浙江科技学院学报,第 15 卷第 4 期,2003 年 12 月
Journal of Zhejiang University of Science and Technology
Vol.15 No.4, Dec. 2003

票据背书转让中的数字签名协议

邵祖华
(浙江科技学院 计算机与电子工程学系,浙江 杭州 310012)

摘　要:研究了商务活动中票据背书转让签名的特点,设计了随机有序多重签名协议,它的安全性基于离散对数的困难性。随机有序多重签名协议可推广到层次管理机构中的公文审批,也可用于电子政务。

关键词:密码学;数字签名;票据背书转让;电子政务
中图分类号: TN918;F713.36　　**文献标识码**: A　　**文章编号**: 1671 - 8798(2003)04 - 0224 - 04

在信息化社会中,我们不仅需要信息的保密性,而且需要信息的真实性和完整性。数字签名就是实现后者的信息技术,它为电子商务和电子政务的安全提供了强有力的技术保障。

数字签名的安全要求是:①签名是可信的;②签名是不可伪造的;③签名是不可抵赖的。

一个数字签名协议由两部分组成:签名算法和验证算法。一个签名人输入要保护的消息和只有自己知道的私钥,通过签名算法计算出数字签名。任何人只要输入对应的公钥,通过验证算法就可以判定数字签名的真假。

自 20 世纪 70 年代 Diffie 和 Hellman 提出公钥密码体制以来[1],相继发明了许多数字签名协议。基于因数分解的 RSA 和基于离散对数的 DSA 成为大浪淘沙后的佼佼者,在电子商务和电子政务中已经得到广泛的应用。我国正在制订的数字签名法将为数字签名奠定法律基础,并将大大促进数字签名在我国的推广应用。

本文研究基于离散对数的 DSA 类型的数字签名在金融票据背书转让中的应用。

1　票据的背书转让

在市场商品经济中,票据是国际通行的结算信用工具。票据的特点在于流通,流通的基础在于票据的转让,它是票据制度的核心。票据转让的主要方法就是背书。《中华人民共和国票据法》对票据的背书转让作了明确的规定:“持票人可以将票据权利转让他人或者将一定的票据权利授予他人行使。……票据以背书转让或者以背书将一定的票据权利授予他人行使时,必须记载被背书人的名称。背书由背书人签章并记载背书日期。……以背书转让的票据,背书应当连续。持票人以背书的连续,证明其票据权利。……所谓背书连续,是指在票据转让中,转让票据的背书人与受让票据的被背书人在票据的签章依次前后衔接。……以背书转让的票据,后手应当对其直接前手背书的真实性负责。”

如果我们从数字签名的角度研究票据的背书转让中的签章,可以发现以下特点:①签名在时间上是离散的,不是同时发生的;②签名的次序是不固定的;③多重签名的次数是随机的,每个签名人不知道以后还有谁会签名;④多重签名的正确性不仅在于验证方程的正确性,而且在于签名次序的连续性。

Harn[2,3]、Okamoto[4]、纪家惠[5]等人都研究过多重数字签名技术,但是他们的方法都无法解决票据背书

收稿日期: 2003 - 05 - 22
基金项目: 浙江省教育厅科研计划项目(20030840)
作者简介: 邵祖华(1948—),男,上海市人,硕士,教授,主要研究密码学和金融数据安全。

转让的连续签名问题。我们把这种数字签名称为随机有序多重签名。

2　随机有序多重签名协议

DSA 类型的数字签名协议需要一些初始化的工作。

2.1　系统初始化

由权威公证机构选择一些共同的参数和函数:①一个素数 p,$2^{640} < p < 2^{1024}$;②$p-1$ 的一个素因子 q,$2^{159} < q < 2^{160}$;③ 一个小于 p 的整数 h,计算 $g = h^{(p-1)/q} (\mathrm{mod} p)$;④ 单向杂凑函数 H。p, q, g 和 H 都是公开的。

每个要签名的出票人或背书人,自己选择一个整数 x,$0 < x < q$,计算

$$y = g^x (\mathrm{mod}\ p)$$

x 是他的私钥,而 y 是他的公钥,ID 是他的标识符。

为了保护公钥的真实性,每个用户的公钥必须经过数字证书认证机构 CA 的公证。

2.2　出票人计算签名方法

一张票据首先由出票人填写有关内容,然后用以下方法计算数字签名。假设制作的票据记载的事项中需要保护的消息是 m,ID_2 是收票人的标识符,T_1 是出票的时间。出票人 ID_1 计算:

