的使用会给系统用户带来严重的不便，以至于消除了远程处理的许多好处。

Manus手稿于1976年6月3日收到。这项工作得到了美国国家科学基金会（NSF）ENG 10173拨款的部分支持。1975年6月23-25日在马萨诸塞州莱诺克斯举行的IEEE信息论研讨会和1976年6月21-24日在瑞典龙内比举行的IEEE信息论国际研讨会上介绍了这项工作的部分内容。

W.Diffie就职于加州斯坦福大学电气工程系和加州斯坦福人工智能实验室（94305）。 . . .

M.E.Hellman就职于斯坦福大学电气工程系，斯坦福，CA 94305。

最著名的密码问题是优先级问题：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。然而，两个事先不认识的人之间的私下交谈在商业中是常见的，并且期望最初的商业接触被推迟足够长的时间以通过某种物理手段传输密钥是不现实的。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10100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。

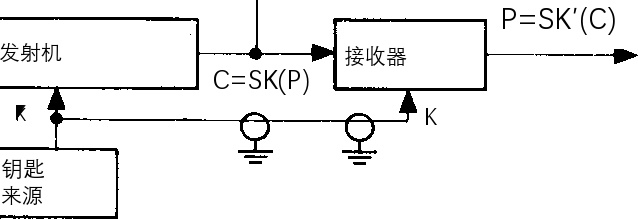
第二个问题，可以用密码解决，它阻碍了取代当代商业-

通过远程处理系统进行的NESS通信是一种认证。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。无论如何，签名的使用需要书面合同的传输和存储。为了有一个纯粹的数字替代

消息P

来源

"p



在这种纸质工具中，每个用户都必须能够生成一条消息，其真实性可以由任何人检查，但不能由其他任何人（甚至是收件人）生成。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求。

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。

在通信和计算引发新的密码学问题的同时，它们的后代——信息论和计算理论也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，“一次性垫”是在通风，并显示是牢不可破的[2，pp。398-400].四分之一个世纪后，信息理论[3]为这一系统和相关系统的理论基础奠定了坚实的基础。一次性键盘需要极长的按键，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的计算困难。这个问题属于计算复杂性和算法分析的范畴，这两个最近的学科研究了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。

在继续进行新的开发之前，我们将在下一节中介绍术语并定义威胁环境。

1. 传统密码学

密码学是对解决两种安全问题的“数学”系统的研究：隐私和认证。保密系统防止未经授权方从消息中提取信息。

图1.传统密码系统中的信息流。

在公共信道上传输，从而向报文的发送方保证它只被预期的接收方读取。身份验证系统防止未经授权的人-

.将消息注入到公共信道中，以确保消息的接收方具有其发送方的合法性。

如果信道的安全性不能满足其用户的需求，则该信道被认为是公共的。因此，诸如电话线的信道可能被一些用户认为是私有的，而被另一些用户认为是公共的。任何信道都可能受到窃听或注入或两者的威胁，这取决于其用途。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哪个电话正在呼叫。需要使用窃听器的窃听在技术上更加困难，在法律上更加危险。相比之下，在广播中，情况是相反的。窃听是被动的，不涉及法律风险，而注入则使非法发送者暴露于发现和起诉之下。

在将我们的问题划分为隐私和身份验证之后，我们有时会将身份验证进一步细分为消息身份验证（这是上面定义的问题）和用户身份验证（其中系统的唯一任务是验证个人是否是他所声称的那个人）。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。尽管在用户身份验证中明显缺少消息，但这两个问题在很大程度上是等价的。在用户身份验证中，有一条隐含的消息“我是用户X ”，而消息身份验证只是验证消息发送方的身份。然而，这两个子问题的威胁环境和其他方面的差异有时使得区分它们很方便。

图图1示出了用于通信保密的常规密码系统中的信息流。有三方：发送方、接收方和窃听者。发射机生成要通过不安全信道传送到合法接收机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SK，以产生密文或密码C=SK（P）。密钥K经由安全信道（由图1中的屏蔽路径指示）仅被发送到合法接收者。1.由于合法接收者知道K，所以他可以通过操作SK-1来解密C，以获得SK-1（C）=SK-1（SK（p））=p，即原始明文消息。安全通道不能

