可证明安全性理论与方法研究*

冯登国+

(信息安全国家重点实验室(中国科学院 软件研究所),北京 100080)

Research on Theory and Approach of Provable Security

FENG Deng-Guo+

(State Key Laboratory of Information Security (Institute of Software, The Chinese Academy of Sciences), Beijing 100080, China)

+ Corresponding author: Phn: +86-10-62658643, Fax: +86-10-62520469, E-mail: fdg@263.net, http://www.is.iscas.ac.cn

Received 2004-07-06; Accepted 2005-08-24

Feng DG. Research on theory and approach of provable security. *Journal of Software*, 2005,16(10):1743−1756.
DOI: 10.1360/jos161743

Abstract: This paper presents a survey on the theory of provable security and its applications to the design and analysis of security protocols. It clarifies what the provable security is, explains some basic notions involved in the theory of provable security and illustrates the basic idea of random oracle model. It also reviews the development and advances of provably secure public-key encryption and digital signature schemes, in the random oracle model or the standard model, as well as the applications of provable security to the design and analysis of session-key distribution protocols and their advances.

Key words: provable security; cryptosystem; security protocol; random oracle model; standard model

摘 要: 论述了可证明安全性理论在安全方案与安全协议的设计与分析中的应用,内容主要包括:什么是可证明安全性,可证明安全性理论涉及到的一些基本概念,RO(random oracle)模型方法论的基本思想及其在公钥加密和数字签名等方案中的应用研究进展,标准模型下可证明安全性理论在公钥加密和数字签名等方案中的应用研究进展,以及可证明安全性理论在会话密钥分配协议的设计与分析中的应用研究进展.

关键词: 可证明安全性;密码方案;安全协议;RO(random oracle)模型;标准模型

中图法分类号: TP309 文献标识码: A

目前多数安全协议的设计现状是:(1) 提出一种安全协议后,基于某种假想给出其安全性论断;如果该协议在很长时间,如10年仍不能被破译,大家就广泛接受其安全性论断;(2) 一段时间后可能发现某些安全漏洞,于是对协议再作必要的改动,然后继续使用;这一过程可能周而复始.这样的设计方法存在以下问题:(1) 新的分析技术的提出时间是不确定的,在任何时候都有可能提出新的分析技术;(2) 这种做法使我们很难确信协议的安全性,反反复复的修补更增加了人们对安全性的担心,也增加了实现代价或成本.

那么有什么解决办法呢?可证明安全性理论就是针对上述问题而提出的一种解决方案(当然,并非是唯一

* Supported by the National Grand Fundamental Research 973 Program of China under Grant No.G1999035802 (国家重点基础研究发展规划(973)); the National Natural Science Foundation of China under Grant No.60273027 (国家自然科学基金)

作者简介: 冯登国(1965−),男,陕西靖边人,博士,研究员,博士生导师,主要研究领域为网络与信息安全.

的解决方案).可证明安全性是指,安全方案或协议的安全性可以被“证明”,但用“证明”一词并不十分恰当,甚至有些误导[1].一般而言,可证明安全性是指这样一种“归约”方法:首先确定安全方案或协议的安全目标.例如,加密方案的安全目标是确保信息的机密性,签名方案的安全目标是确保签名的不可伪造性;然后根据敌手的能力构建一个形式的敌手模型,并且定义它对安全方案或协议的安全性“意味”着什么,对某个基于“极微本原(atomic primitives,是指安全方案或协议的最基本组成构件或模块,例如某个基础密码算法或数学难题等)”的特定方案或协议,基于以上形式化的模型去分析它,“归约”论断是基本工具;最后指出(如果能成功),挫败方案或协议的唯一方法就是破译或解决“极微本原”.换句话讲,对协议的直接分析是不必要的,因为你对协议的任何分析结果都是对极微本原的安全性的分析.可见,称“归约安全”也许比“可证明安全”更恰当.实际上,可证明安全性理论是在一定的敌手模型下证明了安全方案或协议能够达到特定的安全目标,因此,定义合适的安全目标、建立适当的敌手模型是我们讨论可证明安全性的前提条件.

可证明安全性理论的应用价值是显而易见的:我们可以把主要精力集中在“极微本原”的研究上,这是一种古老的、基础性的、带有艺术色彩的研究工作;另一方面,如果你相信极微本原的安全性,不必进一步分析协议即可相信其安全性.

综上所述,可证明安全性理论本质上是一种公理化的研究方法,其最基础的假设或“公理”是:“好”的极微本原存在.安全方案设计难题一般分为两类:一类是极微本原不可靠造成方案不安全(如用背包问题构造加密方案);另一类是,即使极微本原可靠,安全方案本身也不安全(如 DES-ECB 等).后一种情况更为普遍,是可证明安全性理论的主要研究范围.

必须说明的是,可证明安全性理论也存在一定的局限性:首先必须注意模型规划,即注意所建立的模型都涵盖了哪些攻击.显然,一些基于物理手段的攻击都不包含在内,但这并不意味着可证明安全性的方案就一定不能抵抗这类攻击,而是说未证明可以抵抗这类攻击;其次,即使应用具有可证明安全性的方案,也可能有多种方式破坏安全性:有时证明了安全性,但问题可能是错误的,也可能应用了错误的模型或者协议被错误操作,甚至软件本身可能有“Bugs”.

另一个需要注意的问题是基础假设的选取:可证明安全性是以某一假设为基础的,因此一旦该假设靠不住,安全性证明也就没有意义了(当然,不一定意味着可构造对方案的攻击实例);选取基础假设的原则就是“越弱越好”,通常称弱假设为标准假设.基础假设的强弱是比较不同安全方案的重要尺度之一.

上述定义较为抽象,下面以 RSA 为例加以说明.

给定某个基于 RSA 的协议 P,如果设计者或分析者给出了从 RSA 单向函数到 P 安全性的归约,那么 P 具有以下转换性质:对于任何声称破译 P 的敌手(程序)A,以 A 为“转换算法”的输入,必然导致一个协议 Q,Q 可被证明破译 RSA.结论是:只要你不相信 RSA 是可破译的,那么上述的 Q 就不存在,因而 P 是安全的.

对可证明安全性的精确形式化有多种形式,一般是在计算复杂性理论框架下加以讨论,如主要考虑“概率多项式时间(PPT)”的敌手 A 和转换算法,以及“可忽略”的成功概率.这是一种“渐近”观点,有着广泛的适用范围.具体内容可参见 Goldreich 的研究综述[2].

1.1 基本概念

本质上,可证明安全性理论的主要研究途径是规划安全方案或协议的形式化安全模型,不同的安全方案或协议会导致不同的安全模型,而这些安全模型大多基于一些很基本的密码学概念.因此对一些最基本的密码学概念(如加密、签名及其安全性定义等)给予精确的形式化定义是可证明安全性理论的基础组成部分,有助于消除自然语言的语义二义性.下面分别介绍数字签名方案和公钥加密方案的安全模型.

定义 **1**(数字签名方案). 一个数字签名方案由以下 3 种算法组成:

(1) 密钥生成算法 K.对于输入 1^k,K 产生一对匹配值(k_p,k_s),分别称为公钥和私钥,K 可以是概率算法.k 称为安全参数,密钥等因素的规模都依赖于 k.

(2) 签名算法Σ.给定消息 m 和(k_p,k_s),Σ产生签名σ,Σ可以是概率算法.

(3) 验证算法 V.给定签名σ和消息 m 以及公钥 k_p,V 检验σ是否是 m 的对应于公钥 k_p 的合法签名,通常情况

下,V 是确定性算法.

对于任一数字签名方案(K,Σ,V),敌手 A 的模型如下:

A 的目标有如下 3 个:揭示签名者私钥(完全破译);构造成功率高的伪签名算法(通用伪造);提供一个新的消息-签名对(存在性伪造).

存在性伪造一般并不危及安全,因为输出消息很可能无意义,但这样的方案本身不能确保签名方的身份,例如不能用来确认伪随机元素(如密钥),也不能用来支持非否认.

