失败—停止签名方案研究

王平水
(安徽财经大学 信息工程学院,安徽 蚌埠 233041)

摘 要:普通的数字签名方案的安全性几乎都依赖于一个计算假设。为了防止具有无限计算能力的攻击者成功伪造签名,以保护签名者的利益,提出了一个新的更为高效的失败—停止签名方案。方案中使用了两个数学上的困难问题:离散对数和因子分解,从而为接收者提供安全性。该方案具有可证明的安全性以抵抗自适应选择明文攻击。分析比较结果表明该方案在消息长度与签名长度比率方面是最优的,对长消息签名是高效的。

关键词:失败—停止签名;丛同态;离散对数;因子分解;效率
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2008)06-0138-04

Research on Fail-Stop Signature Schemes

WANG Ping-shui
(College of Information Engineering, Anhui University of Finance & Economics, Bengbu 233041, China)

Abstract: Security of ordinary digital signature schemes almost relies on a computational assumption. To prevent a forger with unlimited computational power from forging a signature and protect the signer's benefit, a new and efficient fail-stop signature scheme was proposed. Two hard problems were used, discrete logarithm and factorization, as the basis of receiver's security. The scheme provides provable security against adaptively chosen plaintext attack. As is shown that it is the most optimal scheme with respect to the ratio of the message length to the signature length and is efficient in signing long messages based on the results of analyzing and comparing.

Key words: fail-stop signature; bundling homomorphism; discrete logarithm; factorization; efficiency

0 引 言

数字签名是电子世界最重要的认证技术之一。普通的签名方案始终保持在可计算的水平,因此一个具有无限计算能力的攻击者能够成功伪造一个签名。为了提供一种保护机制以防止一个具有无限计算能力的攻击者成功伪造签名,多种失败—停止签名(以下简称FSS)方案被提出[1-3]。在FSS方案中,如果签名被伪造,签名者能够提供一种证据表明伪造已经发生,并及时停止此签名系统,使得具有无限计算能力的对手的伪造无法成功,因此被命名为失败—停止签名方案。因此,一个失败—停止签名方案提供了一种更高的安全性。

文献[1]基于离散对数困难问题提出了一个高效的FFS方案,这是当时所知的最为高效的方案,被称为vHP方案。文献[2]给出了FFS方案的正式定义,使用丛同态思想定义了方案的一般结构,这一结构的重要特性是能够抵抗"自适应选择明文攻击"并提供了可证明的安全性。文献[3]提出了一个基于RSA的FFS方案,使用了因子分解困难问题,通过揭露模数的非平凡因子来证实伪造的发生。

我们在已有FFS方案的基础上提出了一个新的FFS方案,该方案的安全性基于两个广为接受的计算假设:离散对数困难问题和因子分解问题。介绍了一种与通信带宽的高效使用有关的新的效率量度标准,表明我们的方案设计的比vHP方案还要好(包括所有基于因子分解问题的其它方案)。在最优性与效率方面将此方案和vHP方案进行了比较。

1 预备知识

1.1 失败—停止签名的回顾

与一般的签名方案类似,失败—停止签名方案也包含一个多项式时间密码协议(即密钥产生、签名过程、验证签名)和两个多项式时间算法(即证明伪造、证伪—验证)。

一个安全的FFS方案必须具备以下性质[4]:

① 正确性:接收方必须能够通过相应算法验证签

收稿日期:2007-09-15
基金项目:安徽省自然科学基金资助项目(2006KJ017C)
作者简介:王平水(1972-),男,安徽萧县人,硕士,副教授,研究方向为数据库与网络信息安全。