由于容量或延迟的原因，用于传输P本身。例如，安全通道可能是每周信使，而不安全通道可能是电话线。

密码系统是可逆变换的单参数族

 (1)

从明文消息的空格！PL到明文消息的空格！CL。参数K称为密钥，是从称为密钥空间的有限集合KL中选择的。如果消息空间！PL和！CL相等，我们将用！表示它们。毫升。当讨论单个密码变换SK时，我们有时会省略对系统的提及，而仅提及变换K。

设计密码系统SKI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。由于密码分析的计算成本而安全，但会屈服于无限计算的攻击的系统称为计算安全的；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。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码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，计算安全的密码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性密码，其中明文与随机选择的相同长度的密钥相结合。虽然这样的系统是可证明安全的，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，例如一次性密码。相反，我们考虑的是仅使用几百位密钥的系统，并且在少量数字硬件或几百行软件中是简单的。

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，但不可能很大，则我们称该任务在计算上是不可行的。

就像纠错码分为卷积和分组码一样，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（比特或字符）的形式处理明文，通常产生一个伪随机比特序列，该序列以2为模添加到

明文的比特。块密码以纯粹的组合方式作用于大的文本块，使得输入块中的小变化产生结果输出中的大变化。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是有价值的。

在认证系统中，密码学用于向接收者保证消息的真实性。不仅必须防止爱管闲事者将新的、看起来真实的消息注入到通道中，而且必须防止他通过组合或仅仅重复他在过去复制的旧消息来创建明显真实的消息。一般来说，旨在保证隐私的密码系统不会阻止后一种形式的恶作剧。

为了保证消息的真实性，添加了信息，该信息不仅是消息和密钥的函数，而且是日期和时间的函数；例如，通过将日期和时间附加到每个消息并加密整个序列。这确保了只有拥有密钥的人才能生成消息，该消息在解密时将包含正确的日期和时间。然而，必须注意使用这样的系统，在该系统中，密文中的小变化导致被解密的明文中的大变化。这种故意的错误传播确保了如果在信道上故意注入噪声将诸如“擦除文件7 ”的消息改变为诸如“擦除文件8 ”的不同消息，则它也将破坏认证信息。然后，该消息将因不真实而被拒绝。

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。用于隐私或身份验证的加密图形系统可能会受到以下威胁。

仅密文攻击是密码分析者仅拥有密文的密码分析攻击。

已知的明文攻击是密码分析攻击，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LSKL，因为该信息可以通过研究密码设备来获得。虽然许多密码学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，任何屈服于它的系统都被认为是完全不安全的。

如果一个系统对已知的明文是安全的，那么它的用户就不需要对他们过去的信息保密，也不需要在解密之前对它们进行解释。这对系统的用户来说是一个不合理的负担，特别是在商业情况下

系统本身。因此，接收方的密码表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盗。如后面所示，用于防止这种威胁的一些技术也可以防止争议的TPE威胁。即MES

可以发送产品公告或新闻稿

圣人Ma·y

被发送但随后被

加密表格，供日后公开披露。外交信函中的类似情况导致许多所谓的安全系统被破解。虽然已知的明文攻击并不总是可能的，但它的发生非常频繁，以至于不能抵抗它的系统被认为是不安全的。

选择明文攻击在实践中很难实现，但可以近似实现。例如，向竞争对手提交一份提案可能会导致他将其发送到其总部。因此，对选择明文攻击安全的密码使其用户不必担心他们的对手是否能在他们的系统中植入消息。

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。在已知的纯文本或选择的纯文本攻击下，可以立即排除使用仅密文攻击难以分析的许多系统。

从这些定义中可以清楚地看出，密码分析是一个系统识别问题。已知明文和选择明文攻击分别对应于被动和主动系统识别问题。与许多考虑系统识别的学科（如自动故障诊断）不同，密码学的目标是构建难以识别而不是容易识别的系统。

