第 32 卷 增刊
2002 年 11 月

东南大学学报(自然科学版)
JOURNAL OF SOUTHEAST UNIVERSITY (Natural Science Edition)

Vol.32 Sup.
Nov. 2002

保密散列数字签名

董林芳　武金木　刘　依　　洪流涛

(河北工业大学信息学院，天津 300130)　(杭州萧山经济技术开发区热电有限公司，杭州 311217)

摘要：众所周知，亲笔签名具有非常重要的法律依据.随着计算机网络、电子邮件、电子支付和办公自动化系统的广泛应用，数字签名问题显得更加突出.文章介绍了数字签名中最常用的对称密钥数字签名算法和以公开密钥为基础的数字签名算法——DSA，分析了各自的特点，并结合各算法的优点进行改进，提出一种新的数字签名方式——保密散列数字签名.该方式可以使得数字签名的真实性和加密的安全性结合起来，另外通过对文件的散列值签名使得计算速度大大提高.通过使用这种签名方式，既可以确保文件内容的秘密性，又可以避免普通 Hash 签名使用单密钥的不安全和容易伪造.

关键词：数字签名；对称密钥；公开密钥；保密散列数字签名；DSA；散列

中图分类号：TP309.7　　**文献标识码**：A　　**文章编号**：1001－0505(2002)Sup-0262-03

Secret Hash digital signature

Dong Linfang[1]　Wu Jinmu[1]　Liu Yi[1]　Hong Liutao[2]

([1]School of Information, Hebei University of Technology, Tianjin 300130)

([2]Hangzhou Xiaoshan Economic & Technological Development Zone Thermoelectricity Co. Ltd, Hangzhou 311217)

Abstract: It is well known that autograph has important legal validity. With the wide application of Web, e-mail, e-commerce and e-government, digital signature becomes more important. This paper briefly introduces some of the most significant digital signature algorithms, analyzes the characteristic and gives improvements at the same time. We brought forward a new algorithm—secret Hash digital signature, which is more secret, occupies less space and runs in higher speed. This digital signature combines symmetric algorithm and public-key algorithm, applies one-way Hash function at the same time. The algorithm offers a perfect method of digital signature and has a promising future.

Key words: digital signature; symmetric algorithm; public-key algorithm; secret Hash digital signature; DSA; Hash

签名实质上是证明当事者身份与数据真实性的一种信息，既然签名是一种信息，因此签名可以用不同的形式来表示.传统的以文件为基础的书面签名形式如手签名、印章、指纹等.在计算机文件中，则采用电子形式的签名，即数字签名.

数字签名实现基础是加密技术，可以由对称密钥算法实现，也可以由非对称密钥(公开密钥)算法实现.对称密钥算法的速度较快，但涉及到密钥的交换问题以及仲裁人，安全性和保密性较差.公开密钥算法更加灵活多样，但是速度不如对称密钥算法快，不适用于长文件的数字签名.实际应用当中可以结合两者的优点，扬长避短，形成一个安全性和签名速度都令人满意的系统.

1　对称密钥密码算法进行数字签名

对称密钥密码算法所用的加密密钥和解密密钥通常是相同的，或者可以很容易地由其中的任意一个推导出另一个.对称密钥算法实现数字签名必须有仲裁人参与.用户 A 和仲裁人 T 共享密钥 K_A，用户 B 和 T 共享另一个不同的密钥 K_B.

1) A 用 K_A 加密他准备发送给 B 的明文消息 M，并把加密消息 C_A 传送给 T：$C_A = E_{K_A}(M)$；

2) T 用 K_A 解密 C_A：$M = D_{K_A}(C_A)$；

收稿日期：2002-05-15.　作者简介：董林芳(1972—)，女，硕士.

