基于椭圆曲线密码体制的群体数字签名算法

Digital Multisignature Algorithm based on the Elliptic Curve Cryptosystem

周立章　王世伦

（成都师范高等专科学校计算机科学系　成都611930）（四川师范大学计算机科学学院　成都610068）

Abstract The elliptic curve cryptosystem with its speciality is widely applied to encryption and digital signature. it is used to construct digital multisignature. In this paper we propose digital multisignature and multiblind digital signature based on non-supersigngular elliptic curve over finite field GF(2^n), the safety of these scheme is depend on the discrete logarithm of non-supersingular elliptic curve .it is suitable for some practice.

Keywords ECC, Digital multisignature, Multiblind digital signature, Security

1　前言

椭圆曲线密码体制是一种基于代数曲线的公钥密码体制，它具有"安全性高，密钥量小，灵活性好"[1]的特点，由于椭圆曲线密码体制不是建立在一个大整数分解及素数域乘法群离散对数的数学难题上，而是建立在更难的椭圆曲线离散对数的问题之上[3]，因此其安全性更高。它不仅用于信息的加密解密，还可以用来构造数字签名和盲数字签名[2,3]。

文[1]讨论了特征为2^n 的域GF(2^n)上的安全椭圆曲线及其基点的选取，保证了有限域GF(2^n)上有足够的非超奇异椭圆曲线；文[3]提出了在域GF(2^n)上的非超奇异椭圆曲线上实现单数字签名和单盲数字签名。本文在单数字签名[2]方案的基础上，提出了基于有限域GF(2^n)上的非超奇异椭圆曲线上的群体数字签名和群体盲数字签名方案。

2　有限域GF(2^n)上的椭圆曲线加密体制

2.1　有限域上的非超奇异椭圆曲线

为了增加加密安全，便于计算机实现该算法，我们根据文[2]，选择基于域GF(2^n)上的非超奇异椭圆曲线，其方程是：$y^2+xy=x^3+ax+b$ $(a,b\in GF(2^n), b<>0)$。定义E(GF(2^n))是满足方程 $y^2+xy=x^3+ax+b$ 的点$(x,y)\in GF(2^n)\times GF(2^n)$和曲线上无穷远点O所组成的集合，则(E(GF(2^n)), +, O)是一个Abelian群，其中加法定义如下：

设P、Q是E(GF(2^n))上的两个点，若P=O，则$-P=O$且$P+Q=Q+P=Q$；令$P=(x_1,y_1)$，$Q=(x_2,y_2)$，则$-P=(x_1,y_1+x_1)$，且$P+(-P)=(-P)+P=O$；如果$Q\neq P$，则$P+Q=(x_3,y_3)$，这里：

$$x_3=\mu^2+\mu+x_1+x_2+\alpha$$

$$y_3=\mu(x_1+x_3)+x_3+y_1$$

$$\mu=\begin{cases}(y_2+y_1)/(x_2+x_1) & P\neq Q\\ (x_1^2+y_1)/x_1 & P=Q\end{cases}$$

2.2　基于椭圆曲线上的数字签名算法

根据2.1节，定义在GF(2^m)（要求m>160）上的非超奇异椭圆曲线E，选择E(GF(2^m))上的一个基点G，求出G的阶n（使nG=O的n），根据SHA-1选择一单向安全Hash函数h(x)。用户随机选择一个整数d，计算公钥Q=dG，用户公布(E(GF(2^m)), a, b, G, n, h)，保密d。则基于有限域GF(2^m)上非超奇异椭圆曲线的数字签名可描述如下：

假设用户A要对信息m签名，则：(1)A首先随机或伪随机选择一个整数k，0<k<n，计算R=kG=(x,y)，r=x mod n，如果r=0，则返回(1)；(2)计算e=h(m)；s=(ke+rd)mod n，若r=0，则返回(1)。否则(r,s)是A对信息m的数字签名。