所选择的明文攻击通常被称为敌我识别，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。雷达向收到询问的飞机发送时变询问，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的响应，试图确定正在使用的认证密钥，从而对系统进行选择的明文攻击。在PRA\_CTICE中，此威胁是

发射器或接收器。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，或者客户可能拒绝接受他实际授权的订单，但他后来发现该订单会造成损失。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，但防止他生成明显真实的MES消息，从而防止接收者的认证数据的COM承诺的威胁和争议的威胁。

1. 公钥加密

如图6所示，1密码学已经成为一种衍生的安全措施。一旦存在可以沿其传输密钥的安全信道，就可以通过加密在其上发送的消息来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。

为了发展大型的、安全的电信系统，这种情况必须改变。大量的用户N导致了更大数量的（N2-N）/2个潜在的用户对，他们可能希望与所有其他用户进行私人通信。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（N2N）/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。

我们建议可以开发图1所示类型的系统。其中仅在公共信道上通信并且仅使用公知技术的两方可以创建安全连接。我们研究了解决这个问题的两种方法，称为公钥密码系统。

,.

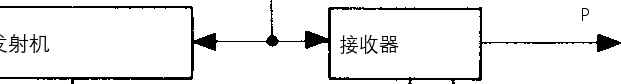
通过限制挑战的形式来应对，挑战不需要是不可预测的，而只需要是不重复的。

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。危害接收方认证数据的威胁是由以下情况引起的

消息P源

关键来源#！

p

密码分析员

关键来源#2

在多用户网络中，接收者通常是

图2.公开密钥系统中的信息流。

分别是TERNS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身份验证问题，而第二个则更接近于实现。

公钥密码系统是一对家族IEKLK E！KL和IDKLK E！KL表示可逆变换的算法， ·

等于EM。设D=E·1，我们有M=DC。因此，加密和解密都需要大约N2次运算。然而，从E计算D涉及版本中的矩阵，这是一个更难的问题。至少在概念上，求任意一对逆矩阵比求给定矩阵的逆矩阵要简单。从单位矩阵I开始，做初等的行和列运算

迭代以获得任意可逆矩阵E。

E l(:{Ml - ！毫升

DG：FML•！毫升

在有限消息空间上！毫升，这样

1. 对于每一个KE {KL，ek是DK的倒数，

(2)

(3)

从I开始，以相反的顺序进行这些相同的初等运算的逆运算，以获得D=G ·-1 .SE

可以容易地从随机位ST环中确定初等运算序列。

不幸的是，矩阵求逆只需要a.bout n 3

1. 对于每个K E！KL和M E！ML，算法EK

和DK易于计算，

1. 对于几乎每一个K e fkl，每一个等价于DG的容易计算的算法在计算上都是不可行的，
2. 对于每一个K E！KL，从K计算逆对Ek和DK是可行的。

由于第三个特性，用户的加密密钥EK可以公开而不损害其秘密解密密钥DG的安全性。因此，密码系统被分成两个部分，一个加密变换族和一个解密变换族，这样，给定一个变换族的成员，就不可能找到另一个变换族的相应成员。

第四个性质表明，当对加密或解密变换是什么没有限制时，有一种计算相应的逆变换对的可行方法。在实践中，密码设备必须包括用于产生K的真随机数发生器（例如，噪声二极管），以及用于从其输出产生EK·-DG对的算法。

给定一个这样的系统，密钥分配的问题就大大简化了。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，但不需要在任何信道上传送。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来公开。然后，任何人都可以加密消息并将其发送给用户，但没有其他人可以破译为他准备的消息。因此，公钥密码系统可以被视为多路访问密码。

保护加密密钥的公共文件免受未经授权的修改是至关重要的。由于文件的公共性质，这一任务变得更加容易。读保护是不必要的，并且由于文件随后被修改，因此可以经济地使用复杂的写保护机制。

