一个基于超椭圆曲线的代理签名

蔡庆华
(安庆师范学院 计算机与信息学院,安徽 安庆 246011)

摘 要:现有的代理数字签名方案大多基于离散对数问题和大数因子分解问题,其安全性受到较大威胁。为提高安全性,在对现有方案分析后,提出了一种新的代理签名方案。与椭圆曲线相比,超椭圆曲线是一种新的密码体制,具有速度快、基域小的优点。文中将代理签名的思想应用于超椭圆曲线数字签名,提出了一种新的基于超椭圆曲线的代理签名方案,并对方案的复杂性和安全性进行了分析。经过比较,本方案比基于椭圆曲线的方案在安全性上有显著提高,在电子商务中有很好的应用。

关键词:超椭圆曲线密码体制;Jacobian 群;代理数字签名;电子商务;除子;亏格
中图分类号:TP309.7 **文献标识码**:A **文章编号**:1673-629X(2010)07-0160-04

A Proxy Signature Scheme Based on Hyper Elliptic Curve Cryptosystems

CAI Qing-hua
(Computer Science Department, Anqing Teachers' College, Anqing 246011, China)

Abstract: Up to now all the known proxy digital signature schemes are based on discrete logarithmic problems or big number factorization problems. To strengthen proxy signature security, and analyses of proxy signature scheme in being, this paper proposed a proxy signature scheme based on the hyper elliptic curve cryptography. HECC has a lot of advantages over ECC, it is faster and the basis field is smaller. In this paper, show how to apply the idea of proxy digital signature scheme to HECC and present a new scheme. Furthermore, also analyze the new scheme's computation complexity and security problem. This scheme is better than that of elliptic curve cryptography on performance of security. It plays a better role in electronic commerce.

Key words: hyper elliptic curve cryptosystems; Jacobian groups; proxy digital signature; electronic commerce; divisor; genus

0 引 言

在现实生活中,当进行商品交易、签订合同时,如果某人(这里称为签名授权人)因某种原因不在现场而不能签名时,一般可委托他人用其私章或公章代其签名。例如在电子商务活动中,CA 证书的签发,电子支票或电子货币的分发或电子选举活动等等,同样需要委托其他人代替自己签名。

一般情况下,一个代理签名方案都应包括:

(1)系统初始化:选定签名体制的参数,包括用户的密钥等;

(2)签名权的委托:签名人将自己的签名权力委托给其他人(代理签名人);

(3)代理签名的生成:代理签名人利用签名人的委托信息,代表原始签名人产生数字签名;

(4)签名的验证:接收签名的人验证签名的有效性。

目前对于代理签名的研究较多,不同专家针对不同的应用环境提出了不同的代理签名方案[1,2],这些方案可以满足他们提出的不同要求。但是大部分方案的安全性是建立在求解离散对数难题或大数素因子分解难题上。而代理签名是一种联合的多层次签名认证协议,现有的方案一般都有着密钥较长、运算较复杂、系统开销较大、安全性不高等不足,因此文中利用超椭圆曲线来构建代理签名方案,以解决上述问题。

1 预备知识

1.1 超椭圆曲线

超椭圆曲线是一类特殊的代数曲线,是椭圆曲线的推广,一般情况下亏格为 1 的超椭圆曲线就是椭圆曲线。对椭圆曲线密码体制进行推广,在 1989 年,

收稿日期:2009-11-04;**修回日期**:2010-02-23
基金项目:国家自然科学基金(60773128);安徽省自然科学基金(KJ2007B043);安徽省高校青年教师资助项目(2007JQL122)
作者简介:蔡庆华(1974-),男,安徽太湖人,硕士,副教授,研究方向为计算机网络与信息安全。

Neal Koblitz[3]提出了超椭圆曲线密码体制(HECC),这种密码体制是基于有限域上超椭圆曲线的 Jacobian 群上计算离散对数问题的困难性提出。它具有与椭圆曲线相似的密码特性,能提供与椭圆曲线相似的群结构。目前,基于 HECC 的密码研究成为大家关注的焦点。

下面先给出超椭圆曲线的定义:

设 F 是有限域,Γ 是其代数闭域,则 F 上亏格为 $g(\geqslant 1)$ 的超椭圆曲线 C 的方程描述如下:

$$y^2 + h(x)y = f(x) \tag{1}$$

其中 $f(x)$、$h(x) \in F(x)$,$h(x)$ 的次数不大于 g,$f(x)$ 的次数为 $2g+1$ 并且首项为 1,对于任意的 $(x,y) \in \Gamma \times \Gamma$,均不能满足下列方程组:

$$h'(x)y - f'(x) = 0 \tag{2}$$

$$2y + h(x) = 0 \tag{3}$$

若 $g = 1$,则称 C 为椭圆曲线。

1.2 Jacobian 群

基于超椭圆曲线的密码体制是建立在 Jacobian 群上,它是由一个无限除子群模它的一个子群,即主除子子群而得到的一个商群,最早用到的群运算是由 Cantor[4]提出。一般将商群 $D_C{}^0(Fq)/P_C(Fq)$ 定义为超椭圆曲线在 Fq 上的 Jacobian 群。

