数字签名方案的分析*
Analysis on Digital Signature Scheme

吕皖丽 钟 诚**
Lu Wanli Zhong Cheng

(广西大学计算机与信息工程学院 南宁 530004)
(College of Computer and Information Engineering, Guangxi University, Nanning, 530004)

摘要 分析数字签名机制、部分特殊签名和分布式系统上较流行的多重数字签名方案，并讨论了在分布式系统上实现高效安全的多重数字签名的有关问题。

关键词 数字签名 公钥算法 PKI 多重数字签名
中图法分类号 TP309.7 A

Abstract The digital signature system, and some schemes of the special digital signatures and popular multi-signature on the distributed systems are analyzed. Some problems about safety and efficiency of the multi-signature are also discussed.

Key words digital signature, public key cryptography, PKI, multi-signature

数字签名的概念由 Whitfield Diffie 和 Martin Hellman 于1976年最先提出，目的是使签名者对电子文件也可以进行签名并且无法否认，验证者无法篡改文件。之后，不同的数字签名方案先后被提出：Rivest、Shamir 和 Adleman 于1978年提出了基于 RSA 公钥算法的数字签名方案，Shamir 于1985年提出了一种基于身份识别的数字签名方案，ELGaml 于1985年提出一种基于离散对数的公钥密码算法和数字签名方案，Schnorr 于1990年提出了适合智能卡的有效数字签名，Agnew 于1990年提出了一种改进的基于离散对数的数字签名方案，NIST 于1991年提出了数字签名算法 DSA，1992年 Scott Vanstone 首先提出椭圆曲线数字签名算法 ECDSA。1993年以来，针对实际应用中大量特殊场合的签名需要，数字签名领域转向对特殊签名和多重数字签名的广泛研究阶段。

1 数字签名机制

数字签名体系的目的在于保证数据来源的可靠性和其签名时间的不可否认性，一般由签

2002-06-16 收稿。
* 国家高性能计算基金和广西大学科研基金的资助项目。
** 中国科技大学计算机系在读博士。

名算法、数字信封结构、公钥机制[1](PKI,普遍采用的标准为ITU-T X.509)等部分组成。

数字信封结构把待签名的数据、时间和数字签名结合成一个不可分割的整体,以抵抗重放攻击和代换攻击,确保签名的法律效力。签名算法一般由公开密钥密码算法(RSA、ELGamal、DSA、ECDSA等)、对称密钥密码算法(DES,AES等)和单向散列函数(MD2、MD4、MD5或SHA等)构成。

在签名过程中,签名方使用单向散列函数得到待签名文件的散列值,用对称密钥密码算法将文件加密,然后用公钥算法生成数字签名并加密对称密钥密码算法中所使用的密钥,最后将加密后的源文件、签名、加密密钥和时间戳放在一个信封中发送出去。验证过程则相反,验证方用公钥算法得到签名方发送的对称密钥和文件的散列值,用对称密钥解密文件并用单向散列函数生成散列值,若该值与签名方发送的散列值相等,则签名被验证。

1.1 实现数字签名的公钥算法

公钥算法建立在一定的数学基础之上。能有效用作数字签名的公钥算法可以分成三类:建立在大整数素因子分解基础上(如RSA)、建立在有限域的离散对数问题上(如DSA)以及建立在椭圆曲线上(ECC)的密码算法[2]。

Rivest、Shamir和Adleman于1978年提出了RSA数字签名和公钥算法,这是第一个较完善的公开密钥算法,其安全性建立在大数因子分解的基础上。它既能用于加密也能用于数字签名,而认证过程相当于保密过程的逆过程。

1991年8月,NIST提出了数字签名算法DSA,并将其用于数字签名标准DSS中。1994年5月19日,该标准(FIPS 186-1)最终被颁布。DSA算法使用一个单向散列函数$H(M)$。该标准指定使用安全散列算法SHA。DSA的安全性是建立在有限域上的离散对数问题之上的。目前,分解因子和解离散对数问题均有了亚指数时间的算法,因此DSA算法的安全性受到威胁。当然,可以通过加大密钥长度来确保安全,但这会造成计算量的剧增以及用户保存密钥的不便。1992年Vanstone首先提出椭圆曲线数字签名算法ECDSA。基于有限域离散对数机制上的密码系统和基于椭圆曲线上的密码系统的安全性均建立在解离散对数问题的难度上。假设P和Q是椭圆曲线E上的2点,Q为P的点乘,即$Q=kP$,若已知Q和P,求k,这便是椭圆曲线上的离散对数问题。目前已知求解椭圆曲线上离散对数问题的算法还都为完全指数时间算法。

在安全性相同的情况下,ECDSA所使用的密钥长度最短。这使得ECDSA算法的执行速度更快、占用存储空间更小、效率更高。并且当加密短消息时,ECDSA所占用的带宽最小。这些优点使得ECDSA相对于其他公钥算法更具有竞争力。