A 的两类攻击:未知消息攻击和已知消息攻击.后一种情况中最强的攻击是"适应性选择消息攻击",即 A 可以向签名方询问对任何消息的签名(当然不能询问欲伪造消息的签名,这是一类自明的约定,后文不再注释),因而可能根据以前的答案适应性地修改随后的询问.

定义 **2**(数字签名方案在适应性选择消息攻击下的安全性). 对任一数字签名方案(K,Σ,V),如果敌手 A 的攻击成功概率

$$Succ_A=\Pr[(k_p,k_s)\leftarrow K(1^k),(m,\sigma)\leftarrow A^{\Sigma_{k_s}}(k_p):V(k_p,m,\sigma)=1]$$

是可忽略的,则称该方案能够抵抗适应性选择消息攻击.这里,A 可以获得签名 Oracle Σ_{k_s} (实际上是一个"黑盒"),这模拟了如上所说的"适应性选择消息询问",而且要求(m,σ)没有询问过 Σ_{k_s}.

定义 **3**(公钥加密方案). 一个公钥加密方案由以下 3 种算法组成:

(1) 密钥生成算法 K.对于输入 1^k,K 产生一对匹配值(k_p,k_s),分别称为公钥、私钥,K 是概率算法.

(2) 加密算法 E.给定消息 m 以及公钥 k_p,E 产生 m 对应的密文 C.E 可以是概率算法,这时记为 $E(k_p,m;r)$,r 表示随机输入.

(3) 解密算法 D.给定密文 C 及私钥 k_s,D 产生 C 对应的明文 m,一般是确定性算法.

一般而言,加密方案的安全目标是单向性(one-wayness,简称 OW)的:在不知私钥的情况下,敌手 A 在概率空间 $M\times\Omega$上成功地对 E 求逆的概率是可忽略的(这里,M 是消息空间,Ω是加密方案的随机掷硬币空间),亦即概率

$$Succ_A=\Pr[(k_p,k_s)\leftarrow K(1^k):A(k_p,E(k_p,m;r))=m]$$

是可忽略的.

然而,许多应用要求具有更强的安全性.

定义 **4**(多项式安全/密文不可区分). 对任一公钥加密方案(K,E,D),如果满足

$$adv_A=2\times\Pr[(k_p,k_s)\leftarrow K(1^k),(m_0,m_1,s)\leftarrow A_1(k_p),c=E(k_p,m_b;r):A_2(m_0,m_1,s,c)=b]-1$$

是可忽略的,则称该方案是多项式安全的或密文不可区分的.这里,敌手 $A=(A_1,A_2)$是一个 2 阶段攻击者(都是 PPT 算法),概率取于(b,r)之上.

上述定义形式化了如下性质:敌手了解明文的某些信息(可任选一对消息,其中一个被加密),但它不能从密文得到除明文长度之外的任何信息.

敌手的几种攻击类型(相当于敌手拥有的 Oracle 数量及性质):

(1) CPA(选择明文攻击),该攻击在公钥方案中显然是平凡的;

(2) PCA(明文校验攻击),敌手获得明文校验 Oracle,用以回答关于任一输入对(m,c)是否为对应明密对的询问;

(3) CCA(选择密文攻击),除了获得加密 Oracle 以外,敌手还获得解密 Oracle,即对于任何询问的密文(除了应答密文),Oracle 都给以相应的明文作为回答.这是最强的攻击(根据是否适应性选择密文,还可以细分为 CCA1 和 CCA2).

对应以上攻击条件的相应安全性定义,均可用类似于定义 4 的方法给出,区别仅在于敌手获得的 Oracle 数量和性质不一样.对称密码方案的安全性可类似定义.

2 RO 模型方法论及其相关研究结果

20 世纪 80 年代初,Goldwasser,Micali 和 Rivest 等人首先比较系统地阐述了可证明安全性这一思想,并给出了具有可证明安全性的加密和签名方案[3,4].然而,以上方案的可证明安全性是以严重牺牲效率为代价的,因此以上方案虽然在理论上具有重要意义,但不实用,这种情况严重制约了这一领域的发展.直到 20 世纪 90 年代中期出现了“面向实际的可证明安全性(practice-oriented provable-security)”的概念,特别是 Bellare 和 Rogaway 提出了著名的 RO(random oracle,随机预言)模型方法论[5],才使得情况大为改观:过去仅作为纯理论研究的可证明安全性理论,迅速在实际应用领域取得了重大进展,一大批快捷有效的安全方案相继提出;同时还产生了另一个重要概念:“具体安全性(concrete security or exact security)”,其意义在于,我们不再仅仅满足于安全性的渐近度量,而是可以确切地得到较准确的安全度量.面向实际的可证明安全性理论取得了巨大的成功,已被国际学术界和产业界广为接受;但 Canetti 和 Goldreich 对此持有异议[6],并坚持仍在标准模型(standard model)中考虑安全性.

Canetti 和 Goldreich 认为:密码方案在 RO 模型中的安全性和通过“hash 函数实现”的安全性之间无必然的因果关系;具体说来,存在这样的实际签名方案和加密方案,它们在 RO 模型中是安全的,但任何具体实现都是不安全的.这实际上是提出了一个反例.不过,Goldreich 也认为,应该明确 RO 模型方法论并不能作为实际方案安全的绝对证据,但该方法论仍是有意义的,如可以作为一种基本测试——任何实际方案通过这种安全测试是必要的,RO 模型方法论至少可以排除很多不安全的设计,虽然并非完备的.Canetti 则进一步指出,RO 模型方法论虽然存在以上缺点,但它可用于设计简单而有效的协议——可以抵抗许多未知攻击;更重要的是,其基本思想可以用来设计某些安全的理想系统.

Pointcheval 等人则认为[7],目前还没有人能提出令人信服的关于 RO 模型实际合法性的反例.文献[6]的反例仅仅是一种理论上的反例,是针对实际目的的“明显错误设计”;RO 模型已经被广为接受,并被认为是度量实际安全级别的一种很好的手段;即使并未提供一个正规的安全性证明(像标准模型那样),但在其“安全性论断”(hash 函数没有弱点)下,RO 模型中的证明确保了整个方案的安全性.更确切些,RO 模型可视为对敌手能力的某种限制——敌手的攻击是不考虑任何特殊 hash 函数实例的一般攻击,而且如果假定存在某些防窜扰设备(如 Smart Cards),则 RO 模型等价于标准模型,这时只要求伪随机函数存在[2].最重要的是,仅就实现效率这一点,RO 模型中的可证明安全性的方案就远远优于那些能够提供标准安全性证明的方案,仅此一点就可以从实际应用中排除当前所有“在标准模型中具有可证明安全性”的方案.事实上,一些有代表性的、有效的标准解决方案,如文献[3,4]中的方案,过于复杂且代价昂贵,归约的复杂性使得难以确定实际安全参数,其有效性也只是相对于过去的标准方案而言.

但可以肯定的是,迄今为止,RO 模型方法论是可证明安全性理论最成功的实际应用,其现状是:几乎所有国际安全标准体系都要求提供至少在 RO 模型中可证明安全性的设计,而当前可证明安全性的方案也大都基于 RO 模型.

2.1 RO模型介绍

文献[5]中提出如下观点:假定各方共同拥有一个公开的 Random Oracle,就可以在密码理论和应用之间架起一座“桥梁”.具体办法是,当设计一个协议 P 时,首先在 RO 模型(可看成是一个理想模拟环境)中证明 P^R 的正确性,然后在实际方案中用“适当选择”的函数 h 取代该 Oracle(潜在论断是理想模拟环境和现实环境在敌手看来是多项式时间计算不可区分的).一般来说,这样设计出来的协议可以和当前协议的实现效率相当.

必须指出,这并非是严格意义上的可证明安全性,因为安全性证明仅在 RO 模型中成立,随后的“取代”过程本质上是一种推测:RO 模型中的安全特性可以在标准模型中得以保持.

