密码学的新方向

邀请文件

惠特菲尔德·迪菲和马丁·E。赫尔曼

摘要研究了当代密码学的两种发展。远程处理的广泛应用引起了对新型密码系统的需求，该系统将对安全密钥分发通道的需求最小化，并提供相当于书面签名的需求。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学问题提供工具。

1介绍

我们今天正站在一场密码学革命的边缘。
廉价数字硬件的发展使其从机械计算的设计限制中解放出来，并将高级加密设备的成本降低到可以用于远程提款机和计算机终端等商业应用。反过来，这样的应用程序又产生了对新类型的加密系统的需求，从而最小化安全密钥分发通道的必要性，并提供相当于书面签名的需求。与此同时，信息论和计算机科学的理论发展显示出了提供可证明的安全密码系统的希望，将这一古老的艺术变成了一门科学。

计算机控制通信网络的发展承诺了世界两端的人或计算机之间轻松和廉价的接触，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，这些联系人必须确保安全，以防止窃听和注入非法消息。然而，目前，安全问题的解决方案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如此严重的不便，从而消除了远程处理的许多好处。

最著名的密码问题是隐私：防止未经授权的提取信息

手稿于1976年6月3日收到。这项研究得到了国家科学基金会ENG 10173。这部分工作在1975年6月23-25日在马州勒诺克斯举行的IEEE信息理论研讨会和1976年6月21-24日在瑞典龙尼比举行的IEEE信息理论国际研讨会上发表。

W.Diffie曾在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工作。

M.E.赫尔曼在斯坦福大学电气工程系工作，邮编94305。

通信通过一个不安全的通道命令来使用密码学来确保隐私，然而，目前通信方需要共享一个任何其他人都不知道的密钥。这是通过发送钥匙提前通过一些安全的通道，如私人快递或注册邮件。然而，两个没有熟人的人之间的私人对话在商业中是很常见的，期望最初的业务联系推迟足够长的时间，以通过某种物理方式传输钥匙是不现实的。这一关键分配问题所带来的成本和延迟是将业务通信转移到大型远程处理网络的一个主要障碍。

第三节提出了两种通过公众信息传递关键化信息的方法。e.，不安全的)通道，而不损害系统的安全性。在公钥密码系统中，加密和破译由不同的密钥E和D控制，因此从E计算D在计算上是不可行的(e。g.，需要10^{100}操作指南因此，加密密钥E可以被公开披露，而不影响破译密钥D。因此，网络中的每个用户都可以将其加密密钥放在一个公共目录中。这使得系统的任何用户都能够向任何其他用户发送消息，以便只有预期的接收方能够破译它。因此，一个公钥密码系统是多重访问密码。因此，任何两个人之间都可以进行私人对话，无论他们以前是否交流过。每个人都向接收方公开加密密钥，并使用自己的加密密钥破译他收到的信息。

我们提出了一些开发公钥密码系统的技术，但这个问题仍然在很大程度上是开放的。

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渠道的需要。在这样的系统中，两个希望交换密钥的用户来回通信，直到他们到达一个密钥。窃听此交换的第三方必须发现从所听到的信息中计算密钥在计算上是不可行的。在第三节中给出了公钥分配问题的一个可能的解决方案，并且Merkle [1]有一个不同形式的部分解决方案。

第二个问题是认证，它可以解决用远程处理系统取代当代商业通信的加密解决方案。在当前的业务中，由签名保证的合同的有效性。已签署的合同可作为达成协议的有效证据

如有必要，持有人可以出庭。然而，使用信号——未经授权将信息注入到公共通道，需要传输和存储书面信息，以确保接收者发送信息的发送者的合法性。契约为了有一个纯粹的数字替代品，如果a频道的安全性不足，就被认为是公开的，每个用户必须能够根据其用户的需要产生信息。像电话线这样的频道，其真实性可以被任何人检查，但因此可能被一些用户认为是私人的，而不是由任何人，甚至收件人制作的。由其他人。任何频道都可能受到窃听的威胁，因为只有一个人可以发送信息，但许多人或注射或两者都可以，这取决于它的使用情况。在电话通勤中可以接收信息，这可以看作是一个广播密码。网络通信，注入的威胁是最关重要的，因为目前所谓的电子认证技术不能满足这一方不能确定哪个电话正在呼叫。窃听，需要。这需要使用窃听，在技术上更为困难，第四节讨论了提供一个真实的、数字的和法律上危险的问题。相比之下，在无线电中，目前的情况与消息相关的签名。出于那里的原因，是相反的。窃听是被动的，不涉及任何法律，我们称之为单向身份验证问题。给出了一些危险，而注入暴露了非法发射器的部分解，并显示了任何公钥的发现和起诉。

密码系统可以转化为单向身份验证——将我们的问题分为隐私和保护系统。我们有时会进一步细分身份验证-第五节将考虑各种加密与消息验证的相互关系，这是问题定义的图形问题，并介绍了上述更困难的问题，以及用户验证，其中唯一的任务是陷阱门。系统是为了验证一个人是否是他所声称的人。同时，通信和计算例如，个人的身份提出信贷引起新的密码问题，注销，卡必须验证，但没有消息，他希望信息理论，和计算理论已经开始传播。尽管在供应工具中明显没有一条关于解决类用户身份验证中的重要问题的信息，但这两个问题在很大程度上是等价的。卡尔密码学。在用户身份验证中，存在一条隐式消息。“我是

寻找牢不可破的代码是用户X最古老的主题之一，”而消息身份验证只是密码研究的验证，但直到本世纪提出的系统——发送消息的一方的身份。茎上的差异最终被打破了。在20世纪20年代，威胁环境和这两个缺点的其他方面，“一次性垫”被使用，并证明是象征，然而，有时使它方便区分牢不可破[2，pp。398 – 400].他们之间的理论基础。

这个系统和相关系统是在一个坚实的基础上的，图1说明了传统的信息流一个世纪后，由信息论提出的[3]。一个时间垫需要用于通信隐私保护的密码系统。白天非常长，因此非常昂贵有三方：一个发射器，一个接收器，和一个屋檐-