公钥密码系统的一个有启发性但不幸无用的例子是通过将明文乘以可逆的二进制n×n矩阵E来加密表示为二进制n向量M的明文。

运营。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，且将需要极大的区块大小来获得106或更大的比率。此外，由I求E的初等运算的知识并不能大大减少计算D的时间，而且，由于在二进制算术中不存在舍入误差，因此数值稳定性在矩阵求逆中并不重要。尽管它缺乏实用性，但这个矩阵例子对于阐明公钥密码系统中必要的关系仍然有用。

寻找一对容易计算的逆算法E和D的更实用的方法；使得很难从E中推断出D，利用了用低级语言分析程序的困难。任何试图确定什么操作是由别人的机器语言程序完成的人都知道，E本身（即E做什么）可能很难从E的算法中推断出来。如果通过添加不需要的变量和语句来故意混淆程序，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。

从本质上讲，所需要的是一个单向编译程序：它接受用高级语言编写的容易理解的程序，并将其翻译成某种机器语言的难以理解的程序。编译器在EWAY上，因为它必须能够进行编译，但不能逆转该过程。由于程序大小和运行时间的效率在该应用中不是至关重要的，因此如果机器语言的结构可以被优化以帮助编译，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发密钥的问题。他的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配系统。目标是让两个用户A和B在一个安全信道上安全地交换密钥。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有一个解决方案，其密码分析成本增长为n2，其中n是合法用户的成本。不幸的是，系统的合法用户在传输时间上的成本与在计算上的成本一样多，因为Merkle的协议需要N。

Diffie和Hellman：密码学的新方向

在可以决定一个密钥之前要传输的潜在密钥。上。默克尔指出，这种高传输

**649**

作为他们的钥匙。用户I获得K；*1*通过从公共文件获得Y*1*并让

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1兆位的限制，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。

*K；1=y，X；型号Q*

*==（A：XJ）X；型号Q*



用户J以类似的方式获得K，-1

*K-1=y，-XJ mod Q。*

(9)

(10) (11)

(12)

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，它只需要交换一个“密钥”。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，一次个人访问允许用户

另一个用户必须从y；计算K；1和Y1，例如，通过计算

*K11=Yi（log “ ” YJL mod Q。* (13)

因此，我们看到，如果很容易计算log mod Q，则系统可能会被破坏。虽然我们目前还没有相反的证明（即，系统是安全的，因为FLOG mod Q很难计算），但我们也没有看到任何方法

向许多用户多次认证他的身份。Merkle的技术要求A和B相互验证

为了计算K，-ther X；或XJ，

从Y，-和Y*1*，而不首先获得EI

通过其他方式的身份。

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。让

*Y= aX modq,* 对于1s×sq-1， (4)

其中a是GF（Q）的固定本原元素，则X被称为y以a为底的对数，mod Q:

如果Q是略小于2b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次乘法mod Q，而假设取对数需要Q112=2B12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，则计算Y最多需要400次；从X；，或K；1从y；和x1，但取log mod Q需要2100或近似值

*X* = loga Ymod *q,* 对于1 s y s Q-1。

(5)

马特利1030操作。

从X计算y很容易，最多需要2 X log2Q次乘法[6，pp。398-422]。例如，对于X=18，

 (6)

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，需要使用最好的已知算法[7，pp.]进行QL/2次运算。9, 575-576], [8].

我们的技术的安全性主要取决于计算模Q的对数的难度，并且如果找到复杂度随log2Q增长的算法，我们的系统将被破坏。虽然问题陈述的简单性可能允许这种简单的算法，但它可能反而允许证明问题的难度。现在，我们假设计算log mod Q的最佳已知算法实际上接近最优，因此，对于适当选择的Q，Q112是问题复杂性的良好度量。

每个用户产生一个独立的随机数X；从整数集合中均匀选取！1，2，•••，Q-ll。各自保持X；秘密，但地方

1. OnK-Way身份验证

与密钥分发问题相比，认证问题可能是普遍采用电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。

为了开发一种能够以某种纯电子通信形式取代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特性的数字现象。任何人都可以很容易地识别签名的真实性，但除合法签名者外，任何人都不可能制作签名。我们称任何这样的技术为单向认证。由于任何数字信号都可以被精确地复制，因此一个真正的数字签名必须是可识别的，而不是未知的。