假设我们提出一个协议问题 Π(这个问题和 h 函数“独立”),要设计一个安全协议 P 解决该问题,可按如下步骤执行:

(1) 建立 Π 在 RO 模型中的形式定义,RO 模型中各方(包括敌手)共享随机 Oracle R;

(2) 在 RO 模型中设计一个解决问题 Π 的有效协议 P;

(3) 证明 P 满足 Π 的定义;

(4) 在实际应用中用函数 h 取代 R.

严格说来,h 不可能真的“像”随机函数:首先,其描述较短;其次,所谓的随机 Oracle 即 hash 函数对每一个新的询问产生一个随机值作为回答(如果问相同的询问 2 次,回答仍相同),这也是和随机函数的一个微小区别.但这并未改变上述方法论的成功,因为只要求在敌手看来“像”随机函数.此外,h 函数“独立”于Π也是至关重要的(否则可能不安全,可构造反例).

一般来说,函数 h 至少要满足以下基本要求:设计上足够保守,能够抵抗各种已知攻击;不会暴露某些相关数学“结构”.文献[5]指出,选择 h 并不需要太麻烦,一个适当选择(但并不需过分苛求)的 hash 函数就是如上 h 函数的一个很好的选择.

RO 方法论也易于推广到基于对称密码本原的协议/方案研究,如 CBC-MAC,虽然没有 hash 函数,但把一个恰当选择的分组密码(如 DES)视为随机函数.

2.2 归约论断和具体安全性

归约论断是可证明安全性理论的最基本工具或推理方法,简单说就是把一个复杂的协议安全性问题归结为某一个或几个难题(如大数分解或求解离散对数等).在 RO 模型中的归约论断一般表现为:首先形式化定义方案的安全性,假设 PPT 敌手能够以不可忽略的概率破坏协议的安全性(如伪造签名);然后模仿者 S(就是设计者或分析者)为敌手提供一个与实际环境不可区分的模拟环境(RO 模型),回答敌手的所有 Oracle 询问(模拟敌手能得到的所有攻击条件);最后利用敌手的攻击结果(如一个存在性的伪造签名)设法解决基础难题.如果把 RO 模型换成现实模型就得到标准安全性证明.

RO 归约论断的一个显著优点是能够提供具体安全性结果.具体地说就是,试图显式地得到安全性的数量特征,这一过程称为“具体安全性处理(concrete or exact treatment of security)”,与前面提到的“渐近”观点有明显区别.其处理结果一般表述为如下形式(举例):“如果 DES(本原)可以抵抗这样条件的攻击,即敌手至多获得 2^{36} 个明密对,那么我们的协议就可以抵抗一个能执行 t 步操作的敌手发动的攻击,t 值如下…”这样,协议设计者就能够确切地知道具体获得了多少安全保证,不必再笼统地说协议是否安全.

例 1:文献[8]中研究了 CBC MAC 的安全特征,结论是:对任意一个运行时间至多为 t、至多见过 q 个正确 MAC 值的敌手,成功模仿一个新消息的 MAC 值的概率至多为$\varepsilon+(3q^2n^2+l)/2$.这里,$l$ 是基础密码的分组长度,n 是明文消息总数,ε是检测到密码偏离随机行为的概率(在 $O(nql)$时间内).

具体安全性处理的一个重要目标就是,在把一个基础极微本原转化成相应协议时,尽可能多地保持极微本原的强度.这表现为要求“紧”的归约方法,因为一个“松”的归约意味着要求采用更长的安全参数,从而降低了效率.

2.3 基于RO模型方法论的代表性研究结果

2.3.1 公钥加密方案

第 1 节的概念推广到 RO 模型,即可得到 RO 模型中的公钥加密方案的定义.公钥加密方案可以通过 PPT 生成器 g 来规定:以安全参数 1^k 为输入,输出一对概率算法(E,D),分别称为加、解密算法,D 保密,运行时间以 g 的运行时间为界.加密: $y \leftarrow E^R(x)$,解密: $x \leftarrow D^R(y)$.

像定义 4 一样,称该方案在 RO 模型中是 CPA 多项式安全的,如果对任意的 CP-敌手(选择明文敌手)(F,A_1),满足

$$\Pr[R \leftarrow 2^{\infty};(E,D) \leftarrow g(1^k);(m_0,m_1) \leftarrow F^R(E);b \leftarrow \{0,1\};$$
$$\alpha \leftarrow E^R(m_b): A_1^R(E,m_1,\alpha)=b] \le 1/2+\mu(n).$$

这里,R 表示一般的 Oracle,是从{0,1}*到{0,1}$^\infty$的函数,2^∞表示所有 Oracle 的集合,“∞”并非真的无限,只是避免提问“足够长是多长”这类问题,$\mu(n)$是可忽略函数.

CCA 安全性:这里的敌手 A 称为 RS-敌手,即有非一致多项式算法 $A=(F,A_1)$,各自获得一个 Oracle R 及一个解密 Oracle 的黑盒实现 D^R;F 的任务就是提出一对明文 m_0,m_1,A_1 被随机给予其中一个的密文α,则只要不允许向解密 Oracle D^R 询问α(因为禁止提出与最终论断等价的询问),A_1 就不可能以不可忽略优势猜中是哪一个

明文.

称 g 在 RO 模型中安全抗 CCA 攻击,如果对任意 RS-敌手(F,A_1),满足:

$$\Pr[R \leftarrow 2^{\infty};(E,D) \leftarrow g(1^k);(m_0,m_1) \leftarrow F^{R,D^R}(E);b \leftarrow \{0,1\};$$
$$\alpha \leftarrow E^R(m_b): A_1^{R,D^R}(E,m_0,m_1,\alpha) = b] \le 1/2 + \mu(n).$$

Bellare 等人在文献[5]中提出了一个在 RO 模型中安全抗 CCA 攻击的方案,由于归约并不紧,应用意义并不大,但其设计思想很好地体现了 RO 方法论的特点.

Bellare 等人把以上思想作了进一步改进,在 1994 年提出了著名的公钥加密填充方案 OAEP[9],可证明是抗 CCA2 攻击安全的,目前该方案已成为新一代 RSA 加密标准.其基本组成是:核心组件是一个 Padding 函数,即 $OAEP^{G,H}(x,r)=x\oplus G(r)\|r\oplus H(x\oplus G(r))$.这里,$x$ 是被加密消息,r 是随机输入;加密算法为 $E^{G,H}(x)=f(OAEP^{G,H}(x,r))$.这里,$f$ 是陷门置换(如 RSA 函数).基本设想是构造一个具有良好随机性的"遮掩函数"隐蔽明文的统计特性.

2.3.2 数字签名方案

Bellare 等人在文献[5]中也给出了一种具有可证明安全性的签名方案.该签名方案要求陷门置换 f 具有"均匀分布"的特点,而标准 RSA 置换不具有这个性质,因此基于 RSA 无法设计该类方案.文献[10]中提出了一种基于 RSA 的签名方案:概率签名方案 PSS,目前有望成为 RSA 签名标准.PSS 引入了概率机制,有更好的安全界.该方案不仅可证明其安全性,而且相应的归约是很紧的,一个敌手伪造签名的能力和对 RSA 求逆的能力相当.总之,安全性和分解整数的困难性紧密相关.稍作改进,也可以具有消息恢复性质.

目前,其他可证明安全性的签名方案大都是基于识别协议的签名方案,这不是偶然的,前面我们提到 Fiat 和 Shamir 曾经应用 RO 假设试图构造一个安全性和因子分解一样困难的签名方案[11],并证明了其与识别协议的等价性.例如,文献[12]中的主要工作是:对基于 Fiat-Shamir 识别协议的签名方案[11]作了具体安全性分析,通过交换应答和承诺的顺序改进设计了一类新的 Fiat-Shamir 类型签名方案(E-swap 签名方案),具有更好的具体安全性.