名者对消息的签名。

② 接收方的安全性:一个多项式计算能力的攻击者无法建立能够成功通过验证算法的伪造签名。

③ 签名者的安全性:当一个具有无限计算能力的攻击者成功伪造了能够成功通过验证算法的签名时,签名者能够证实伪造,并使第三方确信伪造确已发生。

④ 不可否认性:一个多项式计算能力的签名者不能否认他自己对消息的签名。

FFS的安全性是可被攻破的,如果签名者能够构造一个签名,这种签名后来被证实是一个伪造;或者一个具有无限计算能力的攻击者能成功构造一个签名,而签名者又不能证实其是伪造的。这两种类型的伪造是完全独立的,因此有两个不同的安全参数:k 和 σ,用于表示抵抗两类攻击的安全级别。特别地,用 k 表示接收方的安全性,σ 表示签名者的安全性。可以证明,一个安全的FFS能够抵抗"自适应选择明文攻击",对于任意 $c>0$ 和足够大的数 k,一个多项计算能力的攻击者成功的可能性是 k^{-c};对于一个签名者安全参数为 σ 的FFS,一个具有无限计算能力的攻击者成功的可能性为 $2^{-\sigma}$。

1.2 失败—停止签名的一般构造方法

文献[2]使用丛同态构造了FFS方案,丛同态可被看作是一种特殊类型的Hash函数。

定义1　一个丛同态 h 是两个阿贝尔群 $(G,+,0)$ 和 $(H,\times,1)$ 之间满足如下条件的一个同态:

(1) 每个映像 $h(x)$ 至少有 2^{τ} 个前像,2^{τ} 被称为这个同态的度。

(2) 找出碰撞在多项式时间内是不可行的。

为了给出一个更为精确的定义,需要考虑两个群组:$G=(G_K,+,0)$ 和 $H=(H_K,\times,1)$,以及一个阶为 K 的多项式时间函数,K 的值是由应用中根密钥产生算法 $g(k,\tau)$ 决定的,其中 k 和 τ 作为两个输入参数,这两个参数决定了找出碰撞的难度和该丛同态的度。给定一对输入参数 $k,\tau\in N$,首先使用根密钥产生算法 $g(k,\tau)$ 计算出 K,然后再进一步确定 G_K,H_K 和 h_K。以下简述使用丛同态来构造FFS的一般方法。

令 k 和 σ 为FFS的两个安全参数已给定,丛同态的度 τ 可由关于 σ 的函数来确定。

① 根密钥产生:计算根密钥 $K=g(k,\tau)$,由此可确定群 G_K 和 H_K 和一个同态 h_K,令 $G=G_K,H=H_K,h=h_K$。

② 根密钥验证:签名者必须确保 K 是算法 $g(k,\tau)$ 的一个可能的输出,为此可提供一个关于 K 的零知识证明或者由签名者加以测试,在任何情况下,一个坏密钥被接受的可能性最大为 $2^{-\sigma}$。

③ 主密钥产生:签名者随机地选择 $sk_1,sk_2\in G$ 以产生他的秘密密钥 $sk=(sk_1,sk_2)$,并计算公开密钥 $pk=(pk_1,pk_2)$,其中 $pk_i=h(sk_i),i=1,2$。

④ 签名过程:对于消息 $m\in M$ 的签名为 $s=\mathrm{sign}(sk,m)=sk_1+m\times sk_2$,$M$ 为消息空间。

⑤ 验证签名:验证 $pk_1\times pk_2^m=h(s)$ 是否成立。

⑥ 产生伪造证据:给定消息 m 的一个可接受的签名 $s'\in G$,使得 $s'\neq\mathrm{sign}(sk,m)$,签名者计算 $s=\mathrm{sign}(sk,m)$ 和 $\mathrm{proof}=(s,s')$。

⑦ 验证伪造证据:给定一对 $(x,x')\in G\times G$,验证 $x\neq x'$ 和 $h(x)=h(x')$ 是否成立。

对于任意的丛同态和选择的任意参数 k 和 σ 构造的FFS方案满足如下性质:

① 能够产生正确的签名。

② 一个多项式时间计算能力的签名者不能构造一个有效签名及一个伪造证据。

③ 如果一个签名 $s^*\neq\mathrm{sign}(sk,m)$ 是可接受的,则签名者能够构造一个伪造证据。

而且对于两个选定的安全参数 k 和 σ,一个好的根密钥 K 以及两个消息 $m,m^*\in M$,在 $m\neq m^*$ 的情况下,令 $T:=\{d\in G\mid h(d)=1\wedge(m^*-m)d=0\}$,对于给定签名 $s=\mathrm{sign}(sk,m)$ 和一个伪造签名 $s^*\in G$,如果 $\mathrm{test}(pk,m^*,s^*)=\mathrm{ok}$,则 $s^*=\mathrm{sign}(sk,m^*)$ 的可能性最多为 $|T|/2^{\tau}$,从而一个具有无限计算能力的攻击者伪造签名成功的可能性也最多为 $|T|/2^{\tau}$。因此,在选择安全级别参数 σ 时,必须确保 $|T|/2^{\tau}\leqslant 2^{-\sigma}$。

2 FFS方案

2.1 方案描述

简单起见,首先在单一接收方模式下描述文中的方案。然后再将其扩展到多接收方模式。

① 根密钥的产生:首先,在给定安全参数 k 和 σ 的情况下,R 选择两个大的安全素数 p 和 q,然后,R 选择一个素数 p 使得 $n=pq$ 整除 $p-1$,最后,R 选择一个元素 α 使得 α 在模 p 下的阶为 p(即 $\mathrm{ord}_p(\alpha)=p$)。将 α,n 和 p 通过安全通道发送给签名者(α 称为根密钥)。

② 根密钥的验证:如果接收方是可信任的,根密钥将被签名者 S 所接受,没有根密钥的验证也行。另一方面,如果接收方是不可信任的,根密钥的正确性将需要一个零知识证明加以保证。

③ 主密钥产生:S 选择 $k_1,k_2\in Z_n$ 并计算 $\alpha_1=\alpha^{k_1}\bmod p,\alpha_2=\alpha^{k_2}\bmod p$,则私有密钥为 (k_1,k_2),公开密钥为 (α_1,α_2)。

④ 签名过程:对消息 $x\in Z_n$ 进行签名,S 计算 y

$= k_1x + k_2 \bmod n$ 并公布他对消息 x 的签名 y。

⑤ 验证签名：如果 $\alpha^y \stackrel{?}{=} \alpha_1^r \alpha_2 \bmod p$ 成立，则签名 y 通过验证。

⑥ 证明伪造：假设发送者对该消息产生的签名为 y，如果有一个伪造的签名 y' 成功通过上述验证，则有如下等式成立：$\alpha^y = \alpha^{y'} \bmod p$ 或者 $y = y' \bmod p$，$y = y' + cp$，$c \in Z$。因此，可以通过计算 $\gcd(y - y', n)$ 得到 n 的一个非平凡因子。注意到 $y = y'$ 的可能性为 $1/q$。

对密钥产生算法作如下说明。随机选择 n 和 p 使得 $n \mid p-1$，如果 $\mid n \mid_2 = k$，则大概平均需要 $O(\log k)$ 步就可找到一个这样的 p。选择一个元素 α 使得 $\mathrm{ord}_p(\alpha) = p$，这样的元素很容易找到。例如，随机选择一个 $\tilde{\alpha} \in Z_p^*$ 并计算出 $\alpha = (\tilde{\alpha})^{cq} \bmod p$，$c = \dfrac{p-1}{n}$。如果 $\alpha \neq 1$，则 α 在模 p 下的阶为 p。

2.2 安全性分析

首先给出支撑方案的相关安全性假设及丛同态的定义，然后对方案的安全性加以证明。

(1)离散对数假设。给定 $I = (p, \alpha, \beta)$，其中 p 为素数，$\alpha \in Z_p^*$ 为初值，$\beta \equiv \alpha^a \pmod p$，则计算离散对数 $a = \log_\alpha \beta$ 非常困难。