在大多数应用程序。使滴下的东西发射机产生明文或纯文本

相比之下，大多数加密系统的安全性消息P将在一个不安全的通道上通信，除了在计算困难的密码分析人员的鉴定合法的接收者。为了防止窃听者被窃听在不知道钥匙的情况下覆盖明文。这个问题从学习P，发射机以可逆的P上lem属于计算复杂度和转换S_K生成密文或密码C对算法的分析，是最近的两个门徒所研究的= $S_K(P)$.密钥只传输给合法接收器解决计算问题的困难。使用结果通过一个安全通道，如图1中的屏蔽路径表示。在这些理论中，可以扩展安全性的证明由于合法的接收者知道K，所以他可以通过破解C在可预见的将来使用更有用的类系统。部分使用S操作$_K^{-1}$获得$S_K^{-1}(C) = S_K^{-1}(S_K(P)) = P$

VI探讨了这种可能性。原始明文信息。无法使用该安全通道

在继续进行新的开发之前，我们将介绍ter-由于容量或延迟的原因而传输P本身。例如，

并在下一节中定义威胁环境。

2常规密码学

密码学是对“数学”系统的研究，涉及到什么

有两种安全问题：隐私性和身份验证。A

隐私系统防止通过匿名提取信息

利用通过公共渠道传输的信息，

从而向消息的发送者保证它是只读的**图1：传统密码学中的信息单元流程**由预期的收件人。身份验证系统会阻止系统。

安全通道可能是每周的快递，不安全通道可能在明文中添加了模2。阻止密码用来引导电话线。在大型文本块上的纯组合方式中，在加密系统中是一个单一的参数族，这样在输入块中的一个小的变化就会产生a
{S $_K$}；z $_K$={$_K$；z}可逆转换的结果输出的重大变化。本文主要讨论

使用块密码，因为这个错误传播属性是

S_K：{P}→{C} (1)在许多认证应用程序中具有重要价值。

在认证系统中，密码学用于保证从明文消息的空间到tee的空间到接收方的消息的真实性。不仅是密文信息。参数K称为密钥，必须防止调解程序注入全新的，从称为密钥空间的有限集合{K}中选择的。如果消息观察到一个通道中，但他必须被阻止空格和相等，我们将用M来表示它们。通过组合创建明显真实的消息，或当讨论单个加密转换时$_K$，仅仅重复他复制的旧信息，我们有时会忽略对这个系统和过去的提及。一种旨在保护隐私的密码系统
参考变换K。一般来说，不会防止后一种形式的伤害。

设计密码系统的目标$_K$}是保证消息的真实性，信息是加密和破译操作廉价，但添加不仅是一个函数的消息和秘密确保任何成功的密码分析操作太关键，但日期和时间，例如，通过附加plex经济。这个问题有两种方法——每个消息的日期和时间，以及加密整个lem。由于计算代价序列而安全的系统。*这就保证了只有拥有密码分析但会受到密钥攻击的人才能生成消息，当解密时包含无限计算，被称为计算安全；而适当的日期和时间。然而，必须小心使用一个能够抵抗任何密码分析攻击的系统，无论在一个系统中密文的小变化导致允许多少计算，被称为破译明文中无条件的大变化。*此故意错误安全。无条件安全系统的讨论在[3]中，传播确保如果故意注入噪声到[4]和属于信息理论的那部分，称为通道改变一个消息，如“擦除文件7”到a
香农理论，它涉及的最佳性能不同的消息，如“擦除文件8”，它也会破坏
可获得无限的计算。鉴别信息然后，该消息将被拒绝

无条件安全的结果是，存在的多重是不真实的。
对密码学的有意义的解决方案。例如，评估由英文文本可用密码系统产生的密码替代密码XMD是否充分的简单第一步是将它们将要面临的威胁进行分类：现在，和，等等。一个计算对象。相反，加密系统安全密码可能会出现以下威胁，其中包含用于隐私或身份验证的足够项。用来唯一确定明文和键的信息。仅密文攻击是一种密码分析攻击，其中其安全性仅在于计算它们的成本。密码分析人员只拥有密文。

唯一常用的无条件安全系统是已知明文攻击是密码分析攻击，其中明文与密码分析员结合，拥有大量相应的随机选择的相同长度的密钥。而这样的系统则是明文和密文。
是否被证明是安全的，就需要大量的密钥，使它成为一个被选择的明文攻击，是一种密码分析攻击，在其中
对大多数应用程序都不实用。除非另有说明，密码分析人员可以提交无限数量的明文，本文处理计算安全系统，因为他自己选择和检查结果的消息，这些更普遍适用。当我们谈论密码的时候。
需要开发可证明的安全密码系统，我们排除在所有情况下，它假设对手知道一般的那些，如一次性垫，这是笨拙的使用。系统$_K$在使用中，由于这些信息可以获得，我们考虑的系统只使用几百个研究一个加密设备。虽然许多用户的密码位的密钥和可实现在少量的说唱试图保持他们的设备秘密，许多商业
数字硬件或几百行软件。*应用程序不仅要求一般系统是公共的，如果一个任务的成本在计算上不可行，但它是标准的。*
通过使用的内存量或运行时来衡量，仅密文攻击在实践中经常发生。它是有限的，但非常大。密码分析人员只使用有关统计 属性的知识 正如纠错码被划分为正在使用中的语言的卷积一样(e。g.，在英语中，字母e出现13和块码，密码系统可以分为时间百分比)和某些“可能”单词的知识两大类：流密码和块密码。流（e。g.，有一封信可能是以“亲爱的先生”开头的。

这是最弱的
密码以小块（比特或字符）处理明文，系统可能受到的威胁，任何系统通常产生屈服的伪随机比特序列都被认为是完全不安全的。

能够防止已知明文的安全的系统也可以防止争议的威胁。也就是说，消息使用户不必保密过去的消息，可能会发送，但后来被发送器拒绝，或者在分类之前解释它们。这是一个没有理由的问题---------接收者。或者，任何一方都可能声称，一个可以给系统用户造成的信息负担，特别是在通信中，而实际上没有发送。不可伪造的数字签名的商业情况下，需要幸运的公告或新闻稿和收据。例如，一个不诚实的股票经纪人可能会以打字的形式发送，以便以后公开披露。类似的情况可能会试图掩盖未经授权的买卖，通过伪造客户的订单导致了巨大的个人利益，或者客户可能会有许多所谓的安全系统。虽然一个已知的文本攻击否认了他实际上授权的命令，但他后来并不总是可能的，但它的发生已经足够了，一个看到就会造成损失。我们将介绍一些允许无法抵抗它的系统被认为是不安全的概念。由接收者来验证消息的真实性，但要防止