将超椭圆曲线上全体归约除子的集合记为 $J_C(Fq)$,在 $J_C(Fq)$ 中定义归约除子的一个加法运算后,$J_C(Fq)$ 就可转化为一个交换群,它就是实现超椭圆曲线密码体制的基础。由于一般超椭圆曲线的全体有理点不一定能构成交换群,因此超椭圆曲线密码体制是建立在 Jacobian 群上,而不是建立在超椭圆曲线的全体有理点上。

1.3 点到整数的映射

在密码体制中研究的对象是数,而在超椭圆曲线上是点,那么如何将超椭圆曲线上的一个点映射成一个整数,就是一个很重要的问题,下面给出一种签名方案中要用到的映射。

设超椭圆曲线上的点 $D = < a(u), b(u) > \in Jc(Fq)$,是一个约化除子,其中 $a(u) = \sum_{j=0}^{g} a_j u^j$,$b(u) = \sum_{j=0}^{g-1} b_j u^j$,$a_g = 1, a_j, b_j \in Fq$。有下列等式:

$$\lambda = a_0 q^{2g-1} + a_1 q^{2g-2} + \cdots + a_{g-1} q^g + b_0 q^{g-1} + b_1 q^{g-2} + \cdots + b_{g-2} q + b_{g-1} \quad 或$$

$$\lambda = a_0 + a_1 q + \cdots + a_{g-1} q^{g-1} + b_0 q^g + b_1 q^{g+1} + \cdots + b_{g-2} q^{2g-2} + b_{g-1} q^{2g-1}$$

从上式可知 λ 是一个从超椭圆曲线上的点 D 到有限整数集 $Z_q^{2g} = \{0,1,\cdots,q^{2g}-1\}$ 的映射,记为 $(D)_q$。这样的赋值映射较多,例如文献[5,6]。

2 基于超椭圆曲线的加密与签名方案

2.1 加密方案

系统参数:

超椭圆曲线 $C: y^2 + h(x)y = f(x)$,亏格为 g,$J_C(Fq)$ 是它的 Jacobian 群;$\# J_C(Fq) = h\,n$,n 是 160bit 大素数(或更大),h 是较小的余因子(可以是 1),而 G 是 $Jc(Fq)$ 中具有大素数阶 n 的一个约化除子。对任意整数 r,$r * G$ 表示除子标量乘,D 是超椭圆曲线上的点,$(D)_q$ 表示一个由超椭圆曲线的 Jacobian 中的点到正整数的映射。

m 是 A 要通过加密传送给 B 的明文,A 用来加密的公钥是 $Q = d\,G = [a_Q, b_Q]$,d 是 B 的解密密钥,不公开。

· 加密过程:

(1)A 随机选取 $k \in [1, n-1]$,计算 $K = kG$;

(2)A 计算 $R = kQ = [a,b]$;$z = (R)_q$;

(3)A 计算 $c = m + z \pmod n$;

(4)A 发出密文 (K,c)。

· 解密过程:

(1)B 收到 (K,c) 后,计算 $R = d\,K = dkG = kQ$ 和 $z = (R)_q$;

(2)B 由等式 $m = (c - z) \bmod n$ 得到明文。

2.2 签名方案

超椭圆曲线数字签名算法(HECDSA)可以被认为是 DSA 签名算法在超椭圆曲线上的模拟。在 1992 年,Vanstone 提出了椭圆曲线签名算法(ECDSA),该算法按照 NIST's (National Institute of Standards and Technology) 要求,根据人们对 DSS(Digital Signature Standard)的意见而设计的。此后,人们提出了若干种 ECDSA 的变体。一般而言,这些签名体制本质上都是由 ElGamal 签名体制模拟而得到。

在 1989 年,Koblitz[3]模拟椭圆曲线建立密码体制,首次在超椭圆曲线上建立了新的密码体制,即超椭圆曲线密码体制 HEC。后来,人们又提出了相应的超椭圆曲线数字签名算法。本节所给的超椭圆曲线数字签名所需参数同前面加密方案。

·签名文的产生过程:

要对明文 m 签名,签名人 A 按下列步骤操作:

(1)A 任意选择整数 $d \in \{1,\cdots,n-1\}$ 作为私钥,然后计算 $P = d * G$ 作为自己的公钥并公开。

(2)A 随机选择整数 $k \in \{1,\cdots,n-1\}$,计算 $k * G$ 及 $r = (k * G)_q \bmod n$。若 $r = 0$,则重选 k。