3) T把解密消息和他收到A消息的声明 t,一起用 K_B 加密成 C_B:$C_B = E_{K_B}(M, t)$;

4) T把加密的消息包 C_B 连同A用 K_A 加密的 C_A 一起传给B;

5) B用 K_B 解密消息包 C_B 之后,就可以读到A的消息 M 和T的签名证书 t,证明消息来自A:$(M, t) = D_{K_B}(C_B)$.B需要保留 C_A 以备发生分歧时裁决之用.这种签名方式要求仲裁人必须高度的完善和安全,而且得到所有人的信任.

2 公开密钥数字签名算法

公开密钥系统用作数字签名的协议很简单:① A用他的私人密钥对文件加密,从而对文件签名;② A将签名文件法送给B;③ B用A的公开密钥解密文件,从而验证签名.

公开密钥数字签名的算法很多,应用最为广泛的3种是:DSA签名、RSA签名和Hash签名.

2.1 DSS和RSA签名

早在1991年8月30日,美国国家标准与技术学会(NIST)就在联邦注册书上发表了一个通知,提出了一个联邦数字签名标准,NIST称之为数字签名标准(digital signature standard, DSS).该标准为计算和核实数字签名指定了一个公开密钥数字签名算法(digital signature algorithm, DSA).

RSA是最流行的一种加密标准,许多产品的内核中都有RSA的软件和类库.与DSS不同,RSA既可以用来加密数据,也可以用于身份认证.与对称密钥算法实现的数字签名相比,在公钥系统中,由于生成签名的密钥只存储于用户的计算机中,安全系数更大一些.

2.2 Hash签名

在实际的实现过程中,采用公开密钥密码算法对长文件签名效率太低.为了节省时间,数字签名协议经常和单向散列函数一起使用.该编码法采用单向散列函数(Hash函数)将需加密的明文"摘要"成一串128bit的密文,这一串密文亦称为数字指纹(FingerPrint).它有固定的长度,且对相同的明文多次操作生成的摘要一定相同,不同的明文摘要必定不相同.即使是只修改明文的一个标点符号,再生成的摘要也会改变很多.这样这串摘要就可成为验证明文是否是"真身"的"指纹"了.

采用这种方法使得计算速度大大提高,单向散列函数确保不同文件的散列值不相同,因此,对散列函数签名和对整个文件签名一样安全.

3 当前数字签名的不足

对称密钥密码算法实现的数字签名,需有仲裁人参与,这是非常耗时的,容易对整个系统造成瓶颈.仲裁人的数据库中存有每一对签名人的密钥,这对计算机的存储量提出了较高的要求,而且一旦被攻破会造成很大的损失.文件的内容也不能对仲裁人保密.

公开密钥算法实现的数字签名可以解决这个问题,即签名人A用私人密钥加密文件实现签名,验证人用B用A的公开密钥解密,如果能够解密,就验证了签名,因为别人不知道A的私人密钥.但这里有另一个问题,任何人都可以用A的公开密钥解密文件看其内容.这样满足不了用户对文件机密性的要求.

公开密钥系统数字签名满足签名的不可重用,因为签名是文件的函数并且不可能转换成另外的文件,但可能被B把签名和文件一起重用.比如,A交给B一张签名数字支票,B可以复制该支票,在不同的时间或到不同的银行验证支票并兑现支票.

公开密钥系统对长文件的加密速度比对称密钥系统要慢近1000倍,效率太低.

Hash签名的主要局限是接收方必须持有用户密钥的副本以检验签名,因为双方都知道生成签名的密钥,较容易攻破,存在伪造签名的可能.如果中央或用户计算机中有一个被攻破,那么其安全性就受到了威胁.

4 保密散列数字签名

4.1 各种签名方式的改进

针对以上所述,可以如此解决各种签名方法的不足.

对公开密钥算法实现的数字签名而言,为避免任何人都可以用A的公开密钥解密文件看其内容,A可以进一步用B的公开密钥加密其签名文件,B收到之后,先用自己的私人密钥解密,然后用A的公开密钥验证

签名.这样就实现了把数字签名的真实性和加密的安全性结合起来,就好像写信,签名说明了谁是写信人,信封提供了秘密性.

