超椭圆曲线密码体制的研究与进展

张方国,王育民
(西安电子科技大学 ISN 国家重点实验室,陕西西安 710071)

摘 要: 椭圆曲线密码是目前最流行的公钥密码体制,超椭圆曲线密码作为椭圆曲线密码的推广,近几年对它的研究也日益被人们重视. 在该文中,作者就目前国内外对超椭圆曲线密码体制的研究现状作了综述,并提出了在超椭圆曲线密码体制的理论与实现中急需解决的几个问题.

关键词: 超椭圆曲线密码体制 (HCC); Jacobian; HCDLP
中图分类号: TN911 **文献标识码**: A **文章编号**: 0372-2112 (2002) 01-0126-06

Study and Advance of Hyperelliptic Curves Cryptsystems

ZHANG Fang-guo, WANG Yu-min
(P. O. Box 119 Key Lab. on ISN, Xidian Univ., Xi'an, Shaanxi 710071, China)

Abstract: The elliptic curves cryptosystems (ECC) is the most popular public key cryptosystems at present. The hyperelliptic curve cryptosystems (HCC) is a generalization of ECC and the study of HCC has been paid more and more attention by people in recent years. This paper surveys the development and situation of HCC and presents some problems urgenthyneeded to be solved in the theory and implementation of HCC.

Key words: hyperelliptic curve cryptsystems; jacobian; HCDLP

1 引言

自从 1976 年 Diffie-Hellman 提出公钥密码思想,解离散对数问题就成了许多密码体制的基础. Diffie-Hellman 在他们首次提出的密钥交换协议中所用的群是大素数域的乘法群,这个想法可以推广到任意的群. 设 G 是一个 n 阶有限群, a 是它的一个元素, G 的离散对数问题是:给定 G 中一个元素 b,找一个整数 x, $0 \le x \le n-1$,使得 $a^x = b$(如果这样的整数存在). 用于密码中的有限群 G 可以是任意有限域的乘法群,虚二次数域的类群,辫群,有限域上椭圆曲线的有理点群[1,2],有限域上超椭圆曲线的 Jacobian[3],等等.

基于有限域上椭圆曲线加法群的离散对数问题(ECDLP)的公钥密码,是 Neal Koblitz[1]和 Victor Miller[2]在 80 年代中期提出的,由于在一般的椭圆曲线群中没有亚指数时间算法解 ECDLP(除了个别特殊的椭圆曲线以外),所以椭圆曲线密码成了目前最流行的公钥密码体制. 经过了 10 多年的研究,近几年它的实现已经被广泛应用于实际中. 作为椭圆曲线的一个推广,Neal Koblitz[3]在 1989 年提出了超椭圆曲线密码体制(HCC),它是基于有限域上超椭圆曲线的 Jacobian 上的离散对数问题. Cantor 的算法[4]为实现一条超椭圆曲线的 Jacobian 中的群运算提供了一个有效的算法. 在同等安全水平下,超椭圆曲线密码要比椭圆曲线密码所用的基域小,且 HCC 可以模拟基于一般乘法群上的如 DSA、ElGamal 等几乎所有协议,在同样的定义域上,亏格越大,曲线越多,所以选取用于密码中的安全曲线的余地越大. 由于超椭圆曲线密码体制比其他的密码体制有许多优点,所以近几年对超椭圆曲线密码体制的研究也日益被人们重视.

超椭圆曲线密码当前还主要处于理论研究阶段,还有大量未解决的问题. 从已有的 HCC 的实现来看,超椭圆曲线密码的实现速度要比椭圆曲线密码实现速度慢. 所以如何减少超椭圆曲线的 Jacobian 的点加和标量乘的计算量,从而提高超椭圆曲线密码的实现速度是超椭圆曲线密码走向实用的一个非常重要的问题. 研究超椭圆曲线密码有着重大的理论和实际意义,因为超椭圆曲线密码是 ECC 的一个推广,所以用于超椭圆曲线密码上的一些普遍的技术和方法可以用在 ECC 上,从而也对目前已经走向实用化的 ECC 无论是在理论上还是实现上都有益处.

在本文中,我们对超椭圆曲线密码的研究现状作了评述,并提出了超椭圆曲线密码理论与实现中急需解决的几个问题.