考虑多用户计算机中的“登录”问题

*Y；=•AX，模Q*

(7)

系统。当设置他的帐户时，用户选择一个输入到系统的密码DI中的密码

在公共档案里有他的名字和地址。当用户I和J希望私下通信时，他们使用

(8)

教区牧师。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。这，

但是，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。允许这样的合法访问，但阻止所有其他访问，几乎是不可能的。

这导致显然不可能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。虽然从逻辑上讲似乎是不可能的，但这个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（而不是PW）存储在密码目录中。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）与存储值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/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（按二百周年纪念的价格计算，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1-1的计算需要1030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/（PW）作为密码，因为它将自动计算f（f（PW）），而f（f（PW））与密码目录中的条目{（PW）}不匹配。

我们假设函数f是公共信息，所以

使1-1的计算变得困难的并不是无知。这样的函数称为单向函数，最早由R.M.Needham[9，p.1]用于登录过程。91].在最近的两篇论文[10]，[11]中也讨论了它们，这两篇论文提出了设计单向函数的有趣方法。

更准确地说，一个函数f是一个单向函数，如果对于定义域Off中的任何自变量X，很容易计算出相应的值f（X），然而，对于几乎所有在Off范围内的自变量X，对于任何合适的自变量求解方程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的逆不是唯一的（即，存在不同的点x1和x2，使得/（x1）=y=f（x2））时，函数f通常被称为“不可逆”。我们强调，这不是所需要的那种反演困难。相反，在给定y值和/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/在通常意义上是不可逆的，那么它可能会使寻找逆的任务图像更容易。在极端情况下，如果对于定义域中的所有X，/（X）=y*0*，则范围为！yol，并且我们可以将任何X取为 *1*（Y O）。因此，有必要使F不会产生得太少。小程度的退化是可以容忍的，

*r-*

稍后讨论，可能出现在最有前途的一类单向函数中。

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x0比在X=X*0*处计算多项式p（X）要困难得多。Purdy[11]已经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评估时间的比率。第六节详细讨论了单向函数的理论基础。如第五节所示，单向函数在实践中很容易设计。

单向功能登录协议只能解决多用户系统中出现的一些问题。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屋檐掉落的保护，并且对争议威胁的保护也不存在。

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，则他用他的秘密解密密钥“解密”该消息并发送DA（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EA对它进行“加密”来确保它的真实性。B还保存DA（M）作为消息来自A的证明。任何人都可以通过使用公知的操作EA对DA（M）进行操作来恢复M来检查该声明。由于只有A可以生成具有该属性的消息，因此单向认证问题的解决方案将直接遵循公钥密码系统的发展。

Massa Chusets Computer Associates的Leslie Lamport向作者建议了单向消息身份验证的部分解决方案。该技术采用单向函数f将k维二进制空间映射到其自身，K的数量级为100。如果发射机希望发送n位消息，他会生成2n个随机选择的k维二进制向量x1，x1，x2，x2，···，xn，并对其保密。接收机被给予F下的相应图像，即Y1，Y1，Y2，Y2，···，yn，yn•之后，当要发送消息M=（M 1，M 2，•，Mn）时，发射机根据M1=0或1发送x1或x1。他根据M2=0或1发送x2或x2。等等。接收器对第一个接收到的块进行操作，并查看它是否产生Y1或Y1作为其图像，从而了解它是x1还是x1，以及M1=0还是1。以类似的方式，接收器能够确定M*2*，M*3*，•••，Mn。但是接收者不能伪造哪怕是一点点的变化。

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大致为1兆位或更大时，存在消除扩展问题的修改。设G为A从二进制n空间到二进制n空间的单向映射，其中n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=106，则N=50，并且

K=100，这向消息添加了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Y1、Y1、•••、Yn、Yn的初始交换，则需要15%的数据扩展）。即使有

艾奇

!