(2) 因子分解假设。给定 $n = pq$，其中 p 和 q 均为大素数，则在不知 $\phi(n) = (p-1)(q-1)$ 的情况下很难在多项式时间内找到 n 的一个非平凡因子。

(3) 强因子分解假设。给定 $n = pq$（p 和 q 均为大素数），$P = tn + 1$（$t \in Z$ 且 P 也是素数）和 $\alpha(\mathrm{ord}_p(\alpha) = p)$，则很难在多项式时间内找到的一个非平凡因子。

(4) 计算能力假设。在进行安全性分析时，还要对签名者和攻击者的计算能力做出假设。在数字签名研究中普遍接受的假设是签名者具有有限的多项式时间计算能力，而攻击者具有无限计算能力。

(5) 离散对数同态。

① 密钥产生：通过输入 k 和 τ，两个大素数 p 和 q，且 $\mid q \mid_2 = \tau$，$\mid p \mid_2 \approx \mid q \mid_2$，一个素数 P 使得 $n \mid P-1$，$\mid n \mid_2 = k$，很容易得到阶为 p 的元素 α。由此得到密钥 $K = (p, q, \alpha, P)$。

② 选取群组：令 $n = pq$，定义 $G_K = Z_n$，$H_K = Z_p^*$。

③ 定义同态：$h_{(p,q,\alpha,P)}: Z_n \to Z_p^*$，$h_{(p,q,\alpha,P)}(x) = \alpha^x \pmod P$。

定理 1　在离散对数假设和强因子分解假设下，上述构造是一个丛同态。

为了表明上述构造是一个丛同态，必须证明它具有以下 3 个性质[5,6]，证明过程从略。

① 对于任意 $\mu \in Z_p^*$，其中 $\mu = \alpha^c \pmod P$，则 μ 在 Z_n 中至少有 q 个前像。

② 对于给定的 $\mu \in Z_p^*$，其中 $\mu = \alpha^c \pmod P$，要找到 c 使得 $\alpha^c = \mu \pmod P$ 在多项式时间内是不可行的。

③ 不可能在多项式时间内找到两个不同的 $\tilde{c}, c \in Z_n$ 被映射到同一个值，即找出一个碰撞。

定理 2　提出的 FFS 方案对签名者来说是安全的。

根据定理 1[2]，必须在 Z_p^* 中找出集合 T 的大小。

$T := \{d \in Z_n \mid \alpha^d = 1 \Leftrightarrow (m^* - m)d = 0\}$ 或者 $T := \{d \in Z_n \mid \alpha^d = 1 \Leftrightarrow m'd = 0\}$

这里有 q 个 d 满足第一个等式 $\alpha^d = 1 \bmod P$。既然 $m^* \neq m$，就有 $m' \in \{1, 2, \cdots, n-1\}$，并且仅有唯一的消息（设为 $m' = q$）满足 $m'd = 0 \pmod n$。因此 $\mid T \mid = 1$。

结合定理 2[2]，在提出的方案中足可以选择安全参数 $\tau = \sigma$。

2.3 多接收者方案

虽然上述描述的 FFS 方案仅限于单一接收者，但是将其扩展到多接收者模式并非困难。事实上，两者仅仅区别在包含一个信任中心和提供零知识证明来表明根密钥所选参数是正确的。也就是说，需要确保参数 n，p 和 α 的选择符合所要求的形式。虽然很容易证明 α 的阶是 p 的一个倍数，但是，要证明阶 α 的阶就是 p 还需要很大的努力，能够完成关于 $\mathrm{ord}_p(\alpha) = p$ 的零知识证明。

更精确地讲，证明者必须证明他知道满足 $\alpha^p = 1 \bmod P$ 的 p，p 是一个大素数。另一方面，验证这一证明后，接收者只需要检验 $\alpha^n = 1 \bmod P$ 是否成立，因此，也就证明了 $\alpha^p = 1 \bmod P$。