(3)A 根据 r 计算 $s = k^{-1}(h(m) + d\,r) \bmod n$。若 $s = 0$,则返回步骤(2)。

(4)A 对明文 m 的签名文为 (r,s),并将明文 m 和

签名(r,s)发送给接收者B。

· 签名的验证过程：

接收方B收到明文m和签名文(r,s)后，为了验证是否是A的签名，B按下列步骤验证：

(1)B从可信中心(公共机构)获得系统公共参数G以及签名者A的公钥P。

(2)B计算$R = (s^{-1}h(m)) * G + (s^{-1}r) * P$。

(3)B检验等式$(R)q \bmod n = r$是否成立。若等式成立，则接受A的签名，否则，B拒绝该签名或认为不是A发来的签名。

3 基于超椭圆曲线的代理签名

构造基于超椭圆曲线代理签名方案可分为5个操作步骤，它们是系统参数建立、密钥的生成、代理授权、代理签名和代理签名的验证。

3.1 参数建立

(1)设有限域F上亏格为g的超椭圆曲线$C: y^2 + h(x)y = f(x)$；

(2)$J_C(F)$是超椭圆曲线C的Jacobian群；

(3)$\#JC(F) = hn$，n为大素数，h是较小的余因子(可为1)；

(4)G为Jacobian群上1个n阶归约除子；$H1$是一单向Hash函数。

3.2 密钥生成

(1)原始签名人A随机选择$x_A \in \{1,\cdots,n-1\}$，并将x_A作为其私钥保存；

(2)原始签名人A计算$Y_A = x_A * G = (a(u), b(u))$，若$Y_A = \mathrm{div}(1,0)$，则返回步骤(1)；

(3)原始签名人A将Y_A作为公钥并公开；

(4)按照同样的方法代理签名人B产生自己的私钥x_B和公钥Y_B，其中$Y_B = x_B * G$。

3.3 代理授权

(1)A随机选择$u \in Z_n^*$，并计算：$R = u * G \neq 0$，$h = H1((R)q)$，$f = hx_A + u(\bmod n)$，并将(R,f)秘密地发送给B。

(2)B收到(R,f)后，先计算$h = H1((R)q)$并验证等式：$fG = hY_A + R$，若成立，则(R,f)是一个有效的代理密钥，否则B拒绝该密钥，并要求A重新给他发一个新的代理密钥，或者停止操作。

(3)为确保代理密钥包含代理人的身份，B计算：$f' = f + x_B \bmod n$，以此作为B生成代理签名的密钥。

3.4 代理签名

对某个消息m，B以f'作为数字签名的秘钥。生成数字签名(m,s,R,T)并发送给签名验证者，其中：$T = v * G$(v为B选择的一随机数)，$s = (T)_q f' - mv \bmod n$。

3.5 代理签名的验证

接收签名的人收到(m,s,R,T)后，首先计算$h = H1((R)q)$，然后验证等式：

$$(T)_q(h * Y_A + R + Y_B) = s * G + m * T$$

若上面等式成立，则认为代理签名有效；若等式不成立则认定为无效签名。

签名的正确性可由下列等式进行验证，由代理签名生成过程得：

等式右边 $= s * G + m * T = (T)_q f' * G - mv * G \bmod n + m * T = (T)_q f' * G = (T)_q(f + x_B \bmod n)G = (T)_q(f * G + x_B * G) = (T)_q(h * Y_A + R + x_B * G)$ = 等式左边

4 代理签名的分析

4.1 安全性分析

一般的代理签名方案都要满足以下安全性[7~9]：

(1)不可伪造性：除了原始签名人A外，只有指定的代理人B能够代表A产生合法的代理签名。

(2)可验证性：接收签名的人收到代理签名后，能确信原始签名人A认可这份签名。

(3)不可否认性：代理签名人代表原始签名人产生签名后，就不能否认他的代理签名。

(4)可区分性：任何人都可将代理签名和原始签名人的签名进行区分，即代理签名和原始签名是不同的签名。

(5)不符合性：代理签名人能够创建一个被检测到是有效代理签名的签名。

(6)可识别性：原始签名人A能够从不同代理签名中确定代理人的身份。

经过分析，文中所述的代理签名满足以上要求。

在不可伪造性方面，除了原始签名人A外，任何人(包括代理签名者)在不知道签名私钥x_A的情况下，均不能伪造原始签名人的普通签名信息，因为没有人知道A的签名私钥；同样的道理，代理签名者B的签名私钥对于攻击者(包括原始签名人A)也是不知道的。

在可验证性方面，对于签名接收人，在获得了原始签名人A的公钥Y_A及代理签名(s,R,T)后，可以通过$(T)_q(h * Y_A + R + Y_B) = s * G + m * T$对代理签名进行验证。除了原始签名人$A$和代理签名人$B$外，其他人无法用公式$h = H1((R)_q)$生成签名信息。因此，接收签名人能确信原始签名人$A$承认这份代理签