I

明文

密文

Y= f (X)

对于具有相同认证序列的大量其他消息（平均2n-n），G的单向性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。找到这样的函数似乎并不困难（见第五节）。

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ft（X），其中f是单向函数。在时间t，适当的计数器是FT-t（X），其可以由系统通过应用FF（X）来检查。由于这种单向性，过去的反应对形成新的反应毫无价值。这种解决方案的问题在于，合法登录可能需要相当大的计算量（尽管比伪造登录少许多数量级）。例如，如果T每秒递增一次，并且系统必须在每个密码上工作一个月，则T=260万。然后，用户和系统必须每次登录平均迭代130万次。虽然不能安装，但这个问题显然限制了该技术的使用。如果可以找到一种简单的方法来计算）中的f<2)（n=1，2，•••），就可以克服这个问题，就像X8=UNK6UNK7x UNK82)UNK9（0（12（2（3•一样，那么T-T和T的二元分解将允许快速计算FT-T和FF。然而，TN的快速计算可能使F不是单向的。

1. 问题相互关系和陷阱门

在本节中，我们将展示到目前为止提出的一些密码图形问题可以简化为其他问题，从而根据难度定义一个松散的排序。我们还介绍了更困难的活板门问题。

在第二部分中，我们展示了用于隐私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对象。

*对已知明文攻击安全的密码系统可用于产生单向函数。* '

如图6所示，3采用密码系统ISK：IPI ICIIKE/K/，它对已知的明文攻击是安全的，固定P=Po并考虑映射

*f：* (14)

图3.用作单向函数的安全密码体制。

由定义

F{X）=SX（Po）。 (15)

该函数是单向的，因为在给定f（X）的情况下求解X等价于从单个已知明文-密码对中找到密钥的密码分析问题。公共知识OFF现在相当于公共知识！SKI和Po。

虽然这个结果的逆不一定是真的，但对于最初在搜索单向函数中找到的函数来说，产生一个好的密码系统是可能的。这实际上发生在第三节[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位生成器，其输出（密钥流）以模2的形式添加到以二进制形式表示的消息中，以模拟一次性填充。该密钥被用作决定伪随机密钥流序列的“种子”。因此，已知的明文攻击简化为从密钥流中确定密钥的问题。为了使系统安全，从密钥流计算密钥必须在计算上是不可行的。然而，为了使系统可用，从密钥计算密钥流必须在计算上简单。因此，根据定义，一个好的密钥生成器是一个单向函数。

使用任何一种类型的密码系统作为单向函数都会遇到一个小问题。如前所述，如果函数f不是唯一可逆的，则没有必要（或不可能）找到所使用的X的实际值。相反，任何具有相同图像的X就足够了。并且，虽然密码系统中的每个映射SK必须是双射的，但对上面定义的从密钥到密码的函数f没有这样的限制。事实上，保证密码系统具有这种属性似乎相当困难。在好的密码系统中，可以期望映射f具有随机选择的映射的特性（即，从所有可能的y中均匀地选择/（Xi），并且连续的选择是独立的）。在这种情况下，如果X是统一选择的，并且存在相等数量的密钥和消息（X和y），则结果y具有K+1个逆的概率近似为e-1/K！当K=0，1，2，3时，•••。这是A：泊松分布，均值A=1，移动1个单位。因此，逆元的预期数量仅为2。虽然F可能更加退化，但一个好的密码系统\_不会退化太多，因为密钥没有得到很好的使用。在最坏的情况下，如果对于某个Yo，f（X）=Yo，我们有SK（Po）=Co，并且Po的加密将完全不依赖于密钥！

虽然我们通常对do main和range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块大小的块密码，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。他们使用函数，而不是选择固定的Po作为输入

*f（X）=SX（X）。* (16)

这是一种有吸引力的方法，因为这种形式的方程通常很难求解，即使当族相对简单时也是如此。然而，这种增加的复杂性破坏了系统在已知明文攻击下的安全性与单向性之间的等效性。

另一种关系已在第四节中说明。

*公钥密码系统可以用来产生一个单向认证系统。*

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。

由于在公钥密码系统中，使用E和D的一般系统必须是公开的，因此指定E指定了用于将输入消息转换为输出密码的完整算法。这样的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，因为存在简单计算的逆。但是给定正向函数的算法，找到简单计算的逆函数在计算上是不可行的。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，才能容易地找到容易计算的逆。