ECDSA于1998年成为ISO标准,1999年成为ANSI标准,2000年成为IEEE标准。2000年2月15日,NIST正式批准数字签名标准FIPS 186-2取代FIPS 186-1[3],该标准采用椭圆曲线数字签名算法ECDSA。

1.2 公钥机制

公钥机制PKI是一种遵循ITU-T X.509标准的密钥管理平台,它的核心内容就是为所有网络应用透明地提供采用加密和数字签名等密码服务所必需的密钥和证书管理,由PKI用户、注册机构(RA)、认证机构(CA)、证书库和作废证书清单(CRL)等基本组成成分构成。RA是证书的注册机构,是PKI的入口,负责受理PKI的服务申请,并将合法的申请上传给CA。CA是证书的签发机构,是PKI的核心。在使用公钥体制的网络环境中,CA作为可信的机构对任何一个主体的公钥进行公证,其签名用来保证此公钥的确属于用户信息中所指定的用户。

PKI通过作废证书清单来进行作废证书的管理。各个CA周期性地发布作废证书列表，公布最新作废证书序号。

如何对PKI结构进行组织一直是国内外研究的热点。一个能被广泛接受、扩充性良好的PKI解决方案应该真正做到跨平台，并且能够支持上述3种不同类型的公钥算法。国外的理论和技术比较成型，建立了一系列的规范，如ITU-T X.509，ISO/IEC 9594-8，ANSI X9.55等。

在RFC 1422中定义了CA的一种严格的层次结构并将其用于高强度安全秘密电子邮件(PEM)的认证。这种结构层次清晰，简单方便，但用户使用它时却必须接受某些严格的约束条件来明确相关信息，此种认证的使用受到了限制。在RFC 3280中PKI将CA组织成网络结构，可以从拥有某一认证机构公钥的用户开始建立认证路径。

2　特殊签名

当一般数字签名方案不能满足某些特别的签名需要时，便需要借助于特殊数字签名。

(1)盲签名：当签名者签署一份不知道内容的文件时，就需要使用盲签名。由于盲签名具有匿名的性质，因而在电子货币和电子投票系统中得到了广泛的应用。

(2)双重签名：安全电子交易(SET)使用的一种数字签名方案。当签名者希望验证者只知道报价单，中间人只知道授权指令时，能够让中间人在签名者和验证者报价相同的情况下进行授权操作。

(3)群签名：允许一个群体中的成员以整个群体的名义进行数字签名，并且验证者能够确认签名者的身份。群签名中最重要的是群密钥的分配，要能够高效处理群成员的动态加入和退出。一般的群密钥的管理可以分为两大类别：集中式密钥管理(密钥管理员产生密钥并分发给每一个群成员)和分散式密钥管理(由所有群成员共同建立群密钥)。

(4)门限签名：在有n个成员的群体中，至少有t个成员才能代表群体对文件进行有效的数字签名。门限签名通过共享密钥方法实现，它将密钥分为n份，只有当将超过t份的子密钥组合在一起时才能重构出密钥。门限签名在密钥托管技术中得到了很好的应用，某人的私钥由政府的n个部门托管，当其中超过t个部门决定对其实行监听时，便可重构密钥。

(5)代理签名：允许密钥持有者授权给第三方，获得授权的第三方能够代表签名持有者进行数字签名。1996年Mambo首次提出了代理签名的概念，之后，代理签名开始被广泛研究。目前提出了3种不同的代理机制：全权代理、部分代理和授权代理。

(6)门限代理签名：为了控制代理签名中授权的第三方不会乱用签名，此方案将密钥分配给n个代理者，只有超过t个人联合时才可以重构密钥。通过这样的方法可以限制代理者的权限。可以看出，门限代理签名实际上是门限签名和代理签名的综合应用。

(7)不可否认的门限代理签名[4]：用来防止门限代理签名中的t个签名者同谋重构签名，该方案中参与代理签名的t人均不可否认其签名。

3　分布式系统上的多重数字签名

随着分布式网络系统的发展，在分布式的环境中实现高效率、抗攻击的多重数字签名显得尤其重要。1983年，Ltakurak首次提出多重数字签名的概念并提出一个签名次数固定的签名方案。之后，各种不同的多重数字签名方案被相继提出，多重数字签名是一种需要多人对同一文件进行签名后文件才生效的数字签名。多重数字签名与门限签名不同，多重数字签名中的签

名者均有自己不同的一对密钥，而门限签名中的签名者多人共享一个密钥；多重数字签名中的签名者以个人的名义签名，而门限签名中的签名者代表集体签名。较流行的多重数字签名方案有广播多重数字签名和有序多重数字签名2种。

(1)广播多重数字签名。发送者将消息同时发送给每一位签名者进行数字签名，签名完毕后将结果发送到签名收集者计算整理，最终发送给签名验证者。

(2)有序多重数字签名。消息发送者预先设计一种签名顺序，将这种签名按顺序发送到每一位签名者进行数字签名，最终发送给签名验证者。

(3)基于ID号的多重数字签名[5]。1996年，Chou 和 Wu 提出了2种基于ID号的多重数字签名协议，分别适用于广播多重数字签名和有序多重数字签名。该签名算法基于大数因子分解难度，使用认证机构 CA。1999年，Narn-Yin Lee 提出了对这2种多重数字签名进行攻击的方法。