2.4 多重消息签名

现将文中方案进一步加以扩展，使得可用同一秘密密钥对多个消息进行签名。假设有 $t-1$ 个消息要签名。

签名者选择一个秘密密钥 $k_0, k_1, \cdots, k_{t-1} \in Z_n^*$ 并公布相应的公开密钥 $(\alpha_0, \alpha_1, \cdots, \alpha_{t-1}) = (\alpha^{k_0}, \alpha^{k_1}, \cdots, \alpha^{k_{t-1}})$，其中 $\alpha_i \in Z_p^*$，$i = 0, 1, \cdots, t-1$。

为了对一个消息 $x \in Z_n$ 签名，S 计算 $y = k_0 + k_1x + k_2x^2 + \cdots + k_{t-1}x^{t-1} \bmod n$，如果 $\alpha^y \stackrel{?}{=} \alpha_0 \alpha_1^x \alpha_2^{x^2} \cdots \alpha_{t-1}^{x^{t-1}} \bmod P$ 成立，则签名 y 通过验证。可以证明，签名者对 $t-1$ 个不同的消息签名具有无条件安全性。

3 最优性与效率

本部分的目的在于将文中提出的方案与目前已知的最好的FFS方案(vHP方案)在执行效率方面做一个比较。衡量一个失败—停止签名系统的效率主要涉及到三个参数的长度,即秘密密钥的长度、公开密钥的长度和签名的长度,以及在每种情形下的计算量。

为了比较两种FFS方案,重点考查两种方案提供的安全级别,找出三个长度参数的大小,以及用于签名和验证的运算量(以某种典型运算为度量标准)。

表1给出了当接收者和发送者的安全级别为 k 和 σ 情况下两种FSS方案的比较结果。系统中选择相同的 k 和 σ 值,决定三个长度参数的大小。这意味着接收者具有相同的安全级别(由参数 k 给出)被转化为不同大小的素数和模数空间。特别地,要达到151位子群离散对数的安全级别等同于1881位的RSA模数的因子分解。

表1　计算量与效率参数比较

	FFS_DL[1]	New FFS
公钥产生计算量(乘法)	$4K$	$4K$
签名过程计算量(乘法)	2	1
签名验证计算量(乘法)	$3K$	$4K$
秘钥长度(位)	$4K$	$4K$
公钥长度(位)	$2K$	$2K$
签名长度(位)	$2K$	$2K$
消息长度(位)	K	$2K$
K 最小值(位)	151	941
K 最小值(位)	1881	1881
基于的困难问题	离散对数	离散对数和因子分解

为了在vHP方案中找到符合要求的素数,假设安全参数 k 和 σ 已给定,首先,找出 $K = \max(k,\sigma)$,然后,选择素数 q 使得 $|q|_2 \geqslant K$。这个方案中从同态的度为 q,选择参 p 数使得 $q \mid p-1$,并且 $p-1/q$ 有上界(关于 K 的多项式)。$|p|_2$ 的大小必须依照标准的离散对数问题选择,为达到足够的安全性至少是1881位。然而,$|q|_2$ 的大小可低至151位。既然 $|p|_2$ 和 $|q|_2$ 在某种程度上是相互独立的,用 $\hat{K}$ 来表示 $|p|_2$。