所选择的明文攻击在正义上是难以实现的，他可以产生明显真实的信息，因此但可以近似。例如，提交给一个建议，保护的威胁，收到的竞争对手的妥协可能导致他加密它的传输者的认证数据和争议的威胁。
他的总部。一种能防止被选中的密码
因此，明文攻击使用户不必担心是否会发生攻击
他们的对手不能在他们的系统中传递信息。

为了证明系统是安全的，它是近似的
考虑更强大的密码分析
不仅提供了更现实的关怀环境模式
但要对密码系统的性能进行评估
力量更容易。许多系统难以分析
使用密文检查可以立即排除
在已知的解释或所选择的明文攻击下。

从这些定义中可以清楚地看出，密码分析是一种识别-
问题。已知的明文攻击，甚至是明文攻击
对应于被动和主动的识别问题，
各自地不像系统识别中的许多影响
是否考虑到，这种自动故障诊断的目标，在加密-
图形是建立困难的系统，而不是简单的，
鉴定

所选择的明文攻击通常被称为IFF攻击
从发展过程中的起源而产生的术语
密码的“识别朋友或系统后的世界
第二次战争。一个IFF系统使天文雷达能够区分
友军和敌人都会自动发生。雷达发送一个时间-
对接受挑战的飞机进行不同，病人
它在适当的键下，并把它发送回雷达。凭借
将此响应与正确的脚本版本进行比较
挑战性，雷达可以识别友好的飞机。而
飞机在敌人的领土上空，敌人的密码分析人员可以发送
挑战，并期望加密响应的尝试
来确定正在使用的身份验证密钥，从而挂载选定的
文本攻击系统。在实践中，这个威胁被进入了
通过限制挑战的形式，而这并不是
不可预测的，但只是不重复的。

还有其他威胁可以
不用传统密码学治疗，需要
借鉴本文减少的新思想和技术。
ver身份验证数据的威胁是
受多用户网络的情况
接收器通常是系统本身。接收器的密码
那么，表和其他身份验证数据就更容易受到攻击
盗窃比那些发射机（个人用户）。作为
后面展示了一些防止这种威胁的技术

3公钥密码学

如图1所示，密码学一直是一种衍生的安全度量。一旦存在一个可以传输密钥的安全信道，就可以通过加密在它们上面发送的消息，将安全性扩展到其他具有更高带宽或更小延迟的信道。其结果是将密码学的使用限制在那些事先为密码学安全做好准备的人之间的通信中。

为了开发大型、安全的电信系统，必须改变这一情况。大量的用户n会导致一个更大的数字，$(n^2-n)/2$对可能希望与所有其他人私下交流的潜在伴侣。假设一对事先不认识的用户能够等待一个密钥通过某种安全的物理方式发送，或者假设所有的密钥(n^2可以提前安排2对。在另一篇论文[5]中，作者考虑了一种保守的方法，不需要在密码学本身进行新的发展，但这涉及到降低安全性、不便，并限制网络对初始连接协议的恒星配置。

我们建议可以开发图2所示类型的系统，在该系统中，双方仅通过公共通道进行通信，并且仅使用公开已知的技术可以创建安全连接。我们研究了两种解决这个问题的方法，分别称为公钥密码系统和公钥分发系统。第一个更强大，提供身份验证问题的解决方案
下一节讨论，而第二节更接近实现。

图2：公钥系统中的信息流程。

一个公钥密码系统是一对家族{E$_K$*}* $_K$={ *K*涉及一个版本的矩阵，这是一个更难的问题。和{D$_K$} K ={K}对于表示可逆的算法，至少在概念上比对给定矩阵的变换更简单。从单位矩阵I开始，做基本的行和列歌剧-

(2)来得到一个任意的可逆矩阵E。然后从我开始做这些基本运算的逆序得到D = E⁻¹.基本的序列

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

(3)操作可以很容易地从一个随机的位字符串中确定。不幸的是，矩阵反演只需要大约n个时间[3] 歌剧院

在一个有限的信息空间

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

“密码分析”时间的比率(i。e.，计算D来自因此，对加密或破译时间的E)最多为n，和需要巨大的块大小才能获得10的比例[6]

1)为每个K = {K}，E*K*是D的倒数吗*K*，

2)为每一个K = {K}和M = {M}，算法E*K*和D*K*容易计算，或更高。而且，似乎没有知识

3)

德rive f rom *E*$_K$,

4)for 前夕 ry *K*∈ ，计算逆对是可行的的

E$_K$和D*K*从K.

error 在 binary arithmetic,n um er icalstability isu nim p ortant in the matrix inversion. In sp它eo f 它tslack of prac icalu 提litythi s matrix exa mple iss till useful for clarifyingtherelationships necessary iln a pubic key cryptosystem.

ces

的计

由于第三个属性，用户的加密密钥E*K*一个更实用的方法可以找到一对容易的-

在不影响其秘密推反算法E和D的安全性的情况下公开；这样D很难推断出解码密钥D*K*.因此，密码系统从E中分离出来，利用分析程序的困难分为两部分，即加密转换家族和低级语言。任何人试图以这样一种方式确定解读转换的家族，给定的操作是由别人的机器语言，一个家族的成员完成的，找到相应的程序知道E本身(i。e.，E所做的事情)可能很难做到另一个成员。从E的一个算法中推断出来的。如果要制作这个程序

第四个属性保证有一种可行的方法，通过添加不必要的变量来计算相应的逆变换和语句对，然后确定一个逆算法可能是当没有约束放置在什么加密或非常困难。当然，它必须足够复杂，才能破译转换。在实践中，加密设备防止输入输出对识别。