为防止 B 复制 A 签名的数字支票,在不同的时间或到不同的银行验证支票并兑现支票,可以加入时间标记以防止类似的金融诈骗.即把日期和时间附在消息中,并跟消息其他的部分一起签名.银行可以将所兑现支票的时间标记存储在数据库中,兑现支票时检查时间标记是否和数据库中的一样.如果一样就证明该支票已经被兑现.

为提高效率,公开密钥数字签名还应该与单向散列函数一起使用.

4.2 保密散列数字签名算法

总的来说,目前的数字签名算法都是以对称密钥密码体制或公开密钥密码体制来实现的,这就必然会有各种缺陷.我们全面综合各类数字签名方法的优点,把对称密钥算法、公开密钥算法及单向散列函数结合在一起,避免了单独使用一种算法的不足,提出以下的保密散列数字签名算法:

A 和 B 事先协商他们采用的单向散列函数 H,散列函数不必保密.

1) A 产生明文 M 的单向散列值 H_A(或称消息摘要);

2) A 选择密钥 K,利用对称密钥加密方法对明文 M 加密成密文 C: $C = E_K(M)$;

3) A 利用公开密钥算法以私人密钥 K_{AS}对散列 H_A、时间标记 t、密钥 K 加密产生 C_H,从而表示对文件签名: $C_H = E_{K_{AS}}(H_A, t, K)$;

4) A 将签名 C_H 用 B 的公开密钥 K_{BP}加密成 C_H': $C_H' = E_{K_{BP}}(C_H)$;

5) A 将密文 C 和签名 C_H'一起传送给 B;

6) B 用自己的私人密钥解密签名 C_H',得到 C_H;

7) B 用 A 的公开密钥解密 C_H 得到文件摘要 H_A、时间标记 t 和密钥 K;

8) B 用 K 解密 C 得到文件原文 M;

9) B 用明文 M 产生单向散列值 H_B,对比自己计算产生的 H_B 和从 C_H 解密得到的 H_A,如果匹配证明签名是有效的.

这种签名方式用对称密钥加密方法加密文件原文,保证了文件的秘密性,同时弥补了公开密钥算法加密长文件效率较低的不足.利用单向散列函数产生文件摘要进行公开加密数字签名,同时将加密文件的密钥 K 一起签名,避免密钥 K 的泄漏.这样做不需要仲裁人参与就解决了对称密钥算法的密钥传递问题,更加高效而且保密.进一步用接收方公开密钥加密又可以阻止其他人偷看文件原文及验证签名.

5 结 论

以上的保密散列数字签名算法能够满足所要求的所有条件:

1)可信的.只有 A 才能用他的私人密钥对文件签名,否则 B 无法用 A 的公开密钥解密;

2)不可伪造的.只要 A 没有泄漏私人密钥,就不可能有人假借 A 的名义签名;

3)签名不能重复使用.如果 B 把签名附到另一个文件上,A 或仲裁人就要求他出示 A 用私人密钥签名过的文件,B 显然没有以 A 的私人密钥对伪造文件进行的签名;

4)文件不能被改变.用上述方法同样可以验证消息 M 是否被改动;

5)A 不能抵赖消息 M.A 对文件摘要的签名密文可以证明 A 发送过消息 M.

这个数字签名算法不但速度快,而且可以将文件与签名分开传送和保存,保密性强,减少存储空间,应用前景十分广阔.

参考文献

[1] Bruce Schneier. 应用密码学.北京:机械工业出版社,2000.

[2] 冯登国,裴定一. 密码学引导 [M]. 北京:科学出版社,1999.

[3] 卢开澄. 计算机密码学.第 2 版.北京:清华大学出版社,1998.

[4] http://extend.hk.hi.cn/~yrch168/business.html

[5] http://www.szca.gov.cn/yyzn/yyzn3.htm.