文章编号: 1005－0523(2009)01－0039－04

一种基于椭圆曲线的多重数字签名方案

左黎明

(华东交通大学 基础科学学院,江西 南昌 330013)

摘要:对基本的椭圆曲线数字签名算法 (ECDSA)进行了改进,提出了一种新的基于椭圆曲线的多重数字签名方案.该方案能够允许多个用户按顺序地对一份文件进行签名,最后形成一个群体签名.并提出一种新的签名验证方案,可以有效地防止成员的欺诈行为.签名者可以通过验证操作发现伪签名,同时签名中心可以及时通过签名者提供的失败信息查找原因并进行处理,签名中心还可验证签名者公钥的有效性以防止成员内部的欺诈行为.方案充分利用椭圆曲线密码体制密钥小、速度快等优点,降低了通信成本,因而更具有安全性和实用性.

关 键 词:离散对数问题;椭圆曲线;数字签名

中图分类号: TP393 **文献标识码**: A

数字签名方案一般建立在某种公钥系统基础之上,而这种公钥系统的安全依赖于某种数学问题的求解困难性.目前已有的数字签名方案大多依赖于求解大数分解问题和一般有限域离散对数问题 (DLP),而基于半环上的代数分解问题和椭圆曲线域离散对数问题 (ECDLP)的方案比较少.利用椭圆曲线域离散对数问题 (ECDLP)来构造数字签名方案有许多优点:

(1) 由于有限域 F_q 上的可以使用的安全椭圆曲线有许多,同时求解椭圆曲线离散对数问题 (ECDLP)比有限域离散对数问题 (DLP)困难得多;

(2) 椭圆曲线公钥密码系统中的主要计算量是计算 $Q=kg$ 这是一个单向陷门;

(3) 在同等安全条件下,要获得同样的安全强度,密钥长度要比其它算法短,开销较少且速度快,同时也易于硬件实现.

基于以上原因,基于椭圆曲线的数字签名方案将逐步取代各种基于大数分解问题和一般有限域离散对数问题的数字签名方案,本文提出了一种新的基于椭圆曲线域离散对数问题 (ECDLP)的多重数字签名方案.

1 基于一般 DLP的数字签名算法及其变型

基于 DLP的各种数字签名方案,其签名算法一般原理如下:首先选择一个大素数 p然后选择 GF(p)的本原根 g, $q=p-1$,私钥 $x\in[1, q]$,公钥为 $y=g^x \bmod p$ 对消息 m签名时,取满足 $\gcd(k, q)=1$的随机数 k计算 $r=g^k \bmod p$ 大部分使用 DLP来构造的数字签名方案一样基于以下一般的签名等式

$$ax=bk+c \bmod q \tag{1}$$

签名验证等式为

$$y^a=r^b g^c \bmod p \tag{2}$$

其中: a、b、c为系数,是 (m, r, s)的一个置换,根据系数 a、b、c取值的不同,可以推导出如下 6种基本类型的

收稿日期: 2008－08－15

作者简介:左黎明 (1981－),男,江西鹰潭人,理学硕士,软件工程师,讲师,研究方向为信息安全、非线性系统.

签名方程

$r=s+mx(\mathrm{mod}\ q)$ $r=m+sx(\mathrm{mod}\ q)$ $sk=r+mx(\mathrm{mod}\ q)$

$sk=m+rx(\mathrm{mod}\ q)$ $mk=s+rx(\mathrm{mod}\ q)$ $mk=r+sx(\mathrm{mod}\ q)$

若包含扩展型，Ham和 Xu指出共有 18种安全广义 ElGamal型数字签名方案[1]，另外 Nyberg和 Rueppel给出了 6种具有消息自动恢复特性的签名方案[2]. 椭圆曲线数字签名与 ElGamal数字签名很相似，只是椭圆曲线数字签名是基于椭圆曲线离散对数问题 (ECDLP)，而 ElGamal数字签名是基于一般有限域的离散对数问题 (DLP). 从上述 6种不同基本类型的签名方程可以直接推广得到 6种不同类型的基本椭圆曲线签名方程. Nyberg和 Rueppel的 6种具有消息自动恢复特性的签名方案也可做类似推广.