集合必须包含一个真正的随机数生成器(e。g.，一个本质上需要的是一个单向编译器：一个有噪声的二极管)来生成K，连同一个算法，以采取一个容易理解的程序编写的高级

生成E*K*— D*K*从它的输出对。语言，并将其翻译成一个难以理解的程序

给定这类系统，某些机器语言中的密钥分配问题。编译器是单向的，因为它大大简化了。每个用户生成一对反反——编译必须是可行的，但在他的终端形成E和D不可行。破译为转换-反向转换的过程。由于程序大小和信息D的效率必须保密，但不需要通信，运行时在这个应用程序中并至关重要，比如任何通道上的编译器。如果机器语言的结构可以将其与用户名一起放在公共目录中，并进行优化以帮助避免混淆，则加密密钥E可能可以被公开。

地址任何人都可以加密消息并将它们发送到Merkle [1]已经独立研究了分配的问题

用户，但没有其他人可以破译旨在通过不安全的通道清洗密钥的消息。他的方法完全不同。因此，公钥密码系统可以看作是上述公钥密码系统的倍数，

访问密码。并将被称为公钥分配系统。目标是

加密密钥的公共文件必须对两个用户A和B提供支持，以安全地交换一个从未经授权的修改中检测到的密钥。此任务使不安全的通道更容易执行。然后，两个用户在文件的公共性质中使用这个键。读取保护是加密和破译的不必要的普通密码系统。而且，由于文件很少被修改，精心编写的Merkle有一个解决方案，其密码解析成本随着n而增长[2]

保护机制可以经济地使用。其中n是合法用户的成本。不幸的是

暗示，虽然不幸的是无用的，系统的合法用户的成本是在传输密钥密码系统是加密明文，表示时间计算，因为Merkle的协议需要作为二进制n向量m，通过乘以一个可逆的二进制n潜在键传输之前一个关键可以决定n x n矩阵E。因此，这个密码图就等于Em。让D=打开。Merkle指出，这种较高的传输开销阻止了E⁻¹我们有=直c。因此，加密和破译这个系统在实践中都非常有用。如果一个一兆比特需要大约n^2操作然而，从E计算D，限制是放置在设置协议的开销，他的技术

可以实现大约10 000比1的成本比，这是他们的关键。用户我获得K_{ij}通过获得Y_j对于大多数应用程序来说都太小了。如果价格便宜，高带宽的文件和出租
数据链接可用，比率为100万到1或更多
能否实现，该系统将是实质性的实践-(9)cal值。

$$K_{ij} = Y_j^{X_i} \bmod q$$

现在，我们还建议建立一种新的公钥分配系统
有几个优点。首先，它只需要一个“键”来完成(10)
交换。第二，密码分析的努力需要增长

$$= (\alpha^{X_j})^{X_i} \bmod q$$

指数级的在合法的用户的努力。第三，
它的使用可以被绑定到一个用户信息的公共文件中
用于向用户B验证用户A，反之亦然。通过使(11)

$$= \alpha^{X_jX_i} = \alpha^{X_jX_i} \bmod q.$$

公共文件本质上是一个读取记忆，一个个人的外观
允许用户多次多次身份验证其身份用户j获得K_{ij}以类似的方式
用户rkle的技术需要A和B来相互验证
通过其他方式进行活动。K_{ij}= $Y_I^{X_j}$mod q.(12)
新技术利用了明显的困难
计算一个有限域GF (q)上的对数另一个用户必须计算K_{ij}从Y_i和Y_j例如
元素的数量q。让通过计算

$Y = a^X$国防部q，用于1三X三q-1，(4)K_{ij}= $Y_I^{(\log aYj)}$mod q.(13)

这里a是一个固定的基本元素，那么X被安排，我们因此看到，如果日志mod q很容易计算系统
到以Y为基值a的对数，mod q：可以被打破。虽然我们目前还没有证据证明
相反(i。e.，如果日志模块q是，则系统是安全的
X=日志aY模型q，对于1三Y三q-1。(5)很难计算)，我们也没有看到任何计算的方法
K_{ij}从Y_i和Y_j没有先获得X_I或X_j.
从X开始计算Y很容易，最多取2倍的日志2 如果q是一个略小于2的素数b，那么所有的数量都是
乘法[6，pp。398 - 422]. 例如，对于X=，可以表示为b位数。然后就会出现情绪波动
大多数2b乘法mod q，而通过假设取日志
$Y = a^{18}$= $(((a^2)^2)^2)^2$x a^2.(6)要求$q^{1/2}$= $2^{1/2}$操作因此，密码分析的努力
相对于合法的努力，它呈指数级增长。如 果 b = 200，
另一方面，计算Y可以更邪教，而最多需要400个乘法来计算Y_I对于某些精心选择的q值，需要从X开始i，或K_{ij}从Y_i和X_j，但
取日志mod q需要q的顺序$1/2$操作，使用最著名的ithm[7，pp]。9， 2^{100}或大约10^{30}操作
575 - 576]，[8].
我们的技术的安全性关键取决于安全性
计算对数mod q，如果一个算法的**4单向认证**复杂性随着日志的增长而增长2 q会被发现，我们的m就会被发现
破损的虽然问题陈述的简单性可能身份验证的问题可能是一个更严重的允许这样简单的算法，正确而允许一个障碍证明普遍采用电信问题的困难。我们如何假设最著名的业务事务比密钥分配的问题。洗日志mod q的算法实际上是接近最优的，而认证是任何涉及契约的系统的核心，因此$q^{1/2}$是一个很好的衡量问题的复杂性和计费的方法。没有它，企业就无法运转。电流电极
正确选择q。电子认证系统不能满足纯粹的需求
这样的用户生成一个独立的随机数，所选择的数字的，不可原谅的，消息依赖的签名。它们实际上来自于整数的集合{1,2，。..，q-这样保持对第三方伪造的保护，但不保护X_I秘密，但反对发射机和接收器之间的纠纷。
为了开发一个能够取代电流的系统
Y_I= a^{X_i}国防部q (7)书面合同与一些纯电子形式的通信-
阳离子，我们必须发现一个与之相同的数字现象
带有他的名字和地址的公共档案。当用户时，我希望属性作为一个书面签名。任何人都必须很容易私下交流，他们使用识别
签名是真实的，但除了合法的签名者之外，任何人都不可能产生它。我们会打电话给任何人
K_{ij}= $a^{X_IX_j}$*mod q (8)这种技术的单向身份验证*。因为任何数字信号