其他一些进展可参见文献[13–15]等.文献[15]基于计算 Diffie-Hellman(CDH)假设,对一个源于 Schnorr 签名的改进方案 EDL 给出了归约很紧的安全性证明,使得该签名方案得到了业界的广泛重视.另外,值得特别说明的是,文献[13]对于完善 RO 模型方法论具有重大贡献,即提出了以 Folklore 引理为代表的一般安全论断,主要适用于许多基于识别协议的签名方案,特别是证明了迄今为止唯一一个 ElGamal 变形签名方案 MEG 的安全性.基本方法是,Oracle 重放(replay)攻击,即在 RO 模型中实施归约化证明时,重放多项式个不同(但有一定联系)的随机 Oracle(这相当于为敌手提供多个模拟环境),然后敌手若能以不可忽略概率伪造多个签名,设计者或分析者就能根据其内在关联求解基础难题(如 DLP).缺点是归约还不够紧.

3 标准模型中可证明安全性理论研究的一些重要进展

文献[3,4]是满足标准安全性证明的早期有代表性的方案.实际上,前面的结果已经包含了许多这方面的内容,如一些基本概念等,这里我们简要介绍一些近年来的结果.文献[16]研究了数字签名方案中的 hash 函数设计应用问题,降低了对 hash 函数的要求;文献[17]提出了一类基于强 RSA 假设的数字签名方案.其共同之处是都不把 hash 函数形式化为 RO.文献[17]的安全性证明实际上是用满足强计算假设的 hash 函数取代了 RO.

3.1 基于padding函数的RSA签名方案

克服 RSA 签名方案同态缺陷的一种通用解决方案就是先对消息应用 padding 函数作用,然后对结果作解密运算(签名).文献[16]中的主要结果是:基于 padding 函数、对一组消息的 RSA 签名与对多个分组消息的 RSA 签名的安全性等价.而且这里并不要求 hash 函数为 Random Oracle 或具有自由碰撞性质,只是假设存在某个安全的、用于签署固定长度消息的 padding 函数μ;利用它就可以构造一个用于签署任意长度消息的安全 padding 方案.但该文在一般标准安全论断研究方面并未有多少进展.

3.2 没有随机Oracle的安全签名方案(Hash-and-Sign模式)

文献[17]基于强 RSA 假设(即对任意的 RSA 模 $n, s \in Z_n^*$,要在多项式时间内找到一个满足 $r^e=s \bmod n$ 的二元组$(e,r)(e>1)$是不可能的),提出了一种抵抗适应性选择消息攻击的签名方案,仍属于 Hash-and-Sign 结构.密钥和参数说明类似于 RSA,注意公钥为 $n=pq, s \in Z_n^*$.签名算法本身很简单:$e=h(R,M)$,签名σ是 s 模 n 的 e 次根;验证算法略.

在安全性论断研究方面,文献[17]不再把 hash 函数视为 RO,而是把 hash 函数视为具有某些特定性质(如整除难处理性等)的随机函数 $h(R,M)$.这里,R 是随机数.特别之处在于:既充分利用 RO 安全论断的优点,又用一个假想的随机性 Oracle 取代 RO,即假设已知 h 的随机输入因素也对解决强 RSA 难题毫无帮助.文献[17]希望这种"相对模型方法论"能够替代 RO 方法论,但显然其假设过强(虽然文献[17]认为仍是现实的),归约也不紧,更重要的是目前看不到有推广应用的可能,文献[17]也承认这一点.

3.3 Cramer-Shoup加密方案

Cramer 和 Shoup[18]于 1998 年提出了第一个比较实际的标准模型下可证明安全的公钥加密方案,该方案的困难假设是判定性 Diffie-Hellman 问题.由于其安全性归约是在标准的杂凑函数假设(抗碰撞)下得到的,并不依赖于随机预言模型,所以受到了很大的关注.

设 G 是有限域 Z_p^* 的阶为 q 的子群,p,q 为素数,且 $q|p-1$,g_1 和 g_2 是 G 中两个随机的非单位元的元素.设 $x=(x_1,x_2)$, $y=(y_1,y_2)$, $z=(z_1,z_2)$ 表示在 0 和 $q-1$ 之间的数对; $g=(g_1,g_2)$, $u=(u_1,u_2)$ 表示 G 中的元素对;r 是 1 和 $q-1$ 之间的随机数,记 $g^x=(g_1^{x_1},g_2^{x_2})$, $g^{rx}=(g_1^{rx_1},g_2^{rx_2})$.假设 H 是合适的抗碰撞杂凑函数.

用户 Alice 的私钥是 3 对随机产生的数 x,y,z,其公钥由 3 个群元素 $c=g^x$, $d=g^y$, $e=g^z$ 组成.

加密:为了发送消息 $m \in G$,Bob 选择一个随机数 r,令 $u_1=g_1^r$, $u_2=g_2^r$, $w=e^r m$,然后计算 $h=H(u_1,u_2,w)$ 和 $v=c^r d^{rh}$.Bob 把四元组 (u_1,u_2,w,v) 作为密文发送给 Alice.

解密:要解密 (u_1,u_2,w,v),Alice 首先计算 $h=H(u_1,u_2,w)$,然后利用她的私钥计算 u^{x+hy}, 这个结果应该等于 v(因为 $u^{x+hy}=g^{rx+rhy}=c^r d^{rh}$).如果它不等于 v,Alice 就拒绝该消息;如果通过这个检验,Alice 继续进行解密:把 w 除以 u^z,因为 $u^z=g^{rx}=e^r$,而 $w=e^r m$,所以这就是明文 m.

对于 Cramer-Shoup 加密方案,如果存在一个自适应选择密文攻击的敌手能够破坏定义 4 中给出的安全性,那么就可以构造一个算法来求解判定性 Diffie-Hellman 问题.容易看出,Cramer-Shoup 加密方案实际上是 ElGamal 公钥加密方案的一个变型,而后者显然是不能抵抗选择密文攻击的.与 ElGamal 方案相比,Cramer-Shoup 方案的一个重要设计思想,是增加了密文的合法性检验,即在其密文中增加了冗余 v,解密者通过检查 $u^{x+hy}=v$ 来判断密文的合法性.而正是这个密文合法性检验条件,使得解密 Oracle 不能帮助敌手来发动有效的攻击,这也是目前所有的抵抗选择密文攻击的加密方案的重要设计思想之一.

4 会话密钥分配(SDK)协议的可证明安全性研究

通信双方在充满恶意的环境中传送数据,一般需要确保数据的机密性和可认证性.要达到此目的,必须加密和认证被传送的数据,这就需要密钥,而密钥通常需要通过会话密钥分配(SKD)协议来实现.当前最常见的是三方 SKD 协议(可信方参与),因此下文的论述以此为重点.

最早的、最流行的三方密钥分配系统是 1978 年提出的 NS 系统[19],并且有许多具体候选方案.之后的数年,又有 10 多个 SKD 协议出现.但是,似乎所有这些工作都存在这样的"怪圈":提出一个协议;然后是不断地试图破译;不断地修补.实际上,Needham 和 Schroeder 在一开始就提出了警告:这样开发的协议容易有微妙的弱点,且不易在正常操作中检测到,很有必要研究验证协议正确性的技术.作为对这种警告的证实,文献[20]指出了一种 NS 协议的 bug,许多相关协议都有类似的缺陷.如此漫长的攻击历史使得人们终于达成这样的共识:要解决会话密钥分配问题,仅仅由作者给出一个协议、并且作者本人找不到可行的攻击手段是远远不够的.

Burrows,Abadi 和 Needham[21]试图通过使用特定目的的逻辑来解决这个问题,即著名的 BAN 逻辑.形式化

逻辑方法在寻找 Bug 方面很有效,且有些方法可以自动化;但问题在于,一旦抽象的密码运算实例化,“逻辑正确”的证明并不意味着协议本身必然是正确的,也就是说,缺乏严格的安全性证明.

使用可证明安全性理论来研究 SKD 协议最初是由 Bellare 和 Rogaway[5]发起的.与前面的研究相比,不但定义了本原的安全性,还定义了目标安全性,也有助于找到 Bug,更重要的是,SKD 协议的安全性可以得到证明.这项研究在实现基本安全目标方面已经取得了巨大成功,存在的问题是,随着附加越来越多的目标,定义和证明的复杂性大大增加.将来的一个可能方向是把可证明安全性和形式化分析方法结合起来.