(1) 每次重新选择一个随机数 k_1,$0 < k_1 < q$

(2) 计算 $r_1 = g^{k_1} (\mathrm{mod}\ p)$　　(1)

(3) 计算 $s_1 = x_1 H(m) - k_1 H(y_1, \mathrm{ID}_2, T_1, r_1) (\mathrm{mod}\ q)$　　(2)

于是,$\mathrm{sig}(\mathrm{ID}_1, M) = (s_1, r_1)$。

出票人 ID_1 的数字签名 $\mathrm{sig}(\mathrm{ID}_1, M)$ 的验证方程是

$$y_1^{H(m)} = r_1^{H(y_1, \mathrm{ID}_2, T_1, r_1)} g^{s_1} (\mathrm{mod}\ p)　　(3)$$

注意,根据票据法,票据必须记载收票人 ID_2。

2.3　第一背书人及其后手计算签名方法

如果收票人决定背书转让票据,填写有关内容后,可用以下方法计算背书的数字签名。收票人收到票据 m 和 $\mathrm{sig}(\mathrm{ID}_1, m)$ 后,验证数字签名的有效性。如果他以后在日期 T_2 决定把票据背书转让给他人 ID_3,数字签名计算如下:

(1) 选择一个随机数 k_2,$0 < k_2 < q$

(2) 计算 $r_2 = g^{k_2} (\mathrm{mod}\ p)$　　(4)

(3) 计算 $s_2' = x_2 H(m) - k_2 H(y_2, \mathrm{ID}_3, T_2, r_2) (\mathrm{mod}\ q)$　　(5)

(4) 计算 $s_2 = s_2' + s_1 (\mathrm{mod}\ q)$　　(6)

于是,$\mathrm{sig}(\mathrm{ID}_1, \mathrm{ID}_2, m) = (s_2, r_1, r_2)$。

它的验证方程是

$$(y_1 y_2)^{H(m)} = r_1^{H(y_1, \mathrm{ID}_2, T_1, r_1)} r_2^{H(y_2, \mathrm{ID}_3, T_2, r_2)} g^{s_2} (\mathrm{mod}\ p)　　(7)$$

以后的背书人计算数字签名的方法与第一个背书人的方法相同。于是,第 $n-1$ 个背书人的数字签名是:

$$\mathrm{sig}(\mathrm{ID}_1, \mathrm{ID}_2, \mathrm{ID}_3, \cdots, \mathrm{ID}_n, m) = (s_n, r_1, r_2, r_3, \cdots, r_n)$$

它的验证方程是:

$$(y_1 y_2 \cdots y_n)^{H(m)} = r_1^{H(y_1, \mathrm{ID}_2, T_1, r_1)} r_2^{H(y_2, \mathrm{ID}_3, T_2, r_2)} \cdots r_n^{H(y_n, \mathrm{ID}_{n+1}, T_n, r_n)} g^{s_n} (\mathrm{mod}\ p)　　(8)$$

定理:如果各个签名人都根据协议计算数字签名,那么各个验证人都会接受签名。

证明:由等式(2) 得

$$x_1 H(m) = s_1 + k_1 H(y_1, \mathrm{ID}_2, T_1, r_1) (\mathrm{mod}\ q)$$

如果对这个等式两边以 g 为底作指数运算,得

$$g^{x_1 H(m_1)} = g^{k_1 H(y_1, \mathrm{ID}_2, T_1, r_1)} g^{s_1} (\mathrm{mod}\ p)$$

把等式(1)和出票人的公钥代入,就得到验证方程(3)。

由等式(5)得,$x_2H(m) = k_2H(y_2, \mathrm{ID}_3, T_2, r_2) + s_2' \pmod q$

如果对这个等式两边以 g 为底作指数运算,得

$$g^{x_2H(m)} = g^{k_2H(y_2, \mathrm{ID}_3, T_2, r_2)} g^{s_2'} \pmod p$$

把等式(4)和第一背书人的公钥代入,得

$$y_2^{H(m)} = r_2{}^{H(y_2, \mathrm{ID}_3, T_2, r_2)} g^{s_2'} \pmod p$$

与等式(3)两边相乘,得

$$(y_1y_2)^{H(m)} = r_1{}^{H(y_1, \mathrm{ID}_2, T_1, r_1)} r_2{}^{H(y_2, \mathrm{ID}_3, T_2, r_2)} g^{s_1 + s_2'} \pmod p$$