可以精确地复制，一个真正的数字签名必须重新编码-一个值y和f的知识，以计算任何x
在不被知道的情况下可缩小。它的属性为f (x) = y。事实上，iff是不可可逆的

考虑多用户计算机系统中的“登录”问题——通常意义上，它可能会使找到一个逆项的任务。在设置帐户时，用户更容易选择密码图像。在极端情况下，iff (x) = y_0对于域中的所有x，它被输入到系统的密码目录中。那么每个人的偏离范围都是{y_0}，我们可以取任何一个x作为$f^{-1}(y_0)$.当用户登录时，用户再次被要求提供密码。因此，f必须不要太退化。通过对所有其他用户保守这个密码的秘密，伪造的退化程度是可以容忍的，并且，正如后面所讨论的，是登录是可以防止的。然而，这使得保持密码目录的单向类的安全性至关重要，因为它的功能是信息。

包含将允许完美地模拟任何用户。如果系统算子具有合法性，则多项式提供了单向函数问题的一个基本例子。要找到一个根 x要困难得多$_0$的多项式配对访问目录的原因。允许这样的合法方程p (x)比计算在配偶访问时的多项式p (x)，但阻止所有 其他的，几乎是不可能的。$x = x_0$.Purdy [11]建议使用稀疏多项式 这导致了有限字段上非常高的要求，这些字段似乎有新的登录程序，能够判断非常高的解决方案与评估时间比率的真实性。这些理论上的密码，其实并不知道它们。而作为单向函数的基础是更详细的讨论

这在逻辑上是不可能的，这个建议很容易得到满足。当第六节。并且，如第五节所示，用户首先输入密码PW，计算机自动-在实践中很容易设计。

集中和透明地计算一个函数f（PW），并存储单向函数登录协议只解决了其中的一些问题，而不是PW，在密码目录中。在多用户系统中出现的问题。它防止登录，计算机计算f (X)，其中X是系统认证数据的妥协，并将f (X)与存储值f（PW）进行比较。如果在使用中，但仍然要求用户发送真正的密码，只有当它们相等时，用户才被接受为系统。必须提供防檐保护。由于函数f必须在每次登录时计算一次，因此它通过额外的加密，并且对计算时间威胁的保护必须很小。一百万条指令(成本争议完全没有。

大约0美元。一个公钥密码系统可以用来对这种计算产生一个真正合理的限制。但是，如果我们可以确保，单向身份验证系统如下。如果用户A希望停止该计算f^{-1}需要10^{30}或者更多的指令，一些-发送给用户B的消息M，他在他的秘密中“破译”它，这个人破坏了系统以获得密码破译密钥并发送D_A(M).当用户B接收到它时，他的目录实际上不能从f（PW）获得PW，并且可以读取它，并通过“加密”来保证其真实性，因此不能执行未经授权的登录。请注意，f（PW）它与用户A的公共加密密钥E_A.B也保存了D_A(M)不被登录程序接受为密码，因为它可以证明该消息来自于a。任何人都可以检查，这将自动计算f（f（PW））， 这将不匹配的索赔操作在D_A(M)具有公开知道的操作

密码目录中的条目f（PW）。E_A恢复M。因为只有A可以生成一个消息

我们假设函数f是公共信息，因此有了这个属性，单向身份验证的解决方案并不是无知的，从而使计算关闭f^{-1}困难的问题将立即从发展，这些函数被称为单向函数，是第一个公钥密码系统。

用于R的登录程序。M.李约瑟[9，p。单向消息身份验证有一个部分解决方案，建议-
91].他们也在最近的两篇论文[10]中进行了讨论，马萨诸塞州的莱斯利·兰波特向作者提供了[11]，这些论文提出了有趣的单杆协会设计方法。这种技术采用了一个单向函数

方式函数。f将k维的二进制空间映射到其自身中

更准确地说，一个函数f是一个单向函数，如果，对于阶数为100。如果发射机希望发送一个Nbit消息，任何参数x在域关闭，很容易计算他生成2N，随机选择，k维二进制向量对应值f (x)，然而，几乎所有的y在torx范围$_1$,X_1,x_2,X_2，...，x_N,X_N他对此保密。接收方f，在计算上不可能求解方程y =f (x)，给出了f下对应的图像，即y_1,Y_1,y_2,Y_2

对于任何合适的参数x。...,y_N, Y_N之后，当消息m = (m_1,m_2，...,m_N)是

重要的是要注意，我们正在定义一个被发送的函数，发射器发送x_1或X_1这取决于从计算的角度来看是否不可逆，而是其m_1=0或1。他发送x_2或X_2取决于m_2=的不可逆性完全不同于通常的含义-0或1等。接收机在第一个接收到的数学学习表上用f操作。一个函数f通常被称为“非内块”，看看它是否产生y_1或Y_1当一个点y的逆不是唯一的时候，(i。e.，我们可以知道它是不是x_1或X_1，以及m_1=0或1。在存在的点x_1和x_2这样f (x_1) = y = f(x_2)).我们以类似的方式表示，接收器能够确定m_2,m_3，...,m_N.强调这不是那种反转困难，但接收器是不能锻造一个改变，甚至在一个是必需的。相反，它一定是极其困难的，考虑到一点m。