2 椭圆曲线签名算法 ECDSA及其改进

设椭圆曲线公钥密码系统参数为 (F_q, E, g, n, a, b, h)，其中 F_q是有限域，E是 F_q上的椭圆曲线，g是 E上的一个基点，n是椭圆曲线 E的阶，a，b是椭圆曲线 E的系数，h是一个小的素数.

2.1 密钥生成

签名者 A随机选择一个整数 x_A，作为私钥，公钥是 $y_A=x_Ag$.

2.2 签名过程

(1) A随机选取一个整数 k，其中 $1<k<n$，计算 $kg=(x_1, y_1)$，$r=x_1 \mathrm{mod}\ n$;

(2) 设 m为消息，计算散列值 $e=h(m)$，其中 $h(m)$为安全 hash函数;

(3) 计算 $s=k^{-1}(e+rx_A)\mathrm{mod}\ n$，则 m的签名为 $(s\ r)$.

2.3 签名的验证

(1) 验证者 B计算散列值 $e'=h(m)$;

(2) B计算 $u=s^{-1}e'$，$v=s^{-1}r$;

(3) $(x_2, y_2)=ug+vy_A$，$r'=x_2 \mathrm{mod}\ n$;

(4) 如果 $r'=r$则签名验证成功.

2.4 ECDSA方案实现中的计算性能分析

从上面的签名算法可以知道，为了计算 s的值，必须计算 k^{-1}，对一个大整数求逆，若采用扩展欧几里德算法来求逆，平均需完成 $O(\log_2(n))$次除法，影响了整个签名算法的速度.

2.5 一种改进的快速签名方案

从以上对 ECDSA的分析可知，如果我们可以避免求逆运算，则可提高数字签名算法的效率. 这里我们给出一种新的构造快速数字签名方案的方法 (相关参数如 ECDSA中说明)

$$e^{-1}k=s+rx_A(\mathrm{mod}\ n) \tag{3}$$

两边同乘以 e得

$$k=es+erx_A(\mathrm{mod}\ n) \tag{4}$$

因为是 $e=h(m)$已知签名发起方和验收方都知道的消息 m的散列值，令 $\bar{s}=es$可以用 $(\bar{s}\ r)$代替 $(s\ r)$作为对消息 m的签名，于是我们可以得到一个新的签名方程

$$k=\bar{s}+erx_A(\mathrm{mod}\ n) \tag{5}$$

用这个签名方程来构造一个改进的快速签名方案，步骤如下

(1) 签名者 A在 E上选择私钥 x_A，g为 E的基点，计算公钥 $y_A=x_Ag$，计算 $e=h(m)$;

(2) A选择随机整数 k，$1<k<n$，并计算 $r=kg=(x_1, y_1)$，$r=x_1 \mathrm{mod}\ n$，且 $s=k-erx_A(\mathrm{mod}\ n)$;

(3) $(r\ s)$作为对消息 m的签名，并将 $(s\ r\ e)$发送给验证者 B;

(4) B计算 $(x_2, y_2)=sg+ery_A(\mathrm{mod}\ n)$，$r'=x_2 \mathrm{mod}\ n$，如果 $r'=r$则签名验证成功.

以上方案避免了 ECDSA算法的求逆过程，比 ECDSA算法简单. 实验结果表明，若选择同样的参数条件，该方案可以提高数字签名算法的速度 10%以上.

3　一种基于椭圆曲线的多重数字签名方案

利用 2.5中改进的数字签名方案的思想,本文给出一种新的基于椭圆曲线的多重数字签名方案.该签名方案由可信任的秘密分发中心 SDC(Shared Distribution Center)选择系统参数,有 t个签名者 $\{A_i\}$ (i=1, 2, …, t)参与对消息 m进行签名.整个方案由系统初始化、多重签名生成、多重签名验证共 3个阶段组成.

3.1　系统初始化

设椭圆曲线公钥密码系统参数为 (F_q, E, g, n, a, b h),其中 F_q是有限域, E是 F_q上的椭圆曲线, g是 E上的一个基点, n是椭圆曲线 E的阶, a, b是椭圆曲线 E的系数.

