第16卷 第1期
2006年1月

计算机技术与发展
COMPUTER TECHNOLOGY AND DEVELOPMENT

Vol.16 No.1
Jan. 2006

一个基于超椭圆曲线的单向数字签名

蔡庆华,程一飞
(安庆师范学院 计算机与信息学院,安徽 安庆 246011)

摘 要:超椭圆曲线密码体制(HECC)是椭圆曲线密码体制(ECC)的自然推广,但不仅仅是一种简单的推广。HECC与ECC相比有速度快、基域小的优点。而单向签名是一种只有特定的用户才能验证的数字签名方案。该文基于超椭圆曲线密码体制提出了一个单向签名方案,并分析了其安全性。与现有方案相比,本方案有一定的优势。

关键词:超椭圆曲线密码体制;Jacobian;单向数字签名
中图分类号:TP309.7 **文献标识码**:A **文章编号**:1005-3751(2006)01-0221-02

A Directed Digital Signature Based on HECC

CAI Qing-hua, CHENG Yi-fei
(School of Computer and Information, Anqing Teachers' College, Anqing 246011, China)

Abstract: Hyper elliptic curve cryptosystems (HECC) is a natural generalization of elliptic curve cryptosystems, but it is not only a simple generalization. HECC is faster than ECC and the basis field of HECC is smaller than ECC. Directed digital signature is a special signature scheme that must be verified by specific user. A directed digital signature based on hyper elliptic curve cryptosystems was proposed and the security was discussed. This scheme has more advantages than which has been discussed.

Key words: hyper elliptic curve cryptosystems; Jacobian; directed digital signature

在普通的数字签名系统中,任何人都可以成为验证者,因为签名者的公钥是公开的,只要获得签名和消息就可以验证签名。而如果消息不宜公开,就要对验证者的身份作特殊要求,除特定的验证者外任何人都无权验证。为满足这种要求,可以用普通数字签名系统先对消息签名,再对签名加密[1],只有能对加了密的签名正确解密的人才能验证,但此时计算量大,需要进行多交互式通信,不适于实际应用。单向数字签名引入了这样的思想,使数字签名既和签名者相关,又和验证者相关,于是只有特定的验证者才能对签名进行验证,而且不需要交互式通信,节省了时空开销。文中依据单向签名的思想设计了一种基于超椭圆曲线密码体制的单向签名方案。

1 超椭圆曲线密码体制

1.1 超椭圆曲线

超椭圆曲线是一类特殊的代数曲线,它可以看成是椭圆曲线的推广,亏格为1的超椭圆曲线就是椭圆曲线。作为椭圆曲线的一个自然推广,Neal Koblitz[2]在1989年提出了超椭圆曲线密码体制(HECC),它是基于有限域上超椭圆曲线的Jacobian群上的离散对数问题的计算困难性提出的。超椭圆曲线能提供与椭圆曲线相似的群结构,HECC具有与ECC相似的密码特性,与ECC相比,HECC具有在较小基域上提供与ECC相同级别的安全性的优势。因而,超椭圆曲线的理论近几年在密码界倍受重视。

下面首先给出超椭圆曲线的定义:

定义:设 F 是域,Γ 是其代数闭域。则 F 上亏格为 $g(g \geqslant 1)$ 的超椭圆曲线 C 是指具有方程形式 $y^2 + h(x)y = f(x)$ 的曲线。这里 $h(x) \in F(x)$ 是次数不大于 g 的多项式,$f(x) \in F(x)$ 是一个次数为 $2g+1$ 的首一多项式,而且不存在 $(x,y) \in \Gamma \times \Gamma$ 满足下列方程组:

$$y^2 + h(x)y - f(x) = 0$$
$$2y + h(x) = 0$$
$$h'(x)y - f'(x) = 0$$

如果 $g = 1$,则称 C 为椭圆曲线。

1.2 Jacobian群

超椭圆曲线密码体制是建立在超椭圆曲线的Jacobian群上的,有限域上超椭圆曲线的Jacobian群是一个有限交换群。Jacobian群上实用的群运算算法最早是由Cantor[3]提出的。这里将商群 $D_C^0(Fq)/P_C(Fq)$ 定义为 C 在Fq上的Jacobian,记为 $J_C(Fq)$。

$J_C(Fq)$ 实际上也是超椭圆曲线 C 上的全体归约除子的集合。$J_C(Fq)$ 的一个重要事实是,可以在 $J_C(Fq)$ 中定义归约除子的一个加法运算,使得 $J_C(Fq)$ 成为一个交换群,这个有限交换群是超椭圆曲线密码体制的基础。这里说

收稿日期:2005-04-15
基金项目:安徽省教育厅自然科学研究项目(2005KJ365zc)
作者简介:蔡庆华(1974—),男,安徽太湖人,讲师,硕士,主要研究方向为计算机网络与信息安全。

的超椭圆曲线密码实际上是建立在超椭圆曲线的 Jacobian 群上的,并不是建立在超椭圆曲线的有理点全体上的,因为一般超椭圆曲线的有理点全体不一定构成交换群。

1.3 超椭圆曲线上的点到整数的映射

超椭圆曲线密码体制的一个关键就是如何将超椭圆曲线上的一点映射到一个整数,下面给一种映射。

设 $D=<a(u),b(u)>\in Jc(Fq)$是一个约化除子,其中 $a(u)=\sum_{j=0}^{g}a_ju^j$,$b(u)=\sum_{j=0}^{g-1}b_ju^j$,$a_g=1$,$a_j,b_j\in Fq$。可以将 D 对应于如下整数:

$a_0q^{2g-1}+a_1q^{2g-2}+\cdots+a_{g-1}q^g+b_0q^{g-1}+b_1q^{g-2}+\cdots+b_{g-2}q+b_{g-1}$ 或 $a_0+a_1q+\cdots+a_{g-1}q^{g-1}+b_0q^g+b_lq^{g+1}+\cdots+b_{g-2}q^{2g-2}+b_{g-1}q^{2g-1}$。

设 λ 表示该对应关系,则 λ 是一个从 $J(Fq)$ 到有限整数集 $Z_q^{2g}=\{0,1,\cdots,q^{2g}-1\}$ 的一个单射。将其记为$(D)_\tau$或$(D)_q$。显然,这样的赋值映射不是唯一的。在文献[4,5]中给出了另外几种映射。

2 基于超椭圆曲线的密码体制

(1)公共参数:

设 $C:y^2+h(x)y=f(x)$ 是 Fq 上亏格为 g 的超椭圆曲线,$J_C(Fq)$ 是它的 Jacobian 群;$\#J_C(Fq)=hn$,n 是 160bit 大素数(或更大),$h=1$ 或是较小的余因子,q 约为 g^{160}bit 左右。而 G 是 $J_C(Fq)$ 中具有大素数阶 n 的一个约化除子。对任意整数 r,rG 表示除子标量乘。$D\in Jc(Fq)$ 是 n 阶元素,则$(D)_q$表示一个由超椭圆曲线的 Jacobian 中的元素到正整数的嵌入映射。

加密公钥是 $Q=dG=[a_Q,b_Q]$,d 是解密密钥,不公开,要加密的消息是 m。

(2)加密过程:

a.随机选取 $k\in[1,n-1]$,计算 $K=kG$;

b.计算 $R=kQ=[a,b]$;$z=(R)q$;

c.计算 $c=m+z(\mathrm{mod}\ n)$;

d.发送密文(K,c)。

(3)解密过程:

a.收到(K,c)后,计算 $R=dK=dkG=kQ$ 和 $z=(R)_q$;

b.得到明文 $m=(c-z)\mathrm{mod}\ n$。

3 基于超椭圆曲线的数字签名

超椭圆曲线数字签名所需参数同加密过程。

1) 签名产生:

为了对信息 m 签名,实体 A 执行下列步骤:

(1)随机选择 $d\in\{1,\cdots,n-1\}$作为它的私钥并计算除子标量乘 $P=dG$ 作为其公钥。

(2)随机选择 $k\in\{1,\cdots,n-1\}$ 并计算 kG 及 $r=(kG)_q \mathrm{mod}\ n$,如果 $r=0$,则重选 k。

(3)计算 $s=k^{-1}(h(m)+dr)\mathrm{mod}\ n$。如果 $s=0$,则返回上一步。

(4) A 对 m 的签名(r ,s)。

2) 签名验证:

为了验证 A 的签名,实体 B 执行下列步骤:

(1)先获得真实的公共参数以及 A 的公钥 P。

(2)计算除子标量乘 $R=(s^{-1}h(m))G+(s^{-1}r)P$。

(3)检验(R)q mod $n=r$ 是否成立。如果成立,则接受该签名,否则,拒绝该签名。

4 基于超椭圆曲线的单向签名

设签名者为 A,特定的验证者为 B;m 为待签名消息;超椭圆曲线及参数的选择同前。

密钥生成:s_A,s_B 分别为 A,B 的私钥,对应的公钥分别为 $P_A=s_AG$,$P_B=s_BG$。

签名生成:签名者 A 选取随机数 k,计算:

(1) $C=(s_A+k)P_B=(s_A+k)s_BG$

(2)$R=kG$

(3)$s=((C)_q*s_A-m*k)\mathrm{mod}\ n$

签名为(R,s),与消息 m 发送给验证者 B。

签名验证:B 计算 $C'=s_B(R+P_A)$

检验方程$(C')_qP_A=mR+sP$是否成立。

该方案只有特定的用户 B 才能验证,且不需要交互式验证。

任何第三者只能在确定出 s,m 后才能伪造签名,而确定 s,m 属于 HECDLP 问题。如果先确定 s,m,再确定 R,则由于 C' 和 C 矛盾而无法使方程成立。如果 B 想要伪造签名,由于其不知道 C 和秘密参数 k,由 R 计算 k 是 HECDLP 问题,猜测成功概率只有 $1/n$,故为不可能。

5 小 结

超椭圆曲线能提供与椭圆曲线相似的群结构,HCC 具有与 ECC 相似的密码特性,与 ECC 相比,HCC 具有在比较小的基域上提供与 ECC 相同级别的安全性的优势。因而,超椭圆曲线的理论近几年在密码界倍受重视。文中基于此提出了一个新的单向签名方案,用以解决特定签名要由特定用户来验证的问题。

参考文献:

[1] 蔡庆华,陈文莉. RSA 算法在数字签名中的应用[J]. 安庆师范学院学报,2004(2):70-71.

[2] Koblitz N. Hyperelliptic cryptography[J]. J. of Crypto,1989,1(3): 139-150.

[3] Cantor D G. Computing in the Jacobian of a hyper elliptic curve[J]. Mathematics of Computation, 1987,5:95-101.

[4] 张方国. 超椭圆曲线密码体制的研究[D]. 西安:西安电子科技大学,2001.

[5] 游 林. 超椭圆曲线密码体制研究[D]. 大连:大连理工大学,2002.