数字签名验证：验证者计算$X=e^{-1}(sG-rQ)=(x1,y1)$；若X=0，则拒绝这个签名；否则计算v=x1 mod n，若v=r则接受这个签名。

3　基于椭圆曲线的群体数字签名

群体数字签名是在单数字签名的基础上发展而来，它是指多于一人参与数字签名。群体数字签名分为有序数字签名和同时群体数字签名。而后者是指多人同时对同一文件进行签名。下面的方案是基于文[3]的椭圆曲线数字签名的基础上提出的同时群体数字签名，它的关键在于每一位签名者要将自己根据概率计算出的r_i在所有签名人中公开，以便求r。

3.1　系统初始化

签名中心根据2.1节和2.2节选择椭圆曲线，公开(E(GF(2^m)), a, b, G, n, h)（要求m>160）。假设有k个用户u_i要进行群体数字签名，则u_i选择自己的私钥d_i，计算公钥：$y_i=d_iG$，向签名中心发送y_i，并公开y_i。

3.2　群体数字签名生成

假设n个用户u_i要同时对信息m进行数字签名，则其过程如下：

签名中心		签名者u_i
		选择$k_i(0<i<=k)$，计算 $R_i=k_iG=(x_i,y_i)$，$r_i=x_i \bmod n$
	← r	$r=\sum_{i=1}^{n} r_i \bmod n$
计算e=h(m,T)（T是时间戳）	→ e	
	← s_i	$s_i=(k_ie+rd_i) \bmod n$

$$s=\sum_{i=1}^{n} s_i \bmod n$$

$$r=\sum_{i=1}^{n} r_i \bmod n$$

周立章　讲师，研究方向为计算机网络、电子商务及安全。**王世伦**　硕士，副院长，副教授，研究方向为计算机网络及数据库。

则同时群体数字签名是(e,r,s)

3.3 群体数字签名的验证

验证者按如下步骤验证:

(1)从签名中心获得用户 u_i 的公钥 y_i,计算:$y=\sum_{i=1}^{n} y_i \bmod n$;

(2)计算:$X=e^{-1}(sG-ry)=(x,y)$,若 X=0,则群体签名失败;否则计算:v=x mod n;

(3)如果 v=r,则接受签名。

4 群体盲数字签名

群体盲数字签名也是从单盲数字签名发展而来,它指多人同时对同一信息进行数字签名而对信息的内容一无所知,而信息的拥有者却可以从签名者对盲化后的信息的数字签名得到对真实信息的数字签名。由于椭圆曲线加密体制的特点,因此基于椭圆曲线加密体制的群体盲数字签名在电子货币构造和电子投票设计等应用中更具潜力,也更易于实现。下面在文[2]的基于非超奇异椭圆曲线上的盲签名方案的基础上设计了一个同时群体盲数字签名方案,该方案的关键是各用户要将经概率生成的 r_i 传送给验证者,便于生成 r,以及验证者对信息的盲化。

4.1 系统初始化

签名中心根据2.1节和2.2节选择椭圆曲线,公开(E(GF(2^m)),a,b,G,m,h,F_x)(要求 m>160)。其中 F_x 是一取椭圆曲线上点的 x 坐标的函数,即 $F_x(U)$ 表示取点 U 的 x 坐标。假设有 n 个用户 u_i 要进行群体盲数字签名,则 u_i 选择自己的私钥 d_i,计算公钥:$y_i=d_iG$,向签名中心发送 y_i,并公开 y_i。

4.2 群体盲数字签名生成(图1)

则数字签名对(c,s)是用户 u_i 对信息 m 的群体盲数字签名。

4.3 群体盲数字签名验证

验证者 V 只需计算下列等式是否成立:

$c=h(m\|F_x(cY+sG,T) \bmod n)$,其中 $F_x(u)$ 表示取点 u 的 x 坐标。

安全分析及结论 上面两个群体数字签名方案是基于有限域 GF(2^n)上非超奇异椭圆曲线加密体制的,因此其安全性基于非超奇异椭圆曲线的安全性,而有限域 GF(2^n)上非超奇异椭圆曲线的安全性是基于椭圆曲线上离散对数难题的,它比基于有限域上的离散对数问题的公钥体制更安全,是值得

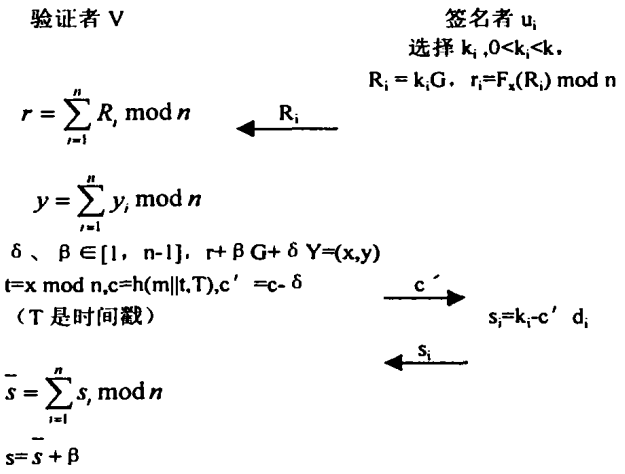

图1

信赖的;另外攻击者想伪造群体(盲)数字签名是不可行的,因为他不知道用户的私钥,即使在传送中获取了某个 r_i,也不可求得用户的私钥,因为他面对的是求解椭圆曲线上的离散对数难题。

基于有限域上的非超奇异椭圆曲线加密体制由于其密钥量小,安全高和灵活性等特点,在公钥体制、数字签名和认证等中的应用具有广泛潜力。本文在文[2]的基础上设计了群体数字签名和群体盲数字签名两种方案,在签名时传送信息量小,具有一定的实用价值。

参 考 文 献

1 刘胜得,郑东,王育民. 域 GF(2n)上安全椭圆曲线及其基点的选取. 电子科学学刊,2000,22(5)

2 张方国,王常杰,王育民. 基于椭圆曲线的数字签名与盲签名. 通信学报,2001,22(8):22~27

3 张龙军,邹涛,沈钧毅. 一种基于椭圆曲线密码体制的盲数字签名方案. 计算机应用,2001,21(3):17~19

4 Chamenisch J L,et al. Blind signature based on the discrete logarithm problem. Rump Session of Eurocrpt'94,1995

5 Harn C,Keisler T. New scheme for digit multisignature. Electro. Lett.,1989,25(15):1002~1003

6 Hardjoiro T,Zheng Y A. Pratical digital multisignature scheme based on discrete logarithm. Advance Cryptology-AUSCRPTO'92,1992

(上接第40页)

统,VPN 路由信息不需要渗透到底层网络的路由系统中。

(8)在路由设计中引入故障隔离方法。

(9)尽可能减少路由处理负担。

(10)定义易管理的路由策略。

(11)可能的话,采用其他系统辅助路由处理。

(12)有条件的话,在 MPLS 体系结构上构建 VPN。

结束语 本文对 VPN 的可扩展性进行了研究,总结了在构建大型 VPN 时应遵循的一些基本原则,但由于 VPN 是一种综合性很强的新技术,而且构建 VPN 的技术和支持 VPN 的设备都还不成熟,因此,对 VPN 的可扩展性还需进行进一步的研究,VPN 的可扩展性仍是 VPN 发展中一项重要的研究内容。

参 考 文 献

1 RFC 2764. A Framework for IP Based Virtual Private Networks

2 RFC 2791. Scalable Routing Design Principles

3 RFC 2547. BGP/MPLS VPNs

4 RFC 3031. Multiprotocol Label Switching Architecture

5 RFC 2796. BGP Route Reflection - An Alternative to Full Mesh IBGP

6 RFC 2917. A Core MPLS IP VPN Architecture