2 超椭圆曲线背景知识

2.1 超椭圆曲线和它的 Jacobian

首先介绍一下有限域上超椭圆曲线的基本定义和性质,更详细的描述参看文献[3~6]. 设 F_q 是一个有限域, $\overline{F}_q$ 是它的代数闭包. 一条定义在 F_q 上,亏格为 g 的超椭圆曲线(有

收稿日期:2001-04-16;修回日期:2001-07-13
基金项目:国家 973 项目资助(No. G1999035804)

时简称 HC)由下式给出:

$$C: v^2 + h(u)v = f(u) \quad (1)$$

其中 $f(u)$ 是次数为 $2g+1$ 的 $F_q[u]$ 中的首一多项式, $h(u)$ 是次数至多为 g 的 $F_q[u]$ 中的多项式,并且没有解 $(u, v) \in \overline{F}_q \times \overline{F}_q$ 同时满足方程 $v^2 + h(u)v = f(u)$ 和偏微分方程 $2v + h(u) = 0$ 和 $h'(u)v - f'(u) = 0$(这样的点称为奇异点,超椭圆曲线没有奇异点). 设 F_{q^n} 是 F_q 的一个扩域, C 上 F_{q^n}-有理点的集合 $C(F_{q^n})$ 定义为所有满足方程(1)的点 $P = (u, v) \in F_{q^n} \times F_{q^n}$ 与一个特殊的在无穷远处的点 ∞ 所成的集合. 设 $P = (u, v)$ 是超椭圆曲线 C 上一个有限点, P 的负值定义为: $\tilde{P} = (u, -v - h(u))$, $\infty = \infty$. C 上的除子是一个有限形式和 $D = \sum_P m_P P$,这里 m_P 是整数,且只有有限个 m_P 是非零的; D 的次数(degree)定义为 $\deg D = \sum_P m_P$. 如果 $D = \sigma(D)$, $\forall \sigma \in Gal(\overline{F}_{q^n}/F_{q^n})$ ($\overline{F}_{q^n}$的 Galois 群),则除子 D 称为定义在 F_{q^n} 上的. 所有定义在 F_{q^n} 上的除子的集合 $D_C(F_{q^n})$ 形成一个加法交换群,次数为 0 的除子形成的集合 $D_C^0(F_{q^n})$ 是 $D_C(F_{q^n})$ 的一个子群,一个多项式 $G(u, v) \in \overline{F}_q[u, v]$ 的除子定义为 $div(G(u, v)) = \sum_P ord_P(G)P - \sum_P ord_P(G)\infty$,其中 $ord_P(G)$ 是在 P 点零化的阶. 有理函数 $G(u, v)/H(u, v)$ 的除子如下定义: $div(G(u, v)/H(u, v)) = div(G(u, v)) - div(H(u, v))$,被称为主除子. 所有主除子构成一个群,记为 $P_C(F_{q^n})$. 因为主除子的次数是 0,所以 $P_C(F_{q^n})$ 是 $D_C^0(F_{q^n})$ 的一个子群,我们将商群 $D_C^0(F_{q^n})/P_C(F_{q^n})$ 定义为 C 在 F_{q^n} 上的 Jacobian,记为 $J(C; F_{q^n})$.

一个除子称为半归约的(Semi-Reduced),如果它的形式表示中,没有两个点是互负的. 这样的一个除子具有 k 个点(允许是有重复点),则称这个半归约除子的权是 k. 一个归约除子是一个权 $k \le g$ 的半归约除子. 超椭圆曲线 C 的 Jacobian $J(C; F_{q^n})$ 恰好是定义在 F_{q^n} 上的归约除子的集合. $J(C; F_{q^n})$ 的一个重要事实是可以在 $J(C; F_{q^n})$ 中定义归约除子的一个加法运算,使得 $J(C; F_{q^n})$ 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,我们说的超椭圆曲线密码实际上是建立在超椭圆曲线的 Jacobian 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见的构成交换群.

由于有限域上的代数函数域和代数曲线是一一对应的,所以也可以从有限域上超椭圆函数域的角度来研究超椭圆曲线. 由于代数函数域与代数数域有着非常类似的性质,它们统称为整体域,所以对超椭圆函数域的研究可以借鉴于代数数论中虚(或实)二次数域的研究手法及其结果. 有关这方面的讨论可以参见文献[7,8].