SKD 的可证明安全性研究主要包括以下 3 方面内容:

(1) 定义.直接给出安全定义,再证明符合定义;

(2) 可信模型.如两方基于对称密码的模型、三方模型等;

(3) 安全目标.主要有认证、新鲜性、机密性、已知密钥攻击、前向机密性(forward secrecy)以及字典攻击等.

需要说明的是,作为一种较新的安全目标,前向机密性是指,在 SKD 协议结束、当前会话密钥产生后,即使这时敌手得到了任何一方的主密钥,也不能得到以前会话密钥的任何特定信息.

4.1 BR安全模型及其应用

4.1.1 BR 安全模型

Bellare 和 Rogaway 在 1993 年和 1995 年分别给出了两个可证明安全性的两方和三方 SKD 协议[22,23].协议本身很简单,其意义在于首次建立了 SKD 协议的形式安全模型,称为 BR 安全模型.这是一种现实模型,亦即协议只定义在现实世界中,而安全性是通过会话密钥与某随机数的计算不可区分性来定义的(基本方法是使会话密钥和一个敌手易于得到的某伪随机数紧密联系).因为原理类似,我们以三方模型为例作简要介绍.

协议参与方.$I=\{0,1,2,\ldots,N\}$(0 代表可信中心 S),敌手 E.

协议定义.$P=(\Pi,\psi,LL)$,这是一个多项式时间可计算的三元组函数,Π描述诚实方的行为,ψ描述 S 的行为,LL 描述用户主密钥的初始分布,具体说明参见文献[23].

敌手模型.E 控制所有合法方之间的通信(如可以控制协议启动时间、篡改、替换或删除数据等),形式化为一个概率图灵机,具有 Oracle $\Pi_{i,j}^{s}$ 和 $\psi_{i,j}^{s}$, $\Pi_{i,j}^{S}$ 形式化了成员 i 试图和成员 j 协商一个会话密钥的通信实例 S, $\psi_{i,j}^{s}$ 形式化了 S 试图给 i,j 分配会话密钥的通信实例.E 所能发起的攻击形式化为 5 种 Oracle 询问:(*SendPlayer*,*i*,*j*,*s*,*x*);(*SendS*,*i*,*j*,*s*,*x*);(*Reveal*,*i*,*j*,*s*);(*Corrupt*,*i*,*K*);(*Test*,*i*,*j*,*s*).前 4 种 Oracle 询问可以是多项式次,形式化了 E 所能发动的各种攻击,如窃听、已知会话密钥、重放、收买某合法方等攻击,(*Test*,*i*,*j*,*s*)则只能询问一次,是为了定义安全性而提供的“测试”Oracle.

安全性定义.除合理性(validity)之外,如果敌手得到 Oracle 询问(*Test*,*i*,*j*,*s*)的回答后,对 challenge“猜测”正确的优势函数 $Adv_{P,f,S_n}^{E}(k)(=2\Pr[good-Guess]-1)$ 是可忽略的,则称协议是安全的.这里,当敌手发起 *Test* 询问时,Oracle 回答如下:$b\in_R\{0,1\}$,如果 b=0,返回一个随机数,否则返回敌手要得到的会话密钥;如果敌手对 b 的取值猜测正确,就称事件“Good-Guess”发生,敌手成功.上述定义是说,如果敌手的成功概率只以可忽略优势偏离 1/2,敌手失败,即协议是安全的.

4.1.2 BR 安全模型的应用

人们基于 BR 安全模型设计了大量的 SKD 协议,有代表性的 SKD 协议可参见文献[22–25].文献[22]提出了一种两方 SKD 协议,该协议是一种基于非对称密码方案(公钥加密、签名)的 SKD 协议.具有如下性质:如果公钥加密和签名方案满足正规的、易理解的安全目标,则协议抗已知会话密钥攻击安全,具有语意安全性(semantic security,即敌手得不到会话密钥 K 的任何信息).

文献[23]提出了一种三方 SKD 协议,概述如下:

$A\rightarrow B:R_A$

$B\rightarrow S:R_A,R_B$

$S\rightarrow A:C_A=Enc_{a[1]}(K),Mac_{a[2]}(A,B,R_A,C_A)$

$$S \to B: C_B = Enc_{b[1]}(K), Mac_{b[2]}(A, B, R_B, C_B)$$

这里,$a[]$,$b[]$表示主密钥,这是基于对称密码(加密,认证码)的 SKD,可证明安全性质同上.

以上协议的缺点是不具有“前向机密性”,Bellare 等人随继又提出了具有“前向机密性”的 SKD 协议[24],该协议与具有认证功能的 Diffie-Hellman 协议基本相同,区别只在于对会话密钥用 hash 函数做了随机化处理:

$$K = H(g^{xy} \bmod p),$$

可证明安全性是基于 RO 模型的.

此外,Bellare,Pointcheval 等人在基于口令的 SKD 协议研究方面也取得了很好的结果,在 2000 年提出的一种兼具“前向机密性”和抗字典攻击性质的 SKD 协议[25],安全性证明是基于 Diffie-Hellman 问题(在 RO 模型下).基于口令的 SKD 协议是一种很有应用前景的协议,后面我们将详细加以论述.

对 SKD 协议主要有两类攻击:其一是利用基础本原的弱点发动攻击,如破译分组密码或伪造 MAC;其二是利用协议设计的缺陷发动攻击,比如对 NS 协议的已知密钥攻击.而可证明安全性的目标是证明不能存在源于协议缺陷的攻击,暗含假设是,不存在针对基础本原的攻击,亦即基础本原具有清晰的、标准的、易于理解的密码性质.

BR 安全模型作为第一个有关 SKD 协议的形式化安全模型得到了广泛的重视,在实践中不断得到改进.然而它只定义在现实世界中,因此归约过程较为繁琐,可操作性稍差.研究定义在两个世界(理想和现实世界)中的协议模型就成为一种很好的选择(因为理想模型中的协议和现实中的协议之间的转换更易于操作和理解),最有代表性的结果就是著名的 BCK 安全模型[26].

4.2 BCK安全模型及其应用

文献[26]中给出了构造和分析 SKD 协议的一般框架以及正确的形式化方法,并建议在设计复杂协议时采用简单、富有吸引力的模块化设计原则,称作 BCK 安全模型.BCK 安全模型的基本思想是:基于模块化观点,首先把 SKD 协议定义在理想模型中,然后像 BR 安全模型那样,利用计算不可区分性来定义理想模型中的安全性,最后协议被“编辑”成现实模型中的协议;归约证明时要求现实敌手必须能够“模仿”理想敌手,所谓“模仿”概念也就是不可区分性.

4.2.1 BCK 安全模型简介

该模型适用于研究认证通信问题,并特别强调相关的密钥交换问题.

敌手模型.敌手控制合法用户的通信信道,可以修改或删除传送消息,甚至插入假消息;还控制了消息发送的延迟;可能还具有额外的能力,如收买用户(很多时候,这模拟了通过入侵用户计算机系统获得用户秘密参数).认证链模型中的敌手称为 AM-敌手,概括说来除了收买某方的情形,AM-敌手不能伪造消息,只是忠实地传递消息(虽然可以改变传递顺序、延迟等);非认证链模型中的敌手称为 UM-敌手,能力要强得多.

安全目标.确保传送数据的可认证性.简单采用签名或 MAC 可能是不够的(当然它们通常是设计完整解决办法的基础),因为网络本质上是异步的,协议经常是“消息驱动”的.

通用编译器 C.这是模块化研究的核心组件,作用是把理想认证模型中的任何协议π转换成现实协议$\pi' = C(\pi)$,后者完成和前者一样的任务,但能够抵抗强得多的现实敌手.认证器(authenticator)是一个特殊的编译器 C:对任何协议π,$C(\pi)$在非认证网络中模仿π.设计认证器通常可以归约为更简单的协议,如 MT-authenticator(消息传播认证器),其目标只是认证用户间简单的消息交换,可以基于简单的密码函数(如 MAC、数字签名、公钥加密)来构造它.认证器的定义涉及认证和非认证模型的形式化定义以及运行在两个模型中的协议的等价概念,后者的基本要素是一个协议被另一个“模仿”的概念,它源于安全多方计算协议的一般定义[27].