在文中方案中,从同态的度和发送者的安全级别为 $|q|_2$,接收者的安全性由 Z_p^* 中离散对数问题和 n 因子分解的困难性决定。假设 $|p|_2 \approx |q|_2 \approx \frac{|n|_2}{2}$,那么,首先找出模数大小 N_k,因此,因子分解的困难性为 k。既然 $P \geqslant n$,那么 Z_p^* 中离散对数的困难性也将是 k,选择 $K = \max(\frac{N_k}{2},\sigma)$,$|q|_2 = K \approx |p|_2$ 并且 $P \geqslant n$,基于这些选择,发送者和接收者的安全级别至少为 σ 和 k。例如,对于 $(k,\sigma) = (151,151)$,首先找出 $N_{155} = 1881$,于是有 $K = \max(\frac{1881}{2},151) = 941$,因此,$|q|_2 \approx |p|_2 \approx 941$,$|n|_2 \approx |P|_2 \approx 1882$。既然 $|P|_2$ 可以选择得比 $|n|_2$ 更大些,用 $\hat{K}$ 来表示 $|p|_2$,因此,当 $|p|_2 \approx |n|_2$ 时,有 $\hat{K} \approx 2K$。

表1表明:由于子群上的离散对数问题,vHP方案中的 K 可低至151位,然而在文中方案中必须至少941位,vHP方案和方案中的 $\hat{K}$ 都必须至少1881位。

实际应用中,还需要考虑消息和签名的相对长度,如果消息和签名的长度分别用 $|x|_2$ 和 $|y|_2$ 来表示,则可用 $\hat{\rho} = |y|_2/|x|_2$ 度量方案的通信效率。例如,$\hat{\rho} = 1$ 意味着对1位消息签名时就会有1位的签名信息通过信道传送。

在文中方案中,消息和签名均取自 Z_n,因此 $\hat{\rho} = 1$。在vHP方案中,消息和签名分别取自于阶为 q 和 $2|q|_2$ 的子群,这意味着 $\hat{\rho} = 2$,因此对1位消息签名时就需传送2位的签名信息。在文献[2]的因子分解方案中,消息和签名长度分别为 ρ 和 $k+\rho+\sigma$,假设 $k = \rho$,则有 $\hat{\rho} > 2$。在文献[3]的RSA方案中,消息取自于 Z_n^*,签名的大小为 $4|n|_2$,则 $\hat{\rho} = 4$。表2概括了这些结果。

表2　有关消息长度的通信效率比较

	FFS_DL[1]	FFS_Fact[2]	FFS_RSA[3]	New FFS
$\hat{\rho}$	2	>2	4	1

表1和表2表明:vHP方案和文中方案对签名算法输入的大小分别为 K 和 $2K$,即至少为151位和1882位,对于更长的消息可采取先Hash再加密的方法。对一个长度为 $l(151 < l < 1882)$ 的消息签名时,相对于文中提出的方案,使用vHP方案平均需要至少 l 次模乘法运算,因此效率较低。

4 结束语

在两个计算性假设前提下提出了一个新的高效的FFS方案。为保证接收方的安全性使用了离散对数和因子分解两个困难性假设,这两个假设同样可满足证实伪造。方案中证实伪造是通过揭露模数的非平凡因子,从而加快了验证过程。还介绍了一个新的与通信信道有效使用相关的FFS效率度量方法,鉴于该度量方法,文中方案比vHP方案更好。

参考文献:

[1] van Heyst E, Pedersen T. How to make efficient fail－stop signatures[C]//In Advances in Cryptology－Euro－Crypt'92. Berlin: Springer－Verlag, 1992: 337－346.

[2] Pedersen T P, Pfitzmann B. Fail－stop signatures[J]. SIAM Journal on Computing, 1997(2): 291－330.