2.2 Jacobian 上的群运算和离散对数问题

亏格为 g 的超椭圆曲线 C 定义在有限域 F_q 上(设 $q = p^r$),它在 F_{q^n} 上的 Jacobian 是一个交换群,由 Neal Koblitz[3]和 Cantor[4]的工作知道: C 的 Jacobian 中的元素 $D = \sum m_i P_i - (\sum m_i)\infty$(这里 $\sum m_i \le g$, $P_i = (x_i, y_i)$)可由 $F_{q^n}[u]$ 中的两个多项式 a、b 惟一确定,其中 $a(u) = \prod (u - x_i)^{m_i}$,且 a、b 满足: (1) $\deg b < \deg a \le g$, (2)对所有 $m_i \neq 0$ 的 i, $b(x_i) = y_i$, (3) $b^2 + hb - f \equiv 0 \pmod{a}$. $D = g.c.d.(div(a(u)), div(b(u) - v))$,一般简记为 $D = [a, b]$. 两个除子 $D_1 = \sum m_i P_i - (\sum m_i)\infty$ 和 $D_2 = \sum n_i P_i - (\sum n_i)\infty$ 的 $g.c.d.$ 定义为 $g.c.d.(D_1, D_2) = \sum \min(m_i, n_i) P_i - (\sum \min(m_i, n_i))\infty$.

Jacobian 中的加法由两个过程完成:复合和归约.

算法 1　Jacobian 中的加法

输入:两个 Jacobian 中的除子 $D_1 = [a_1, b_1]$, $D_2 = [a_2, b_2]$

输出: $D_3 = [a_3, b_3] = D_1 + D_2$

复合:

(1)计算 $d = \gcd(a_1, a_2, b_1 + b_2 + h) = s_1 a_1 + s_2 a_2 + s_3(b_1 + b_2 + h)$,

(2)令 $a = a_1 a_2 / d^2$,

(3)令 $b = (s_1 a_1 b_2 + s_2 a_2 b_1 + s_3(b_1 b_2 + f))/d \pmod{a}$.

归约:

(4)令 $a_3 = (f - bh - b^2)/a$, $b_3 = (-h - b) \bmod a_3$,

(5)如果 $\deg a_3 > g$,则令 $a = a_3$, $b = b_3$,返回 4),

(6) c 是 a_3 的首项系数,令 $a_3 = c^{-1} a_3$,

(7)输出 (a_3, b_3).

算法 2　Jacobian 中的倍除子

输入:Jacobian 中的除子 $D_1 = [a_1, b_1]$,

输出: $D_2 = [a_2, b_2] = D_1 + D_1$

复合:

(1)计算 $d = \gcd(a_1, 2b_1 + h) = s_1 a_1 + s_3(2b_1 + h)$

(2)计算 $a = a_1^2 / d_2$, $b = (2s_1 a_1 b_1 + b_1^2 + f)/d \pmod{a}$.

归约:

(3)令 $a_2 = (f - bh - b^2)/a$, $b_2 = (-h - b) \bmod a_2$,

(4)如果 $\deg a_2 > g$,则令 $a = a_2$, $b = b_2$,返回 2),

(5) c 是 a_2 的首项系数,令 $a_2 = c^{-1} a_2$,

(6)输出 (a_2, b_2).

上面的归约是 Cantor[4]归约,它实际上等价于高斯的二元二次型归约算法,后来又有许多人对归约运算作了研究,例如 Lagrange、Andreas Enge 等.

Andreas Enge 在文[9]中对几种除子加运算的计算量作了分析,得到了一次除子加运算用到有限域 F_{q^n} 中运算的一个平均值($q = p^r$):

	有限域乘法	有限域中求逆
$p \neq 2$, g 是偶数	$17g^2 + 5g - 7 + 1/qO(g^3)$	$3/2g + 3 + 1/qO(g^2)$
$p \neq 2$, g 是奇数	$17g^2 + 6g - 4 + 1/qO(g^3)$	$3/2g + 7/2 + 1/qO(g^2)$
$p = 2$, g 是偶数	$14g^2 + 6g - 6 + 1/qO(g^3)$	$3/2g + 2 + 1/qO(g^2)$
$p = 2$, g 是奇数	$14g^2 + g - 3 + 1/qO(g^3)$	$3/2g + 5/2 + 1/qO(g^2)$

一次倍除子运算用到有限域 F_{q^n} 中运算的一个平均值($q = p^r$):

	有限域乘法	有限域中求逆
$p \neq 2$, g 是偶数	$16g^2 + 7g - 6 + 1/qO(g^3)$	$3/2g + 2 + 1/qO(g^2)$
$p \neq 2$, g 是奇数	$16g^2 + 8g - 3 + 1/qO(g^3)$	$3/2g + 5/2 + 1/qO(g^2)$
$p = 2$, $h = 1$, g 是偶数	$7g^2 + 3g - 3 + 1/qO(g^3)$	$1/2g + 2 + 1/qO(g^2)$
$p = 2$, $h = 1$, g 是奇数	$7g^2 + 4g + 1/qO(g^3)$	$1/2g + 5/2 + 1/qO(g^2)$
$p = 2$, $h = u$, g 是偶数	$11g^2 + 4g - 3 + 1/qO(g^3)$	$1/2g + 3 + 1/qO(g^2)$
$p = 2$, $h = u$, g 是奇数	$11g^2 + 5g + 1/qO(g^3)$	$1/2g + 7/2 + 1/qO(g^2)$

$J(C; F_{q^n})$ 上的标量乘是指: D 是 $J(C; F_{q^n})$ (或 $J(C; F_{q^n})$

的一个 n 阶子群)的一个生成元,任取 $m < \#\ J(C; F_{q^n})$ (或 $m < n$),计算 $mD = D + D + \cdots + D$.