协议定义.设计与分析在非认证网络中的协议可划分为两个独立的阶段:首先在认证模型中设计并证明协议安全性;然后应用特定的认证器确保被“编译”后的协议在非认证环境中维持和理想认证模型中相同的行为.这样极大地简化了设计与分析工作,还为设计者提供了一种“debug 工具”,帮助消除不必要的协议元素.具体而言,SKD 协议定义为如下一种“消息驱动协议”:一个这样的迭代进程,具有某初始状态(协议的输入、随机输入,

身份)的某方调用协议后,协议等待激活(activation):可由两类事件引起,来自网络的消息到达或一个外部请求(这形式化了来自该方运行的其他进程的信息);激活后,协议根据输入数据、当前内部状态,产生一个新的内部状态、一个向网络发出的消息、一个给该方运行的其他协议(或进程)的外部请求.此外,还产生一个输出(它是累加的,即开始为空,每次激活后的输出被附加上去);激活结束后,协议等待下一次激活.协议可以形式化表示为一个(概率)函数:

π(当前状态,接收的消息,外部请求)=(新状态,发出消息,发出请求,输出).

在认证链模型 AM(authenticated-link model)或非认证链模型中激活都由对应敌手 A 控制和编排.协议的整体输出即各方(包括敌手)的累加输出的联结.这里,敌手的输出是敌手观察(adversary view)的函数.敌手观察是指:敌手在整个计算期间,利用自己的随机输入,看到或推导出的信息.

协议的模仿.设 π,π' 是 n 方消息驱动协议,称 π' 在非认证网络中模仿 π,如果对任何 UM-敌手 U,存在 AM-敌手 A,使得对任何输入 x,满足

$$Auth_{\pi,A}(x)\overset{c}{\approx}Unauth_{\pi',A}(x).$$

上式表示计算不可分辨.这里, $Auth_{\pi,A}(x,r)=ADV_{\pi,A}(x,r),Auth_{\pi,A}(x,r)_1,...,Auth_{\pi,A}(x,r)_n$,是指在认证链模型中,根据输入 x 及随机输入 r 与敌手交互运行协议 π 之后,敌手以及全部 P_i 的累加输出, $Unauth_{\pi,A}(x)$ 的说明类似,但限于非认证链模型.

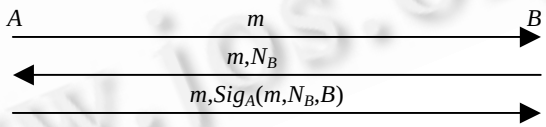
综上可见,认证器把(某种良好定义意义上)在认证链模型中安全的协议转化成非认证链模型中的安全协议,无疑,构造认证器至关重要.

MT-认证器主要用于设计认证器(authenticator):首先设计一个"低层"协议 λ,接收外部要求发送消息的请求,然后以认证的方式发送这些消息;其次,已知某协议 π(在认证链模型中工作),认证器输出一个协议 π',与 π 只有一个区别——消息要经过 λ 传递,也就是说,发出的消息不再直接传给网络,而是激活 λ 去传递消息;不再直接由网络接收消息,而是取自 λ 的输出.显然,MT-认证器 λ 在非认证网络中模仿认证网络中的消息传送协议(MT).因此可以给出如下编译器.

编译器 C_λ 定义:给定协议 π,生成 $\pi'=C_\lambda(\pi)$ 在 P_i 范围内运行,首先调用 λ;对 π 发送的每一条消息,π' 用发送该消息给预定收方的外部要求激活 λ;每当 π' 被某接收消息激活,都用它激活 λ,当 λ 输出"P_i 从 P_j 处收到 m",π 就被来自 P_j 的 m 激活.

定理 **1**. 设 λ 是 MT-认证器,C_λ 是基于 λ 的编译器,则 C_λ 是一个认证器.

文献[26]中还指出,MT-认证器作为最基础模块,可以根据基本的密码学工具构造,例如可以根据公钥签名构造如下的 MT-认证器 λ_{sig}:



定理 **2**. 假设签名方案在选择消息攻击下是安全的,则 λ_{sig} 在非认证网络模仿协议 MT.

4.2.2 BCK 安全模型的应用

因有如下结论,无妨重点研究认证链模型中的 SKD 协议(这时敌手实际是被动的).

定理 **3**. 如果 π 是认证链模型中的安全 SKD 协议,C 是认证器,则 $C(\pi)$ 是非认证链模型中安全的 SKD 协议.

定义安全 SKD 协议:首先规定理想进程——表示了我们凭直觉对 SKD 协议所能期望的最好特征;称一个 SKD 协议(在认证或非认证链模型中)是安全的,如果它能模仿对应理想进程.

理想 SKD 进程的形式化:存在 n 方 $P_1,\ldots,P_n$ 以及一个理想敌手 S,假设还有一个可信方 T.计算过程包括一系列由 S 导致的激活,共有如下 4 类激活.

I. 调用 P_i,以便和 P_j 建立一个新密钥.最终效果是值"P_i 和 P_j 建立了一个密钥(K,s)"被加到 P_i 的输出.这里,K 是按预定分布选择的密钥,s 包括身份、序号等信息.S 仅能得到 s,不知道 K(实际上,我们可以想像由 T 把 K 传给 P_i.如果建立密钥的双方有一方被收买,规定由敌手选择密钥).

II. 调用 P_j,以便和 P_i 建立会话 s 的密钥.与以上说明类似,但 R 规定 P_j 是应答方(我们可以想像由 T 把 K 传给 P_j).

III. 收买会话 s.这种激活仅当 s 当前是合法的;效果是敌手得到了对应会话 s 的密钥 K.此外,"会话 s 被收买"被加到发起方的输出上.

IV. 收买 P_i.效果是 P_i 知道的所有密钥都为敌手所知.此外,"P_i 被收买"被附于 P_i 的输出.

理想进程的整体输出.各方包括敌手的累加输出的联结:

$Ideal_S(r_S,r_T)=Adv_S(r_S,r_T),(Ideal_S(r_S,r_T))_1,...,(Ideal_S(r_S,r_T))_n$,具体说明与前面类似.

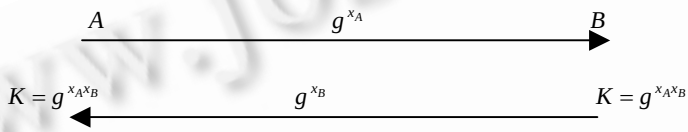
定义 5(两种模型中安全的 **SKD** 协议). 设π是 n 方消息驱动协议,称π在非认证网络中是安全的 SKD 协议,如果对任意 UM-敌手 U,存在一个理想敌手 S,使得

$$Unauth_{\pi,U}(\cdot)\overset{c}{\approx}Ideal_S(\cdot);$$

称π在认证网络中是安全的,如果对任意 AM-敌手 A,存在一个理想敌手 S,使得

$$Auth_{\pi,A}(\cdot)\overset{c}{\approx}Ideal_S(\cdot).$$

就具体应用而言,基于以上理论和必要的安全假设(DLP),不难证明,著名的原始 Diffie-Hellman(DH)协议:



就是认证链模型中安全的 KE 协议.然后基于前面介绍的认证器 λ_{sig},不难转化成现实模型中的安全 SKD 协议.也不难看出,这正是人们出于对中间人攻击的考虑对 DH 协议的改进,即认证 Diffie-Hellman 密钥协议,而 BCK 模型理论恰好证明了这种改进的安全性.

4.3 PSDK安全模型

以上介绍的 SKD 协议通常依赖于 PKI 技术或通信双方共享高品质的秘密钥(主密钥).问题是完全应用公钥技术成本较高,而对称密码算法的主密钥长度一般较长,显然不易记忆.因此,一个自然的思路就是,各方共享易于人类记忆的口令,由它构造出较高品质的会话密钥,当然,因上述口令可能取自一个较小的字典(多项式级),易受离线字典攻击,因此必须慎重评估其安全性.