(下转第147页)

由于经济全球化的影响,应该以前瞻的目光来发展我国的PKI。由于电子商务多为全球跨国界行为,因此CA与CA间特别是国与国之间CA的交互认证问题亦有待解决,而这其中所涉及的问题除技术层面外,政治与经济利益等因素也是用户或国家考虑的重点。目前国内相关专家学者已考虑三种可行解决方案,即Root CA、Bridge CA及OCSP(Online Certificate Status Protocol) Responder(即证书状态在线查询)。无论未来我国会以何种方案来实施,必须既要考虑建立统一的国家证书管理中心来解决CA交互认证问题,还要尊重并依循市场发展机制,提供统一数据查询平台,供一般使用者在线查询数字证书合法性及有效性,使数字证书的相关业务朝更多元化发展。

4 结束语

据IDC调查,全球PKI市场正在急剧扩大,预计到今年有望达到30亿美元的规模[6]。若针对以上在建制PKI系统中提出的问题采取较好的应对措施,这将会极大促进PKI在我国各行业的应用和普及,推进我国信息化建设。

参考文献:

[1] 李明柱. PKI技术及应用开发指南[EB/OL]. 2002-06-12. www.developerworks.com.

[2] 谷和启. 公钥基础设施PKI技术与应用发展[EB/OL]. 2003-11-10. http://network.ccidnet.com.

[3] 从国际电子商务立法到中国的电子商务政策法律环境[EB/OL]. 2004-07-13. http://www.chinaeclaw.com.

[4] 吴世忠. 规范CA认证中心的建设已成当务之急[N]. 光明日报,2000-07-19(B1).

[5] 卢旭成.《电子签名法》实施两年成绩显著,电子认证服务:在规范中开拓发展[N]. 中国计算机报,2007-05-09(A2).

[6] 余 勇. 标准化推动PKI发展[EB/OL]. 2003-06-27. http://www.ccidnet.com.

(上接第141页)

[3] Susilo W, Safavi-Naini R, Pieprzyk J. RSA based fail-stop signatures schemes[C]//International Workshop on security. Washington, D C, USA: IEEE Computer Society Press, 1999: 161-166.

[4] 马春波,何大可. 门限失败—停止签名[J]. 计算机工程与应用,2004(19):145-146.

[5] 杨 波. 现代密码学[M]. 北京:清华大学出版社,2003:143-181.

[6] 卿斯汉. 安全协议[M]. 北京:清华大学出版社,2005:66-75.

(上接第143页)

又 $e = r^{-1}e' = r^{-1}r_x m' = r^{-1}r_x r m_x m_y = r_x m_x m_y$

由上可知,该签名能通过验证。

(2) 盲性。盲性是盲数字签名的重要特性,匿名意味着签名者不知道需要签名的真实内容。在此方案的签名过程中,签名者B在不知道用户A的盲因子的情况下,只能获得用户A盲化后的信息m',而由m'得到m等价于求解椭圆曲线离散对数问题,所以签名者不可能看到明文消息。

(3) 不可伪造性。任何人要伪造签名(y,e),并通过验证方程$e = r_x m_x m_y \bmod l$的检验,其困难性等价于求解椭圆曲线离散对数问题。

(4) 不可追踪性。假设签名者保留(y,e,m',R'),若签名者想追踪签名,他需要通过盲化消息m'求得有关A的秘密信息,但是由于m'求解m的难度等价于求解椭圆曲线的离散对数问题,所以在签名被接收者泄露后,签名者不能追踪签名。

3 结束语

设计了一种基于椭圆曲线密码体制的盲数字签名及其身份识别方案,具有较高的安全性,并在电子商务、电子投票中具有一定的理论和实用价值。众所周知,目前还没有有效求解椭圆曲线离散对数问题的算法,所以该方案目前是安全的。

参考文献:

[1] Fan C I, Chen W K, Yeh Y S. Randomization enhanced Chaum' blind signature schemes[J]. Comput. Commun, 2000,23:199-203.

[2] Shao Z. Improved user efficient blind signatures[J]. Electronic Letter,2000,36(16):209-219.

[3] Chaum D. Blind Signature System[C]//Advances in Cryptology, CRYPTO'83. NEW YORK: Spring Verlag,1983.

[4] 杨义先,钮心忻. 应用密码学[M]. 北京:北京邮电大学出版社,2005:133-147.

[5] 冯登国. 密码分析学[M]. 北京:清华大学出版社,2000.