这只是一个部分解，因为近似的，如图所示。3、采用密码系统{S_K：{P}→需要100倍的数据扩展。然而，有一个修改的=是安全的，可以防止已知的明文攻击，它消除了当N是=时的扩展问题0考虑一下地图
大约一兆比特或更多。设g是一个单向映射
二值n空间到二值n空间，其中n大约为50。f:{K} → {C} (14)
取N位信息m，用g对其进行操作，得到
n位向量m，。然后使用前面的方案发送m，。定义为
IfN = 10^6，n = 50和100，这增加了kn = 5000身份验证
消息的位。因此，它只需要5%的数据扩展-f(X)=$S_X(P_0)$ (15)
腐蚀在传输期间腐蚀(或15%，如果初始交换

y_1，Y_1， ...， y_N,Y_N包括在内）。即使有很大，这个函数是单向的，因为求解给定的Xf(X)是其他消息的数量(2^{N-n}平均而言)，与从身份验证序列中寻找密钥的密码分析问题相同，单向性使它们成为一个已知的明文密码对。公共知识在理论上不可能找到，我们也无法伪造。实际上，g必须关闭，现在相当于对{S的公共知识$_K$}和P_0.比正常的单向函数稍强一些，因为这个结果的逆不一定是正确的，它的对手不仅而且有它的逆像m。对于一个最初在搜索中找到的函数，即使给定m，也很难找到一个不同的逆像单向函数来产生一个好的密码系统。这实际上是m。找到这样的函数似乎没有带来什么麻烦（见第五节中讨论的离散指数函数）。第三节[8]。

还有一个关于单向用户授权的另一个部分解决方案——单向函数是块密码和关键阳离子问题的基础。用户将生成一个密码，并保存其生成器。密钥生成器是一个伪随机位生成器的秘密。他给出了系统^T(X)，其中是一个单向函数。它的输出，密钥流，被模2添加到一个消息在时间t，适当的身份验证器是f^{T-t}(X)，可以用二进制形式表示，模仿一次性垫。由系统通过应用f进行检查^t(X).由于一个键被用作“种子”，它决定了伪随机路径关闭，响应在建立一个新的关键流序列中没有价值。一个已知的明文攻击因此减少为响应。这个解决方案的问题是，它可能需要从密钥流中确定密钥。对于合法登录的大量计算（虽然系统是安全的，从密钥的计算比伪造的数量级要少）。例如，如果树在计算上是不可行的。而，对于系统t每秒增加一次，系统必须工作才能可用，从密钥计算密钥流必须一个月的每个密码，然后T=260万。两者都很简单。因此，一个好的密钥生成器是，几乎是用户，系统然后必须迭代f平均130万的定义，一个单向函数。
每次登录次数。虽然不是不可克服的，但这个问题是，使用任何一种类型的密码系统作为一个单向函数

大大限制了该技术的使用。这个问题可能会有一个小问题。如前所述，如果函数出现，如果一个简单的计算f（2吨），用于n = 1,2， ...f不是唯一可逆的，它是没有必要的（或可能的）可以被找到的，许多类型的X^8= ((X^2)^2)^2.然后对于二进制解密-找到所使用的X的实际值。相反，任何具有T-和T位置相同的X都将允许快速计算f^{T-t}图像就足够了。并且，当每个映射S_K在一个密码和f^t.然而，这可能是一个快速的计算过程^{n}前置器必须是双射的，对函数没有这样的限制
不是单向的。f从密钥到上面定义的密码符。的确，保证

一个密码系统具有这种特性似乎相当困难。在一个好的密码系统中，映射f可以预期有

5问题相互关系和 一个随机选择的映射的特征(i。e.， f (X$_i$是

陷阱门是独立的。在这种情况下，如果X是一致选择的和

从所有可能的Y和连续的选择中一致地选择

键和消息的数量都是相同的（X和Y），

在本节中，我们将展示一些密码，然后合成的Y有k + 1逆的概率是目前提出的问题，可以简化为其他问题，因此
根据难度来定义一个松散的顺序。我们还介绍了
产生更困难的问题，陷阱门。

在第二节中，我们展示了一个密码系统的扩展
对于隐私，也可以用于提供身份验证，以对抗
第三方伪造。这样的系统可以用来创建其他的系统
还有加密对象。

一种对已知明文机安全的密码系统
*攻击可以用来产生一个单向的函数。***图3：作为单向函数使用的安全密码系统。**

约e— 1/k!对于k=0,1,2,3，。...这是泊松生活并不比任何人好。情况精确分布，平均入=为1，移动1个单位。预期的类似于一个组合锁。因此，任何知道逆数的人只有2。虽然f密码系统可以在几秒钟内完成，即使是一个熟练的锁匠也会更退化，但一个好的密码系统不会需要太多几个小时来完成。然而，如果他忘记了从那时起的组合生成，钥匙就没有得到很好的使用。因此，他没有任何优势。

worst c a se, i f f (*X)* =*Y* 0f 大约 我 *Y* 0我们
and en c i ph e r m e nt of *P0* w 古尔德 不 d e 悬而未决
Whi l e we ar e 我们ua lly 在 terest edi n

h ave $S_K(P_0) = C_0$,
o n the key at all!

A trap-door cryptosystemcanbeusedtoproduceapublic key distribution system.

functions whose domain

而且范围的大小相当，也有例外。在对于A和B建立一个公共私钥，选择a在上一节中，我们需要一个单向函数随机映射长键，并发送一个任意的明文-密码对字符串到更短的。通过使用一个块密码，谁的到B。B，他公开了陷阱门密码，但保持密钥长度大于块大小，这些功能可以是陷阱门信息秘密使用明文密码对

使用上述技术获得的。来解决钥匙。A和B现在有了一个共同的密钥。

埃文斯等人。[10]对这个问题有不同的方法，目前几乎没有证据表明存在从块密码构造单向函数。而不是门密码。然而，它们是一种明显的可能性，而且应该如此

而不是选择一个固定的P0 作为输入，他们使用的函数被记住时，接受一个密码系统从一个可能的

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

这是一种很有吸引力的方法，因为这种形式的方程通常很难解决，即使S族相对简单。然而，这种增加的复杂性，破坏了系统S在已知的明文攻击下的安全性和单向关闭之间的等价性。

另一种关系已经在第四节中显示出来。

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建成为一个比单向身份验证更困难的问题。类似地，公钥加密系统可以作为公钥分发系统，但不能相反使用。