SDC选择 t个随机整数 k_1, k_2, …, k_t,计算 $k=\sum_{i=1}^{t} k_i$,将 k和 k_1, k_2, …, k_t保密.再计算: r=kg=(x_0, y_0),散列值 e=h(m+x_0+y_0), w=e⊙g. SDC通过可信信道把 w和 k_i发送给签名者 A_i(i=1, 2, …, t),并将参数 g, e, r公开.签名者 A_i(i=1, 2, …, t)选择 1个随机整数 v_i作为自己的私钥,计算自己的公钥 $u_i=v_i g$和 $c_i=w+u_i$,并将 u_i公开.

3.2　多重签名生成

签名过程由 SDC发起,签名顺序为: SDC→A_1→A_2→…→A_t→B,每个签名者 A_i依次进行签名,最终签名将由 A_t提交给验证者 B.

签名者 A_i接收到了签名者 A_{i-1}发来的 (e c_{i-1}, $\bar{r}_{i-1}$, $\bar{s}_{i-1}$),执行以下操作:

(S1)验证 $u_{i-1}+w=c_{i-1}$是否成立,若不成立,拒绝签名;若成立,转向执行 (S2);

(S2)计算 $r_i=k_i g=(x_i, y_i)$, $s_i=k_i-ex_i v_i \pmod n$, $\bar{r}_i=\bar{r}_{i-1}+r_i$, $\bar{s}_i=\bar{s}_{i-1}+s_i$其中 $\bar{r}_1=r_1$, $\bar{s}_1=s_1$, A_i公开 (r_i, s_i),此时显然有: $\bar{r}_i=r_1+r_2+\cdots+r_i$, $\bar{s}_i=s_1+s_2+\cdots+s_i$;

(S3)若 $1\leqslant i<t$ A_i将 (e c_i, $\bar{r}_i$, $\bar{s}_i$)发送给 A_{i+1}, A_{i+1}转向执行 (S1),若 i=t则转向执行 (S4);

(S4) A_t将 (e c_t, $\bar{r}_t$, $\bar{s}_t$)发送给签名验证者 B,完成签名过程.

3.3　多重签名验证

验证者 B收到最终签名 (e c_t, $\bar{r}_t$, $\bar{s}_t$)后,执行以下操作:

(SS1)首先判断 $\bar{r}_t=r \pmod n$是否成立,若不成立,拒绝签名,若成立,执行执行 (SS2);

(SS2)查询签名者 A_i(i=1, 2, …, t)公钥 u_i和部分签名 (r_i, s_i),验证 $r=\bar{r}_t=\bar{s}_t g+\sum_{i=1}^{t}(ex_i u_i) \pmod n$是否成立,若成立,则接受签名.

3.4　签名验证过程的正确性与方案的安全性分析

(1)若签名者都是诚实的,则必有

$$\bar{r}_t=\sum_{i=1}^{t}(s_i g+ex_i u_i)=\sum_{i=1}^{t}[(k_i-ex_i v_i)g+erx_i u_i]=\sum_{i=1}^{t}k_i g=g\sum_{i=1}^{t}k_i=kg=r \pmod n$$

(2)本方案是基于椭圆曲线的数字签名方案在抵抗被动攻击中,即使攻击者知道了签名者 A_i的公钥 u_i,要解出 u_i的秘钥 v_i,或者是知道公开的 r或 r_i,要解出 k或 k_i,都相当于求解椭圆曲线离散对数问题,这比解大整数因式分解和一般有限域离散对数问题要困难的多;

(3)通过 t个签名者的签名才是有效签名,多于或少于 t个签名无效,最终验证者验证签名同时使用了每个签名者的部分签名和最终的多重签名,可以发现签名过程中的恶意攻击者;

(4)签名者既签名又验证前一个签名者的签名真实,所以能够有效防止代换攻击和中间人攻击.