在前面的段落中已经看到了活板门的形式，即活板门单向功能，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。这允许设计者在将系统出售给客户后破坏系统，但却错误地维护其作为安全系统构建者的声誉。值得注意的是，并不是更多的聪明或密码学知识使设计者能够做别人做不到的事情。如果他丢失了陷阱门信息，他的处境也不会比别人好多少。这种情况恰恰类似于密码锁。任何知道密码的人都可以在几秒钟内完成即使是熟练的锁匠也需要几个小时才能完成的事情。然而，如果他忘记了密码，他就没有优势了。

*陷门密码系统可用于产生公钥分发系统。*

为了使A和B建立共同的私钥，A随机选择一个密钥，并向B发送任意的明文-密文对。B公开了陷门密码，但对陷门信息保密，使用明文-密文对来求解密钥。A.和B现在有一个共同的密钥。

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]。

根据定义，我们将要求活板门问题是一个在计算上设计活板门是可行的问题。这为第三种类型的实体留下了空间，我们将使用前缀“准”。例如，准单向函数不是单向的，因为存在容易计算的逆。然而，即使对于设计者来说，找到容易计算的逆在计算上也是不可行的。因此，可以使用准单向函数来代替单向函数，而基本上不会损失安全性。

将陷门信息丢失到陷门单向函数使其成为准单向函数，但也可能存在无法以这种方式获得的单向函数。

将拟单向函数排除在单向函数类之外完全是一个定义问题。相反，人们可以谈论广义或严格意义上的单向函数。

类似地，准安全密码是这样的密码，其将成功地抵抗密码分析，甚至由其设计者抵抗，并且对于其存在计算上有效的密码分析算法（其当然在计算上是不可行的）。同样，从实用的角度来看，安全密码和准安全密码之间本质上没有区别。

我们已经看到，公钥密码系统隐含着陷门单向函数的存在。然而，反过来是不正确的。对于可用作公钥密码系统的陷门单向函数，它必须是可逆的（即，具有唯一的逆）。

1. 计算复杂性

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。批评家希望通过密码分析来恢复意义，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的演示。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，许多所谓的安全系统随后被攻破。

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，数学论证经常被引用来论证密码方法的强度，通常依赖于显示天文数字的计数方法

Diffje和Hellman：Crypt Ograp Hy中的新直接IO

可能的钥匙。虽然这个问题很难用这种简单的方法来解决，但即使是著名的格布雷主义者卡尔达诺也掉进了这个陷阱[2，p。145].由于系统的力量被反复论证，为系统的安全性提供数学证明的概念声名狼借，并被通过密码分析攻击的认证所取代。

然而，在本世纪，钟摆开始摆回另一个方向。在一篇与信息论的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性PAD系统提供了“完全保密”（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，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。在简单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复杂度类p（

多项式），如果它可以由确定性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。存在已知不属于P类的问题[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，类NP包括类P，并且复杂性理论中的一个重大公开问题是类NP是否严格地更大。

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[13，pp。363-404], [14].我们看到它并不缺乏。

653

使人们无法在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，但目前对其困难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。这表明有几个有趣的研究课题。信息理论家所熟悉的系综和典型性概念具有明显的作用。

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。

*如果一个系统能够在P时间内完成加密和解密操作，则该系统的CRY PT分析困难不能大于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PTIME中验证它是否正确。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。

密码学可以直接从NP复杂性理论中得出，通过检查NP完全问题可以适用于密码学使用的方式。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•X，其中a是n的已知向量（a1，a2，•••，a n），X是二元n-向量。Y的计算很简单，最多涉及n个整数的和。求F的逆的问题被称为背包问题，并且需要找到和Toy的La；L的子集。

所有2N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且每个a；为32位长，Y最多为39位长，并且F是高度退化的；再