把等式(6)代入,就得到验证方程(7)。从中可以看到票据转让的次序是:$\mathrm{ID}_1 \rightarrow \mathrm{ID}_2 \rightarrow \mathrm{ID}_3$。

同理可证验证方程(8)。从中可以看到票据转让的次序是:

$$\mathrm{ID}_1 \rightarrow \mathrm{ID}_2 \rightarrow \mathrm{ID}_3 \rightarrow \cdots \rightarrow \mathrm{ID}_{n+1} \qquad \text{Q.E.D.}$$

3 安全性讨论

(1) 式(3)是出票人 ID_1 的数字签名(s_1, r_1)的验证方程,它跟 Harn 研究的广义的 ElGamal 型数字签名协议[6]中的第一个方案 $y_1{}^{r_1} = r_1{}^{H(m)} g^{s_1} \pmod p$ 的区别是 r_1 的指数改成 $H(y_1, ID_2, T_1, r_1)$,我们作这样的改进的目的在于强调收票人 ID_2 和出票时间 T_1。由于票据内容包括 ID_2 和出票时间 T_1,这样可以提高协议抵御生日悖论攻击的能力。不过,为了防止同态攻击,出票人的会话密钥不可重复使用,或者产生较小系数的线性关系。

(2) 式(7)是第一背书人的数字签名(s_2, r_1, r_2)验证方程,这是使用两个秘密密钥和两个会话密钥的数字签名,它的安全性高于使用一个秘密密钥和一个会话密钥的数字签名。假设攻击者还截获出票人 ID_1 的数字签名(s_1, r_1)。那么由等式(6)攻击者还可以算出(s_2', r_2),它满足等式 $y_2{}^{H(m)} = r_2{}^{H(y_2, \mathrm{ID}_3, T_2, r_2)} g^{s_2'} \pmod p$,它跟 Harn 研究的广义的 ElGamal 型数字签名协议[6]中的第一个方案 $y_2{}_2^{H(m)} = r_2{}^{r_2} g^{s_2} \pmod p$ 相比,有一个区别,即用 $H(y_2, \mathrm{ID}_3, T_2, r_2)$ 代替了 r_2,因而提高了安全性。

(3) 最近,Li 等人提出一种针对多重签名的内部人攻击[7]。一个内部签名人故意选择一个假公钥 $y_1 = g^u \prod_{i=2}^{n} y_i^{-1} \pmod p$,其中,$u$ 是他选择的整数。于是,$g^u = y_1y_2\cdots y_n \pmod p$,内部人就可以伪造多重签名。

有两种方法可抵御内部人的攻击,如果证书机构在作公钥证书前,要求申请人用申请的密钥签名,就可以发现假公钥;否则,多重签名的验证公式中,$y_1y_2\cdots y_n$ 必须改为 $y_1{}^{y_1} y_2{}^{y_2}\cdots y_n{}^{y_n}$。但这样一来,验证计算显著增加。

4 性能分析

(1) Harn 等人在研究多重签名的性质时[2],曾经提出最优多重数字签名应该具有两条性质:一是多重数字签名的长度等于单个数字签名的长度;二是多重数字签名的验证计算量等于单个数字签名的验证计算量。

在我们设计的随机有序多重签名协议中,多重数字签名的长度等于数字签名的重数加 1,多重数字签名的验证中指数运算次数等于数字签名的重数加 1。即,第一个签名的长度和验证中指数运算次数都是 2,以后每增加一个签名,这两个量都增加 1。然而,这两个量是同样重数的 ElGamal 型数字签名的相应量的一半。

因此,这个多重数字签名协议还未达到最优多重数字签名的性质,但是,目前还没有一个 DSA 类型的多重数字签名协议达到这个最优的性质。不过,我们还可以使用多指数计算方法[8]进一步减少验证计算量。

所幸的是,在实际商务活动中,票据背书转让的次数较少,一般只转让一次。在我国的票据印刷格式上,背书转让的次数是 1 ~ 3 次。有的票据制度甚至规定票据只可背书转让一次。比如国际商会的《跟单信用证统一惯例》规定,"可转让信用证只可转让一次"。因此,我们设计的随机有序多重签名协议跟最优多重数字签名相比,性能上没有实质性的差别。