(4)签名权限各异多重数字签名。该方案由 Harn 于1999年提出。其特征是参与签名的各人均持有不同的签名权限，所以系统可以识别每个签名者，但是不能保证每个签名者只有一个签名权限。

(5)使用自鉴定公钥的 ELGamal 型多重数字签名[6]。该算法由 Yuh-Shihng Chang 于2000年提出，它通过验证多重数字签名来进行公钥的鉴定。其优点是减少了一般签名算法将公钥保存在 PKI 中而验证算法时必须先从 PKI 中检索得到公钥的过程，缺点是签名中需要较多的参数。

(6)基于文件分解的多重数字签名[7]。该方案由 Tzong-Chen Wu 于2001年提出。当对一个内容广泛、包含不同主体的文件进行多重数字签名时，可以按主题将文件分解为一些不相交的子文件，让各个签名者分别对自己熟悉的部分而不是对整个文件进行签名，验证时可以通过群体的公共密钥进行验证。该方案的安全性基于求离散对数问题的难度。这种方案的好处是即使有很多人参与签名，但每个人仅仅对子文件签名，就不会造成签名后的文件变得很大；并且由于仅仅在网络中传输给每个签名者需要签名的子文件，所以对网络的通信带宽要求也很低。其缺点是每次签名前必须人工地将文件分割成不同领域的子文件并将其分别传输给不同领域的签名者。

上述的多重数字签名方案从安全性上来说均基于大整数因子分解或有限域上的离散对数难题，用更加安全的椭圆曲线密码算法实现分布式系统中的多重数字签名将更能满足实际应用的需要。从设计方案上来说，也都各有缺点和不足，容易找到攻击的入口。因而，目前迫切需要设计出适合在分布式系统上进行多重数字签名的椭圆曲线密码方案。将多重数字签名和特殊签名结合在一起，设计出适合特殊需要的多重数字签名也是亟待解决的问题。

另外，大多数分布式系统上的多重数字签名均需要 PKI 的支持与验证，而现在的 PKI 中对 CA 的组织还不能安全、高效、快速地支持多重数字签名方案，需要在现有基础上改进 CA 的组织结构，以满足分布式系统中多重数字签名的需要。

4 结束语

目前我国数字签名技术与国外相比还有一定的差距。美国联邦政府已制定了新的基于椭圆曲线的数字签名标准(FIPS 186-2)。可以预见，中国急需自己的数字签名标准。针对中国国

(下转第170页)

参考文献

1 施发中. 计算机辅助几何设计与非均匀有理B样条. 北京:北京航空航天大学出版社,1994. 273.

2 肖轶军等. 基于迭代最近点的B样条曲线拟合方法研究. 中国图象图形学报,2000.(7):585～588.

3 Farin. Curves and Surfaces for Computer Aided Geometric Design. Second Edition. Academic Press. 1990. 154.

(责任编辑:黎贞崇)

(上接第164页)

情.怎样将PKI法制化、规范化,建立具有中国特色的PKI是我们的当务之急。在公钥算法的选定上,国外已经开始选用安全系数较高的椭圆曲线数字签名算法ECDSA进行数字签名,而国内仍然处于选用RSA或DSA的状况。因此,加强对ECC的研究,在现有理论和技术基础上充分吸收国外先进经验,开发自己的算法、标准、体系,形成自主的创新的密码技术,以对付来自国际社会的挑战。

参考文献

1 Housley R. Polk W. Ford W et al.. RFC 3280 Internet X 509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. http://www.ietf.org/rfc/rfc3280.txt?number=3280.2002.

2 William J Caelli. Edward P Dawson. Scott A Rea PKI Elliptic curve cryptography and digital signatures. Computers & Security. 1999. 18:47～66.

3 William M Doley. Digital Signature Standard (DSS). http://csrc.nist.gov/cryptval/dss.htm. 2002.

4 Hsu Chienlung. Wu Tzongsun. Wu Tzongchen. New nonrepudiable threshold proxy signature scheme with known signers. The Journal of Systems and Software. 2001. 58:199～124.

5 Lee Narn-Yin. Hwang Tzonelih. Wang Chin-Hung. The security of two ID-based multisignature protocols for sequential and broadcasting architectures. Information Processing Letters. 1999. 70:79～81.

6 Chang Yuhshihng. Wu Tzongchen. Huang Shinchan. ELGamal-like digital signature and multisignature schmes using self-certified public keys. The Journal of Systems and Software. 2000. 50:99～105.

7 Wu Tzongchen. Huang Chinchan. Guan D J. Delegated multisignature scheme with document decomposition. The Journal of Systems and Software. 2001. (55):321～328.

(责任编辑:黎贞崇)