由于在公钥密码系统中，使用E和D的一般系统必须是公共的，因此指定E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套活门单向功能。*这些函数并不是单向的，因为简单计算的逆存在。但给定一个正向函数的算法，在计算上找到一个简单计算的逆是不可行的。*只有通过了解某些陷阱门的信息(e*。g.，产生E-D对的随机位串)可以很容易地找到容易计算的逆。

陷阱门在前一段中已经以陷阱门单向功能的形式出现过，但也存在其他的变化。陷阱门密码是一种强烈抵制任何不拥有陷阱门信息的人的密码分析的密码

对手[12]。

根据定义，我们将要求一个陷阱门问题是一个设计陷阱门是在计算上可行的问题。*这就为第三种类型的实体留下了我们将使用前缀“准”的空间。例如，一个拟单向函数不是单向的，因为存在一个很容易计算的逆。*然而，即使对设计者来说，在计算上找到容易计算的逆也是不可行的。因此，准单向函数可以用来代替单向函数，而基本上没有安全损失。

将陷阱门信息丢失给陷阱门单向函数，使其成为准单向函数，但也可能存在这样无法获得的单向函数。

拟单向函数被排除在单向函数类之外，这完全是一个定义问题。人们可以讨论广义上或严格意义上的单向函数。

类似地，准安全密码是一种能够成功抵抗密码分析的密码，即使是它的设计者，但却存在一种计算效率高的密码分析算法（当然在计算上是不可能找到的）。同样，从实际的角度来看，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，公钥密码系统暗示着陷阱门单向功能的存在。然而，反之亦然，事实并非如此。一个陷阱门单向函数要想作为公钥密码系统使用，它必须是可逆的(i。e.，有一个独特的逆。)

6计算复杂度

用于密码的设计。这使得设计师的密码学不同于所有其他领域的努力，在打破系统后，他已经把它卖给客户，但错误地缓解，它的要求可能似乎得到满足。以保持他作为一个安全系统的构建者的声誉。简单的转换将把一个清晰的文本转换为一个明显重要的注意，它不是更聪明或知识，毫无意义的混乱。批评家希望声称密码学允许设计者做其他人想要的可能通过密码分析恢复的事情，但他就不能面对。如果他失去了活板门的信息，他将用一个艰苦的演示，如果他要证明他的观点

查看正确。然而，经验表明，很少有系统能够抵抗技术娴熟的密码分析人员的协同攻击，而且许多据称是安全的系统随后被破坏了。

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16世纪和17世纪，数学论证经常被用来论证密码学方法的力量，通常依赖于计数方法来显示天文数字和可能的密钥。虽然这个问题很难用这些简单的方法来解决，但即使是著名的异教教徒卡尔达诺也落入了这个陷阱[2，p]。145].由于那些曾被这样论证的系统被反复打破，为系统的安全性提供数学证明的概念就会声名狼藉，并被通过加密分析攻击的认证所取代。

然而，在本世纪内，钟摆已经开始重新向另一个方向摆动。在一篇与信息论的诞生密切相关的论文中，香农指出，自20年代末以来就一直在使用的一次性衬垫系统提供了“完全保密”（一种无条件安全的总和）。香农研究的可能安全术语依赖于它们的长度随使用长度线性增长，或者是完美的源编码，因此对于大多数目的来说过于方便。我们注意到，无论是公共密码系统还是单向认证系统都不能无条件地安全，因为公共信息总是在有限集的成员之间唯一地确定秘密信息。因此，通过无限的计算，问题可以通过一个直接的触摸来解决。

在过去的十年里，有两个密切相关的解释，致力于研究计算计算复杂度理论的成本和对数的分析。前者将计算中已知的问题按难度划分为大类，而后者则专注于寻找更好的算法和利用它们所消耗的资源。在对复杂性理论的简要讨论之后，我们将研究它在密码学中的应用，特别是对单向函数的分析。

如果该函数可以由确定性制造机在其输入长度的多项式函数限定的时间内计算，则称为复杂度类P（多项式）。人们可能会认为这是一类容易计算的函数，但更准确地说，一个不在这个类中的函数必须至少有一些输入很难计算。存在已知不属于P类的问题[13,405-425]。

在工程中出现了许多问题，它们不能在多项式的时间内用任何一项已知的单一问题来解决，除非它们运行在具有适当并行度的计算机上。这些问题可能属于也不属于类P，但属于“不确定性”计算机上可解多项式时间问题的类NP（不确定性，多项式）。e.，具有无限的并行程度)。清楚地

该NP包括类P，在复杂性理论中最大的开放部分之一是该类NP是否直接更大。 在已知的在NP时间内可解决的、在P时间内不可解决的问题中，有推销问题、位置演算的可满足性问题、背包问题、图环问题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阻止了人们在P时间找到这些问题的解决办法。因此，我们坚信这些问题中至少有一个不在类P中，因此类NP严格更大。

Karp已经确定了NP问题的一个子类，称为NP完备问题，其性质是如果其中任何一个在P中，那么所有的NP问题都在P中。Karp列出了21个NP完整的问题，包括上面[14]中提到的所有问题。

虽然NP完全问题显示了密码使用的前景，但目前对其困难的理解只包括最坏的情况分析。出于密码学的目的，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下的计算时间作为我们的复杂度度量，那么目前的NP完全问题之间的等价性证明就不再有效。这就提出了几个有趣的研究课题。信息理论家所熟悉的集合和典型性概念可以发挥着明显的作用。

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。

一个可以在P时间内进行加密和解密操作的系统的密码分析难度不能大于NP。

要了解这一点，请观察任何密码分析问题都可以通过从一个有限的集合中选择一个密钥、逆像等来解决。不确定地选择这个键，并在P时间内验证它是正确的。如果有M个可能的键可供选择，则必须使用M倍并行性。例如，在一个已知的明文攻击中，明文同时在每个密钥下进行加密，并与密码进行比较。由于假设加密只需要P个时间，所以密码分析只需要NP个时间。