654 IEEE信息理论汇刊。1976年11月

平均只有2个38试图找到解决方案。更平凡的是，如果a；=2i-l则对/求逆等价于求y的二元分解。

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。对于任何特定的阵列，没有任何困难的迹象。然而，似乎从Io，I，2，•••，2n-LJ中一致地选择LAD导致了一个困难的问题，其概率为n-+-OO。

另一个在算法分析中感兴趣的潜在单向函数是指数mod Q，它是由斯坦福大学的John Gill教授向作者提出的。这种功能的单向性已经在第三节中讨论过。

1. 历史视角

虽然本文中提出的公钥系统和单向认证系统最初似乎不是由过去的密码学发展所预示的，但可以将其视为数百年前密码学发展趋势的自然产物。

保密是密码学的核心。然而，在早期的密码学中，关于什么是保密的，存在着混乱。密码系统，如凯撒密码（其中每个字母都被后面的13位替换，因此A被携带到D，B被携带到E，等等）的安全性依赖于保持整个加密过程的机密性。在电报发明之后[2，191]，一般系统和特定密钥之间的区别允许一般系统被泄露，例如通过盗窃密码设备，而不需要对新密钥中加密的未来消息进行通信。这一原则由Kerchoffs编纂[2，p。）。他在1881年写道，密码系统的泄密不应给通信者带来不便。大约在1960年，密码系统\_h投入使用，这被认为是足够强大的，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。这些发展中的每一项都减少了系统中必须保护公众知识的部分，消除了诸如在外交急件出现之前对其进行解释等繁琐的权宜之计。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间里，出现了一种革命趋势，这种趋势现在正在取得成果。专用机器是为加密而开发的。然而，在通用数字硬件开发之前，密码术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许多尝试的失败导致了由Kerchoffs[2，p.]提出的通过密码分析攻击进行认证的范例。上个世纪有234个）。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，选择纯文本攻击）。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。生产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，主要来自于自动化工程师。托马斯·杰斐逊，一位密码学爱好者，在第二次世界大战中仍在使用的系统[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，在最近的过去，由于几乎完全的政府垄断，参与一直受到阻碍。

参考文献

[1）R.Merkle，“在不安全信道上的安全通信”，提交给美国计算机学会通讯。

*[2]）D.卡恩，密码破译员，秘密写作的故事。纽约：麦克米伦出版社，1967年。*

[3）C.E.Shannon，“保密系统的通信理论”，《贝尔系统技术杂志》，第第28页656-715，1949年10月。

[4]）M.E.Hellman，“密码学香农理论方法的扩展”，提交给IEEE Trans。通知。理论，9月1975.

[5]）W.Diffie和M.E：Hellman，“多用户密码技术”，1976年6月7-10日在纽约国家计算机会议上发表。

1. *D.Knuth，《计算机编程艺术》，2、半数值算法。雷丁，马萨诸塞州：阿迪森，或艾迪生-韦斯利，1969年。*
2. *《计算机编程艺术》，3、排序查找。雷丁，马萨诸塞州：阿迪森，或艾迪生-韦斯利，1973年。*
3. S.Pohlig和M.E.Hellman，“ GF（p）中计算算法的改进算法及其密码学意义”，提交给IEEE Trans。通知。理论。
4. *M.诉威尔克斯，分时计算机系统。纽约：埃尔塞维尔，1972年。*

[10）A.Evans，Jr.，W.Kantrowitz，和E.Weiss，“计算机中不要求保密的用户认证系统”，“ ACM的通信”，VFLI。第17页，437-442，1974年8月。

1. G.B.Purdy，“高安全性登录程序”，《美国计算机学会通讯》，第17页，442-445，1974年8月。
2. W.Diffie和M.E.Hellman，“ NBS数据加密标准的密码分析”，提交给计算机，1976年5月。

[13）A.V.Aho，J.E.Hopcroft和J.D.Ullman，计算机算法的设计和分析。雷丁，马萨诸塞州：阿迪森，或艾迪生·韦斯利，1974年。

[14）R.M.，Karp，“组合问题中的可归约性”，《计算机计算的复杂性》。R.E.Miller和J.W.Thatcher编辑。纽约：全体会议，1972年，85- 104.