名。

在不可否认性方面,从签名信息(s,R,T)中,s的值由等式$s=(T)_q f'-m\,v \bmod n$确定。委托信息$f=hx_A+u(\bmod n)$中包含原始签名人A的私钥x_A,并且是通过安全的信道传递给B的;而签名密钥$f'=f+x_B \bmod n$中有B的私钥,因此,B一旦进行了代理签名,他就不能向A及其他人否认所做的工作。

在可区分性方面,因为有效的代理签名(s,R,T)中包含有授权人公钥,代理签名人私钥,而且原始签名人和代理签名人的公钥在代理签名的验证过程中要使用。在出现问题时,可信第三方能够将原始签名与代理签名区分开。

在不符合性方面,普通超椭圆曲线数字签名结果为二元组(r,s),而代理签名结果为三元组(s,R,T)。因此,验证人通过这一特征就可以区分原始签名人A数字签名和A委托B生成的代理签名。

在可识别性方面,由于代理签名结果(s,R,T)中的R是A发送给B的委托信息的一部分,因此,原始签名人A在保存委托信息(R,f)和代理签名人的身份后,通过对比不同代理签名人生成的签名信息中的R值,从而确定代理签名人的身份。

4.2 效率分析

(1)签名的授权可以撤销。

当原始签名人A想撤销代理签名者B的签名授权时,A可以通过媒体宣布原有的委托信息(R,f)不再有效,并向可信中心注销代理签名密钥f'。这样,代理签名人B就不能再行使签名权,即使用签名别人也不会承认,因为每个人都能看到A的声明。

(2)算法简洁、效率高。

本代理签名方案很好地发挥了HECC密钥较短、安全性较高的优点。在实现时可以使用单个计算机的字处理,避免多精度整数的运算,从而减少了存储空间和降低了运算的系统开销。

5 结束语

在理论上亏格为1的超椭圆曲线就是椭圆曲线,因此超椭圆曲线可看成是椭圆曲线的一般推广,它具有与椭圆曲线相似的密码特性[10],并提供与椭圆曲线相似的群结构。但与椭圆曲线相比,它在较小的基域上提供了与椭圆曲线级别相同的安全性。由于降低了实现难度,因此基本超椭圆曲线的密码体制近来倍受关注。

随着网络技术的发展,电子商务与电子政务与人类生活联系日益紧密,代理签名的应用情景也越来越多。文中在充分发挥超椭圆曲线密码体制中自身的优势的基础上,设计了面向一般应用的代理签名方案,特别适合目前网络业务快速发展的需要,有非常好的应用前景[11]。

在对超椭圆曲线密码体制的研究中,发现关键的问题是如何选取合适的超椭圆曲线,使得在Jacobian群上实现安全的密码体制。要解决这个问题一般要知道超椭圆曲线的阶,目前计算超椭圆曲线的Jacobian的阶有许多方法,例如Adleman, Huang和Pila提出的Schoof算法,复乘(CM)方法, 模曲线法,Weil猜想法等。但是在具体应用时这些方法有时显得不太实用,有时得到的曲线受到一定限制[12]。目前还没有找到一个较好的办法,用来计算有限域上任意超椭圆曲线的Jacobian的阶(一般要求至少是160比特)。那么如何有效选择合适的超椭圆曲线,使得建立的密码体制安全层度最高,是超椭圆曲线密码体制研究中的难题,同时也是今后研究的方向。

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] 左为平,王彩芬. 具有前向安全性质的指定验证人代理签名方案[J].计算机应用, 2007(8):1898-1900.

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

[4] Cantor D G. Computing in the Jacobian of a hyper elliptic curve[J]. Mathematics of Computation, 1987,48(177):95-101.

[5] 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.

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

[7] 易小琳,周　巍,赵　磊,等. 一种基于超椭圆曲线的代理签名方案[J]. 北京工业大学学报,2009,35(5):1126-1131.

[8] 谷利泽,高　宏,杨义先.一种改进的代理多重签名方案[J].电子学报, 2005, 33(1): 88-90.

[9] 明　洋,姜正涛,王育民.一种改进的强代理签名方案[J].西安电子科技大学学报, 2006, 33(5):778-781.

[10] 陈玉春,朱艳琴,刘月琴,等. 亏格为2的超椭圆曲线上的二分算法及其优化[J].计算机应用与软件,2008, 25(7):94-96.

[11] Mambo M, Usuda K, Okamoto E. Proxy Signature for Delegating Signing[C]// In Proc. 3rd ACM Conference on Computer and Communications Security. New York: ACM Press, 1996.

[12] 张方国,王育民.超椭圆曲线密码体制的研究与进展[J].电子学报,2002, 30(1): 126-130.