基于口令的 SKD 协议(简单记为 PSKD)的安全目标:任何 PPT 敌手的成功概率上界为 $O(t/|D|)+\mu(n)$.这里,t 是敌手发动的会话数目,$\mu(\ )$是安全参数的可忽略函数.

第一个 PSKD 协议由 Bellovin 和 Merritt 提出[28],很快就成为该领域研究的基础,然而,这些协议并未证明其安全性,仅仅具有基于假想论断的推测安全性.第一个对此进行严格研究的是 Halevi 和 Krawczyk[25],他们实际上是考虑了一种非对称混合(hybrid)模型:一方(服务器)持有一个高质量的密钥,其他方(人)仅持有口令;任何人都可以安全地得到服务器的公钥.Halevi-Krawczyk 模型适用于非对称访问控制环境,但对于两个人之间建立通信则完全不适用,而且要求人在访问控制环境中持有不易记忆的公开密钥也不现实.那么是否可能实现仅基于易于记忆的口令的安全访问控制机制和认证密钥交换协议呢?

Bellare 等人首先给出了安全的基于口令的访问控制方案[29],但安全性证明是基于 RO 模型的.在标准模型下可证明安全的方案参见文献[30,31],文献[30]基于一次签名技术提出的 PSKD 协议称为 KOY 协议,安全性基于 DDH(判定性 Diffie-Hellman)假设.文献[32]则把 KOY 协议进一步推广到门限机制.Goldreich 则提出了第一个(也是唯一一个)仅基于标准密码假设——"陷门置换存在"的可证明安全 PSKD 协议[31].其核心思想是:一方首先选择在一个较大的域上的线性多项式 Q,与另一方执行一个安全的多项式赋值算法(安全多方计算),$Q(w)$即会话密钥.这里,w 是口令.

文献[31]也采用了"协议模仿"的观点进行安全性证明.通俗地讲,敌手对以上协议的攻击效果可以类比为这样的攻击:敌手只被允许询问常数次"w 是 A 的口令吗"这样的问题.该协议的缺陷是实现效率仍然不理想,而且不支持一对用户的并行操作.但有着较深远的理论意义.

下面我们主要来介绍 PSKD 安全模型.

基本约定:通信双方 A,B;信道 C 即 PPT 敌手,具有 Oracle A,B, $C^{A(x),B(x)}(\sigma)$ 是 C 以σ作为辅助输入,与分别以 x,y 为输入的 A,B 通信时的输出;(口令)字典 $D\subseteq\{0,1\}^n$,可以 PPT 取样,$\varepsilon=1/|D|$.

定义 **6** (($\mathbf{1}-\boldsymbol{\varepsilon}$)-不可区分). 设$\{X_n\}$和$\{Y_n\}$是两个概率空间,称它们是$(1-\varepsilon)$-不可区分,表示为 $\{X_n\}\overset{\varepsilon}{\approx}\{Y_n\}$,如果对任意 PPT 算法 D 及所有辅助输入 $z\in\{0,1\}^{poly(n)}$,

$$|\Pr[D(X_n,1^n,z)=1]-\Pr[D(Y_n,1^n,z)=1]|<\varepsilon+\mu(n).$$

显然,这是计算不可区分概念[2]的推广.

定义 **7** (($\mathbf{1}-\boldsymbol{\varepsilon}$)-伪随机性). 称$\{X_n\}$是$(1-\varepsilon)$-伪随机的,如果它与$\{U_n\}$是$(1-\varepsilon)$-不可区分的.

基本思想:采用“模仿”论断,即使得运行于现实模型的协议模仿理想模型的功能,两种情况下的输出不可区分.

理想模型.A',B'是共享口令 $w\in_R D$ 的诚实方,C'是任意 PPT 理想模型敌手,有辅助输入σ,A',B'把口令交给可信第三方,C'发送 0 或 1(接受/拒绝),若 C'发送 1, $k\in_R\{0,1\}^n$,发给 A',B';若 C'发送 0, $k\in_R\{0,1\}^n$,k 被发给 A',而 B'则收到符号$\perp$(失败符号),两种情况下 C'未收到输出.

理想分布. $Ideal_{C'}(D,\sigma)=(w,output(A'),output(B'),output(C'(\sigma)))$, 即如果 C'发出 1,则 $Ideal_{C'}(D,\sigma)=(w,U_n,U_n,\ output(C'(\sigma)))$, 否则, $Ideal_{C'}(D,\sigma)=(w,U_n,\perp,output(C'(\sigma)))$.

现实模型.A,B 说明同前,C 是任意 PPT 现实模型敌手亦即信道,有辅助输入σ;初始化同前,协议执行表示为 $C^{A(x),B(y)}(\sigma)$,C 有一个决定比特,决定某一方的私有输出是密钥或$\perp$(失败符号),无妨设是 B;现实分布为

$$Real_C(D,\sigma)=(w,output(A),output(B),output(C^{A(w),B(w)}(\sigma))).$$

协议安全性定义.称一个 PSKD 协议是安全的,如果满足以下两个条件:

(1) 被动敌手:任给 PPT 现实敌手 C,存在 PPT 理想敌手 C'(总发送 1),满足

$$\{Ideal_{C'}(D,\sigma)\}_{n,D,\sigma}\overset{c}{\equiv}\{Real_C(D,\sigma)\}_{n,D,\sigma};$$

(2) 主动敌手:任给 PPT 现实敌手 C,存在 PPT 理想敌手 C',满足

$$\{Ideal_{C'}(D,\sigma)\}_{n,D,\sigma}\overset{O(\varepsilon)}{\equiv}\{Real_C(D,\sigma)\}_{n,D,\sigma}.$$

这里,$\varepsilon=1/|D|$.

上述安全性定义有如下特点:输出会话密钥是$(1-O(\varepsilon))$-伪随机的;具有前向机密性:口令泄漏不影响当前会话密钥的安全,抗已知密钥攻击;具有入侵检测特性:敌手对任何会话消息的修改,至少以概率$(1-O(\varepsilon))$被检测出.

定理 **4**. 假设存在单向陷门置换,则存在安全的(强化)PSKD 协议.

这是文献[31]的主要结果,证明完全是构造性的.

5 结束语

本文试图全面、系统地介绍“可证明安全性”理论的发展历程、主要研究方向、有代表意义的方法论和重要结果,并融入作者的一些观点.叙述上尽可能采用模型化观点,以有助于说明方法论.鉴于可证明安全理论是一个较新的研究方向,希望能达到抛砖引玉的目的.

致谢 作者在写作过程中,得到了张振峰副研究员和陈伟东博士的大力支持,在此表示感谢.

References:

[1] Bellare M. Practice-Oriented provable-security. In: Damgard I, ed. Modern Cryptology in Theory and Practice. LNCS 1561, Berlin, Heidelberg: Springer-Verlag, 1999. 1−15.

[2] Goldreich O. Foundations of Cryptography. Cambridge: Cambridge University Press, 2001.

[3] Goldwasser S, Micali S. Probabilistic encryption. Journal of Computer and System Science, 1984,28:270−299.

[4] Goldwasser S, Micali S, Rivest R. A digital signature scheme secure against adaptive chosen-message attacks. SIAM Journal of Computing, 1988,17(2):281−308.

[5] Bellare M, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols. In: Proc. of the 1st ACM Conf. on Computer and Communications Security. New York: ACM Press, 1993. 62−67. http://doi.acm.org/10.1145/168588.168596

[6] Canetti R, Goldreich O, Halevi S. The random oracle methodology, revisited. Journal of the ACM, 2004,51(4):557−594.

[7] Pointcheval D. Asymmetric cryptography and practical security. Journal of Telecommunications and Information Technology, 2002, 4:41−56.

[8] Bellare M, Bilian J, Rogaway P. The security of cipher block chaining. In: Desmedt Y, ed. Proc. of the Advances in Cryptology—Crypto'94. LNCS 839, Berlin, Heidelberg: Springer-Verlag, 1994. 341−358.

[9] Bellare M, Rogaway P. Optimal asymmetric encryption. In: Santis A.D, ed. Proc. of the Advances in Cryptology—EUROCRYPT'94. LNCS 950, Berlin, Heidelberg: Springer-Verlag, 1995. 92−111.