3.5方案实现中的若干问题

针对一般的 ECDLP问题,主要有两种比较有效的攻击算法[3]: Pohlig—Hellman方法和 Pollard—ρ方法.但是对于超奇异椭圆曲线 (设 F_q的特征为 p E/F_q的 q阶 Frobenius变换的迹 t是 p的倍数时, E称为超奇异的),采用 MOV算法和 FR算法等亚指数概率攻击算法可以很好的求解此类曲线的 ECDLP.另外,还有一类特殊椭圆曲线是异常 (anomalous)椭圆曲线 (设 $q=p^m$, $p\neq 2, 3$为素数, E/F_q由方程 $y^2=x^3+ax+b$定义,阶为 p当 p=q时,异常曲线上的 p阶 Frobenius变换的迹 t=1),使用 Semaev-Smart-Satoh-Araki算法可以较好

的求解此类曲线的 ECDLP.

通过以上分析,要保证椭圆曲线密码系统的安全性,就要使所选取的曲线能抵抗上述关于 ECDLP求解算法的攻击,目前如何选取最合适的曲线是一个理论难题,在本方案的实现中,参考 IEEE1636等标准来产生一条椭圆曲线:

(1)为了对抗 Pollard-ρ算法攻击,所选取 EC的阶 $\#E(GF(q))$的分解式中应该包含一个较大素因子,应不小于 160 bit;

(2)为了抗击 Weil对和 Tate对的攻击,对于 $1\leqslant k\leqslant 30$, n不能除 q^k-1,不宜选取超奇异椭圆曲线;

(3)为了抗击 Semaev-Smart-Satoh-Araki算法的攻击所选曲线的阶不能等于该曲线所定义的有限域的阶,即 $\#E(F_q)\neq q$,不宜选取异常椭圆曲线;

(4)若选取二进制域 $GF(2^m)$,度 m最好为素数.

椭圆曲线密码体制应用中的大量运算是倍乘(数乘),为了提高程序的运行速度,在实现中,椭圆曲线上点的运算采用复乘(Complex Multiplication)算法,速度可以提高 10%左右,如果采用多标量乘法,速度可以提高 15%~20%.

4 结语

对标准椭圆曲线签名方案进行了改进,消除模逆运算,在此基础上构造出一种多重数字签名方案并分析了它的安全性.从分析得出,它比文献[4,5]中提出的基于 RSA和基于 Schnorr算法的多重签名方案更安全有效,计算复杂性更小,易于在电子商务和电子政务系统中使用.

参考文献:

[1] Ham L, Xu Y. Design of generalized ElGamal type digital scheme based on discrete logarithm [J]. Electronics letters, 1994, 30(24): 2 025-2 026.

[2] Nyberg K, Rueppel R A. Message recovery for signature scheme based on the discrete logarithm problem [J]. Designs Codes and Cryptography, 1996, 7(1): 61-81.

[3] 张龙军,沈钧毅,赵 霖.椭圆曲线密码体制安全性研究 [J].西安交通大学学报, 2001, 35(10): 1 038-1 041.

[4] 张键红,韦永壮,王育民.基于 RSA的多重数字签名 [J].通信学报, 2003, 24 (8): 150-155.

[5] 褚红伟,葛 玮.基于 Schnorr算法的多重数字签名方案 [J].计算机工程, 2005, 23(1): 129-130.

A Digital Multi-signature Scheme Based on the Elliptic Curve

ZUO Li-ming

(School of Basic Sciences, East China Jiaotong University, Nanchang 330013, China)

Abstract: The basic elliptic curve digital signature algorithm (ECDSA) is improved and then a new multi-signature scheme based on the elliptic curve cryptosystem is presented. It can allow multiple users to sign the same document orderly and finally to form a group signature. Furthermore, a new signature verification scheme is proposed, which can prevent members of the fraud effectively. The signer can find false signature through the verification operation. At the same time, according to the failure information the signature center can find the reasons and deal with it in time. It also can verify the validity of signer's public key to prevent members of the internal fraud. The scheme takes full advantage of elliptic curve cryptosystem features such as small private keys, speed, etc. Reducing the costs of communication, the scheme is safer and more practical.

Key words: discrete logarithm problem; elliptic curve; digital signature

(责任编辑:刘棉玲)