在文献[6]中,Harn 把广义的 ElGamal 型数字签名协议的签名方程表示为 $ax = bk + c \pmod{p-1}$,其中,(a, b, c) 可以是(m, r, s)的数学组合。如果要满足最优多重数字签名的两条性质。x 应该是各个签名的私钥

的乘积,k 应该是各个签名的会话密钥的乘积。由于模加法和模乘法都满足交换律,无法表示出随机有序多重签名中的有序性。

(2) 我们设计的随机有序多重签名协议是一种更广泛的多重数字签名协议的特殊情况。

假设第一个签名人要对信息 m 签名 sig_1,第二个签名人要对信息(m,sig_1,m_2) 签名 sig_2,…… 第 n 个签名人要对信息$(m,\mathrm{sig}_1,m_2,\cdots,m_n)$ 签名 sig_n。

只要对第二节签名算法稍加修改,就可得到第 n 个签名人的签名

$$\mathrm{sig}_n = (s_n, r_1, r_2, \cdots, r_n)$$

它的验证方程是

$$(y_1 y_2 \cdots y_n)^{H(m)} = r_1^{H(y_1,m_1,r_1)} r_2^{H(\mathrm{ID}_1,y_2,m_2,r_2)} \cdots r_n^{H(\mathrm{ID}_{n-1},y_n,m_n,r_n)} g^{s_n} (\mathrm{mod}\ p)$$

其中 m_1 是信息 m 中最敏感的部分。

如果说,票据背书转让中数字签名的次序是指定后手,那么这里的签名的次序是指定前手。例如,票据的保证和票据的承兑时应该指定出票人,使用的数字签名要指定前手。

在一般的组织机构中,管理是分层次的。在这样的层次机构中,一项公文的逐级审批制度就是采用指定前手的随机有序多重签名。每个管理层都要签署自己的意见 m_i 和签名。只有在审查了前面各层的意见 m,$m_2,\cdots,m_{i-1}$,第 i 层才签署自己的意见 m_i 和签名。

更一般的随机多信息多签名协议的验证方程是

$$(y_1 y_2 \cdots y_n)^{H(m)} = r_1^{H(y_1,m_1,r_1)} r_2^{H(y_2,m_2,r_2)} \cdots r_n^{H(y_n,m_n,r_n)} g^{s_n} (\mathrm{mod}\ p)$$

每个签名人可以在自己的意见 m_i 中,根据自己的需要说明自己的前后次序。

我国政府的组织结构属于层次机构的模式,因此,本文设计的有序多重签名协议可以直接应用到电子政务中。本文设计的多重签名协议不仅可用于电子票据的保护,也可用于传统的纸质票据的保护。

参考文献:

[1] Diffie W, Hellman M E. New directions in cryptography[J]. IEEE Trans.,1976,(IT-22):644-654.

[2] Harn L. Group-oriented (t,n) threshold digital signature scheme and digital multisignature[J]. IEE Proc-Comput Digit Tech,1994,141(5):307-313.

[3] Harn L. New digital signature scheme based on discrete logarithm[J]. Electronics Letters,1994,30(5):396-398.

[4] Okamoto T. A digital multisignature scheme using bijective public-key cryptosystems[J]. ACM Trans on Comp Systems,1988,6(8):432-441.

[5] 纪家惠,赵仁杰.基于 Schnorr 体制的数字多签名体制[A].密码学进展——CHINACRYPT[C].北京:科学出版社,1996.170-176.

[6] Harn L. Design of generalised ElGamal type digital signature scheme based on discrete logarithm[J]. Electronics Letters,1995,31(20):2025-2026.

[7] Li Z C, Hui L C K, Chow K P, *et al*. Cryptoanalysis of Harn digital multisignature scheme with distinguished signing authorities[J]. Electron Lett,2000,36(4):314-315.

[8] Yen S M, Lain C S, Lenstra A K. Multi-exponentiation[J]. IEE Proc-Comput Digit Tech,1994,141(6):325-326.

Multisignature scheme for endorsement

SHAO Zu-hua

(Dept. of Computer and Electronic Engineering, Zhejiang University of Science and Technology, Hangzhou 310012, China)

Abstract: This paper studies the security properties of signatures for endorsement in business, designs a random order multisignature scheme based on discrete logarithms. Furthermore, the paper proposes a generalized hierarchical system for document examination and approval, which can be applied to e-government.

Key words: cryptography; multisignature; endorsement; e-government