[10] Bellare M, Rogaway P. The exact security of digital signatures—How to sign with RSA and rabin. In: Maurer U, ed. Proc. of the Advances in Cryptology—Eurocrypt'96 Proc. LNCS 1070, Berlin, Heidelberg: Springer-Verlag, 1996. 399−416.

[11] Fiat A, Shamir A. How to prove yourself: Practical solutions to identification and signature problems. In: Odlyzko A, ed. Proc. of the Advances in Cryptology—Crypto'86. LNCS 263, Berlin, Heidelberg: Springer-Verlag, 1986. 186−194.

[12] Micali M, Reyzin L. Improving the security of digital signature schemes. Journal of Cryptology, 2002,15(1):1−18.

[13] Pointcheval D, Stern J. Security proofs for signature schemes. In: Maurer U, ed. Proc. of the Advances in Cryptology—EUROCRYPT'96. LNCS 1070, Berlin, Heidelberg: Springer-Verlag, 1996. 387−398.

[14] Bellare M, Neven G. Transitive signatures based on factoring and RSA. In: Zheng Y, ed. Proc. of the Advances in Cryptology—ASIACRYPT 2002. LNCS 2501, Berlin, Heidelberg: Springer-Verlag, 2002. 397−414.

[15] Goh EJ, Jarecki S. A signature scheme as secure as the Diffie-Hellman problem. In: Biham E, ed. Proc. of the Advances in Cryptology—EUROCRYPT 2003. LNCS 2656, Berlin, Heidelberg: Springer-Verlag, 2003. 401−415.

[16] Koeune F. Careful design and integration of cryptographic primitives with contributions to timing attack, padding schemes and random number generators [Ph.D. Thesis]. Louvain-la-Neuve: Universite Catholique de Louvain, 2001.

[17] Gennaro R, Halevi S, Rabin T. Secure Hash-and-sign signatures without the random oracle. In: Stern J, ed. Proc. of the Advances in Cryptology—EUROCRYPT'99. LNCS 1592, Berlin, Heidelberg: Springer-Verlag, 1999. 123−139.

[18] Cramer R, Shoup V. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In: Krawczyk H, ed. Proc. of the Advances in Cryptology—Crypto'98. LNCS 1462, Berlin, Heidelberg: Springer-Verlag, 1998. 13−25.

[19] Needham R, Schroeder M. Using encryption for authentication in large networks of computers. Communications of the ACM, 1978, 21(12):993−999.

[20] Sacco G. Timestamps in key distribution protocols. Communications of the ACM, 1981,24(8):523−536.

[21] Burrows M, Abadi M, Needham R. A logic for authentication. ACM Trans. on Computer Systems, 1990,8(1):18−36.

[22] Bellare M, Rogaway P. Entity authentication and key exchange. In: Stinson D.R, ed. Proc. of the Advances in Cryptology—Crypto'93. LNCS 773, Berlin, Heidelberg: Springer-Verlag, 1993. 232−249.

[23] Bellare M. Provably secure session key distribution—The three party case. In: Proc. of the ACM Symp. on the Theory of Computing. New York: ACM Press, 1995. 57−66. http://doi.acm.org/10.1145/225058.225084

[24] Bellare M. The challenge of session-key distribution protocols. In: Proc. of the 7th Annual Workshop on Selected Areas in Cryptography (SAC 2000). Waterloo, 2000. http://www-cse.ucsd.edu/users/mihir/papers/kd-talk.pdf

[25] Halevi S, Krawczyk H. Public-Key cryptography and password protocols. In: Proc. of the 5th ACM Conf. on Computer and Communications Security. San Francisco: ACM, 1998. 122−131. http://doi.acm.org/10.1145/288090.288118

[26] Bellare M, Canetti R, Krawczyk H. A modular approach to the design and analysis of authentication and key exchange protocols. In: Proc. of the 30th Annual Symp. on the Theory of Computing. New York: ACM Preee, 1998. 419−428. http://doi.acm.org/10.1145/276698.276854

[27] Micali S, Rogaway P. Secure computation. In: Feigenbaum J, ed. Proc. of the Advances in Cryptology—Crypto'91. LNCS 576, Berlin, Heidelberg: Springer-Verlag, 1991. 392−404.

[28] Bellovin SM, Merritt M. Encrypted key exchange: Password-Based protocols secure against dictionary attacks. In: Proc. of the IEEE Symp. on Research in Security and Privacy. 1992. 72−84. http://doi.ieeecomputersociety.org/10.1109/RISP.1992.213269

[29] Bellare M, Pointcheval D, Rogaway P. Authenticated key exchange secure against dictionary attacks. In: Preneel B, ed. Proc. of the Advances in Cryptology—EUROCRYPT 2000. LNCS 1807, Berlin, Heidelberg: Springer-Verlag, 2000. 139−155.

[30] Katz J, Ostrovsky R, Yung M. Efficient password-authenticated key exchange using human-memorable passwords. In: Pfitzmann B, ed. Proc. of the Advances in Cryptology—EUROCRYPT 2001. LNCS 2045, Berlin, Heidelberg: Springer-Verlag, 2001. 475−494.

[31] Goldreich O, Lindell Y. Session-Key generation using human passwords only. In: Kilian J, ed. Proc. of the Advances in Cryptology—CRYPTO 2001. LNCS 2139, Berlin, Heidelberg: Springer-Verlag, 2001. 408−432.

[32] Raimondo MD, Gennaro R. Provably secure threshold password-authenticated key exchange. In: Biham E, ed. Proc. of the Advances in Cryptology—EUROCRYPT 2003. LNCS 2656, Berlin, Heidelberg: Springer-Verlag, 2003. 507−523.

敬 告 作 者

《软件学报》创刊以来,蒙国内外学术界厚爱,收到许多高质量的稿件,其中不少在发表后读者反映良好,认为本刊保持了较高的学术水平.但也有一些稿件因不符合本刊的要求而未能通过审稿.为了帮助广大作者尽快地把他们的优秀研究成果发表在我刊上,特此列举一些审稿过程中经常遇到的问题,请作者投稿时尽量予以避免,以利大作的发表.

1. 读书偶有所得,即匆忙成文,未曾注意该领域或该研究课题国内外近年来的发展情况,不引用和不比较最近文献中的同类结果,有的甚至完全不列参考文献.

2. 做了一个软件系统,详尽描述该系统的各个方面,如像工作报告,但采用的基本上是成熟技术,未与国内外同类系统比较,没有指出该系统在技术上哪几点比别人先进,为什么先进.一般来说,技术上没有创新的软件系统是没有发表价值的.

3. 提出一个新的算法,认为该算法优越,但既未从数学上证明比现有的其他算法好(例如降低复杂性),也没有用实验数据来进行对比,难以令人信服.

4. 提出一个大型软件系统的总体设想,但很粗糙,而且还没有(哪怕是部分的)实现,很难证明该设想是现实的、可行的、先进的.

5. 介绍一个现有的软件开发方法,或一个现有软件产品的结构(非作者本人开发,往往是引进的,或公司产品),甚至某一软件的使用方法.本刊不登载高级科普文章,不支持在论文中引进广告色彩.

6. 提出对软件开发或软件产业的某种观点,泛泛而论,技术含量少.本刊目前暂不开办软件论坛,只发表学术文章,但也欢迎材料丰富,反映现代软件理论或技术发展,并含有作者精辟见解的某一领域的综述文章.

7. 介绍作者做的把软件技术应用于某个领域的工作,但其中软件技术含量太少,甚至微不足道,大部分内容是其他专业领域的技术细节,这类文章宜改投其他专业刊物.

8. 其主要内容已经在其他正式学术刊物上或在正式出版物中发表过的文章,一稿多投的文章,经退稿后未作本质修改换名重投的文章.

本刊热情欢迎国内外科技界对《软件学报》踊跃投稿.为了和大家一起办好本刊,特提出以上各点敬告作者.并且欢迎广大作者和读者对本刊的各个方面,尤其是对论文的质量多多提出批评建议.