$J(C; F_{q^n})$ 上的离散对数问题(HCDLP)是指:给定定义在 F_{q^n} 上的 $J(C; F_{q^n})$ 中的两个除子 D_1、D_2,确定出整数 m,使得 $D_2 = mD_1$(如果这样的 m 存在).

2.3 Frobenius 自同态及其性质

设 F_q 是一个有限域,$\bar{F}_q$ 是它的代数闭包. $C: v^2 + h(u)v = f(u)$ 是一条定义在 F_q 上,亏格为 g 的超椭圆曲线,F_{q^n} 是 F_q 的一个 n 次扩域. 域上的 Frobenius 自同态:$\phi: \bar{F}_q \to \bar{F}_q$, $x \to x^q$ 诱导了 Jacobian 上的一个自同态:

$$\phi: J(C; \bar{F}_q) \to J(C; \bar{F}_q)$$

$$D = \left(\sum_P m_P P\right) \bmod P_C(\bar{F}_q) \to \phi(D) = \left(\sum_P m_P \phi(P)\right) \bmod P_C(\bar{F}_q)$$

这里如果 $P = (x, y)$, $\phi(P) = (x^q, y^q)$;如果 $P = \infty$, $\phi(P) = \infty$.

如果 D 是 $J(C; F_{q^n})$ 中的一个元素,$D = [a(u), b(u)]$, $a(u) = \sum_{i=0}^{k} a_i u^i \in F_{q^n}[u]$, $b(u) = \sum_{i=0}^{k} b_i u^i \in F_{q^n}[u]$,则 $\phi(D) = [\phi(a(u)), \phi(b(u))] = [\sum_{i=0}^{k} a_i^q u^i, \sum_{i=0}^{k} b_i^q u^i]$.

不难证明,$J(C; F_{q^n})$ 上的 Frobenius 自同态是一个线性变换,从而有一个 $2g$ 次的特征多项式. 在 $g = 2$ 的情形,定义在 F_q 上的超椭圆曲线的 Jacobian 的 Frobenius 自同态的特征多项式为:$P(T) = T^4 - s_1 T^3 + s_2 T^2 - s_1 qT + q^2$,

其中 $s_1 = q - (M_1 - 1)$, $s_2 = (M_2 - 1 - q^2 + s_1^2)/2$,这里 M_1、M_2 是定义在 F_q 上的超椭圆曲线在 F_q 和 F_{q^2} 上的有理点的个数(包括一个无穷远点). 对所有的 $D \in J(C; \bar{F}_q)$,有 $\phi^4(D) - s_1\phi^3(D) + s_2 q\phi^2(D) + q^2(D) = \infty$.

3 超椭圆曲线密码体制

有了有限域上超椭圆曲线的 Jacobian 有限群结构及超椭圆曲线离散对数问题的知识,就可以构造离散对数密码体制. HCC 可以模拟基于一般乘法群上的如 Diffie-Hellman 密钥协商、DSA、ElGamal 加密等几乎所有协议. 这里仅以 Diffie-Hellman 协议进行说明.

Diffie-Hellman 算法是第一个公钥算法,它可以用于一组用户进行秘钥协商. 下面以 Alice 和 Bob 二方进行秘钥交换为例来讨论它的超椭圆曲线实现.

公开公共参数:$C: v^2 + h(u)v = f(u)$, $\#\ J(C; F_{q^n}) = nh$, n 是 160bit 大素数(或更大), $h = 1$ 或是较小的余因子, q^n 约为 $160/g$ bit 左右, $D \in J(C; F_{q^n})$ 是 n 阶元素.

(1) Alice 选一个大的随机数 x,然后计算 $X = xD$,将 X 发送给 Bob; (2) Bob 选一个大的随机数 y,然后计算 $Y = yD$,将 Y 发送给 Alice; (3) Alice 计算 $K = xY$; (4) Bob 计算 $K = yX$.

假设超椭圆曲线离散对数问题是困难的,所以公共信道上的其他人不能计算 $K = xyD$,这样,Alice 和 Bob 就可以用事先约好的方法从 K 中获取所需的私钥.