我们还观察到一般的密码解析问题是NP完备的。这源于我们对密码学问题的定义的广度。接下来将讨论一个具有NP完全逆的单向函数。

密码学可以直接从NP复杂性的理论中提取，通过检查NP完全问题可以如何适应密码学的使用。特别地，有一个NP完全问题，称为背包问题，它可以很容易地构造一个单向函数。设Y = f (x) = a。..其中a是n个整数的已知向量$1,a_2$，...， a_n)，x是一个二进制的n向量。y的计算很简单，最多包含n个整数的和。这个

反f问题称为背包问题，计算可以用手工或简单进行
需要找到{a的一个子集$_i$它之和为y。类似幻灯片规则的设备。第二次世界大战后的一段时期

详尽搜索所有2^n子集呈指数增长，我看到了一个革命性趋势的开始，现在在n大于100左右的计算上是不可行的。关怀即将实现。然而，在选择加密参数时，必须使用特殊用途的机器。直到开发通用数字化问题，以确保捷径不可能。然而，例如tal硬件，密码学仅限于操作，如果n个= 100和每个a$_i$是32位长，y最多是39位，可以用简单的机电系统长来执行，而f是高度退化的；平均只需要项目。数字计算机的发展已经使它从
2^{38}试图找到一个解决方案。更琐碎的是，如果a$_i$=的限制计算与齿轮，并允许了$2^{i} - 1$那么逆变f等价于根据y的纯加密寻找更好的二值分解加密方法。图形标准。

这个例子证明了巨大的希望和失败的无数次试图证明的合理性，当代复杂性理论的重大缺点。对密码系统的数学证明导致的理论只告诉我们，背包问题可能是范式认证的密码分析攻击设置的困难在最坏的情况下。没有迹象表明它的困难。在上个世纪。虽然有些是对任何特定数组的通用的。然而，似乎选择规则已经发展出来，这有助于设计师避免{a$_i$从{012开始一致。...2^{n-1}}结果在一个难题上有明显的弱点，最终的测试是对系统的攻击
概率为1为n→w。由熟练的密码分析师在最有利的条件下进行分析

另一个潜在的单向函数，对分析感兴趣(e。g.，一个被选择的明文攻击)。计算机算法的发展，是指数mod q，这是首次提出了数学理论的算法教授。斯坦福大学的约翰·吉尔。如何解决这些函数的单向估计的难题已经在破解密码系统的计算困难中进行了讨论。
第三节。因此，数学证明的位置可能会原点

并重新成为认证的最佳方法。
我们在密码学的历史上注意到的最后一个特征是-
7历史透视摄影是业余和专业加密货币之间的划分

tographers.生产密码分析技术一直是
虽然起初公钥系统和单向身份验证的专业人员，但创新，部分系统建议在本文似乎是重要的新类型的加密系统的设计，过去密码的发展，可以认为他们主要来自业余爱好者。托马斯·杰斐逊，作为密码学业余爱好者发展趋势的自然产物，发明了一个仍在使用的系统
追溯到几百年前。在第二次世界大战中使用。而最值得注意的是

保密是密码学的核心。在早期的密码学，二十世纪的密码系统，转子，然而，有一个混淆什么是保留机器，是由四个独立的人同时发明的，秘密。密码系统，如凯撒密码(其中每个是所有的业余爱好者[2，pp。415， 420， 422 - 424].我们希望这封信能被三个地方取代，所以A能激励其他人在这个迷人的领域工作，参与D，B到E，等等。)为了他们的安全，最近几乎整个加密过程的秘密。在政府垄断企业的发明之后。
电报[2，p。，即一般制度之间的区别
而一个特定的密钥则允许对一般系统进行补偿
例如，通过盗窃一个加密设备，没有**参考文献**
在新密钥中隐藏的妥协的未来信息。这个
原则由Kerchoffs [2，p。他在[1] R中道。“不安全的安全沟通
1881年，密码系统的妥协应该通道，“提交给ACM的通信。
不给记者造成任何不便。约1960年，[2] D．*卡恩，密码破解者，秘密写作的故事。*
密码系统被认为是强大的纽约：麦克米伦，1967年。

en ough t ore司st a known pla英特尔xt cryptanalytic attack, thereby e李min a提ng th eburden of keep 在g old messages secret. Each 这些发展减少了系统的部分 “提交给IEEE翻译。
crecy sys-
Oct. 1949
non theory
[3]C. E. Shannon, “Co mmu nic a tion theo ry of se tems,.” *Bell Syst Tec h. J* , vol 28, pp. 65 6–715 ,
[4]M. E Hellman, “An ex tension of the Shan

哪些必须被公众知识，消除*通知。理论，9月。*1975.
诸如改写外交派遣这样枯燥乏味的权宜之计[5 } W . DiffieM。E.“多用户密码学”
在他们被出示之前。公钥系统是一个很自然的系统技术，提出在国家计算机连接-
继续保持这种减少保密性的趋势。1976年，1976年6月7-10日，纽约。

在本世纪之前，密码系统仅限于[6] D。*《计算机编程的艺术》，第1卷。2，*

半数值算法。阅读，马萨诸塞州。: AddisonWesley, 1969.
[7]———，计算机编程的艺术，Vol。3、排序-正在搜索。阅读，马萨诸塞州。当前位置地址：艾迪生-韦斯利，1973年。
[8] S.Pohlig和M。E.“在GF (p)中计算算法的改进算法及其密码意义”，提交给IEEE Trans。*通知。理论。*
[9] M.V.*威尔克斯，分时计算机系统*。纽约：爱思唯尔，1972年。
[10] A.小埃文斯。坎特罗维茨和E。魏斯，“用户身份验证系统不需要在计算机中保密”，通信，卷。17, pp.437-442年8月。1974.
[11] G.B.珀迪，“一个高安全的登录过程”，ACM的通信，vol。17, pp.442-445年8月。1974.
[12] W.DiffieM。E.赫尔曼，“国家统计局数据加密标准的密码分析”，提交给计算机公司，1976年5月。
[13] A.V.Aho, J.E.霍普克罗夫特和J。D.*计算机算法的设计与分析*。阅读，马。：艾迪生-韦斯利，1974年。
[14] R.M.“组合问题之间的可约性》，《计算机计算的复杂性》。R.E.米勒和J。撒切尔，Eds。纽约：全会，1972年，页。85 - 104.