4 有限域上超椭圆曲线有理点及 Jacobian 的阶的计算

设 $C: v^2 + h(u)v = f(u)$ 是定义在 F_q 上,亏格为 g 的超椭圆曲线,由著名的 Weil 猜想[10]可知,计算下面 3 个问题是紧密相连的:(1) 计算 $\#\ C(F_q)$; (2) 计算 $\#\ J(C; F_q)$; (3) 计算 C 的 Frobenius 自同态的特征多项式 $P(T)$. 这 3 个问题有如下联系:设 $\alpha_1, \cdots, \alpha_g$ 是 $P(T) = 0$ 的根,则 $\#\ C(F_{q^n}) = 1 - \sum_{i=1}^{2g} \alpha_i^n + q^n$, $\#\ J(C; F_{q^n}) = \prod_{i=1}^{2g} (1 - \alpha_i^n)$. 从而可以得到有限域 F_q 上超椭圆曲线的有理点的个数与 Jacobian 的阶的关系,例如 $g = 2$ 时, $\#\ J(C; F_q) = 1/2\ \#\ C(F_q)^2 + 1/2\ \#\ C(F_{q^n}) - q$.

下面,逐个说明一下目前常用的几种计算 Jacobian 的阶的方法:

(a) 利用 Weil 猜想的方法:

Weil 猜想的方法是利用 Weil 猜想,将定义在小特征的较小的有限域上的超椭圆曲线提升到较大的扩域上的超椭圆曲线的一种方法,这种方法找的曲线数目较少,且找的曲线有一定的局限性(即不可能找到 Jacobian 的阶具有任意想要的位数的超椭圆曲线),但由于它比较简单,且速度快,所以目前寻找小特征域上的超椭圆曲线大都采用这种方法[3,11~13].

(b) Schoof 算法:

Schoof 算法是随机选曲线,然后计算它的 Jacobian 的阶的方法. 计算出的阶如果含有大素因子,就有可能在它上面构造安全的密码体制. 这一方法最早由 Schoof[14]提出,主要用于计算有限域上椭圆曲线的有理点的个数,后由 Adleman, Huang[15]和 Pila[16]推广到超椭圆曲线上. Schoof 算法的计算复杂度是多项式时间的,但由于计算量和存储太大,并不实用. 在椭圆曲线情况($g = 1$),Atkin 和 Elkies 对 Schoof 算法进行了一些改进,即 SEA 算法,使得这一算法在实际中实现成为可能. 最近,Gaudry 和 Harley[17]综合多种技术,实现了推广的 Schoof 算法,能够计算 $p = 10^{19} + 51$ 的有限域 $GF(p)$ 上的亏格为 2 的超椭圆曲线的点数.

(c) 利用复乘的方法:

Frey 和 Spallek[18]将计算椭圆曲线点的复乘算法推广到了亏格为 2 的超椭圆曲线. 之后又有许多人对此进行了研究[19],最近,A. Weng[20]将这一方法进行了归纳. CM 法是比较有效的,实现速度也比较快,但是由这种方法找出的超椭圆曲线具有复乘,并且和虚二次域的某个阶有内在的联系,所以建立在其上的密码体制可能会存在潜在的不安全性.

(d) 利用 Weil Decant 方法:

这一方法主要针对特征为 2 的有限域,是由 P. Gaudry, F. Hess, N. P. Smart[21]提出. 此方法是首先利用随机产生安全椭圆曲线,然后再经过 Weil 下降方法产生超椭圆曲线,效率比较高,但这种方法的弱点是它产生的超椭圆曲线不是完全随机的,只是在超椭圆曲线的一个子集里是随机的,因此构成的密码体制有可能存在某种弱点,这也是一个值得研究的问题. 由文[22]的讨论,所能利用的椭圆曲线只占全体曲线的极少一部分.

(e) 模曲线法[23]

由于模曲线 $X_0(N)$ 被研究的比较多,这类曲线的 Jacobian 的阶比其他一般曲线的计算要相对容易一些. Muller[23]在他的博士论文中用到了这种技术,不过许多学者对这类曲线上

构造的密码体制的安全性比较怀疑,因为这些曲线具有许多特殊的性质,有可能受到某些新的攻击.

5 超椭圆曲线离散对数问题的攻击

超椭圆曲线密码体制就是建立在求超椭圆曲线离散对数困难基础之上的.超椭圆曲线密码最重要的研究是它的安全性的研究,而它的安全性依赖于 HCDLP 的安全性.对于 HCDLP 的攻击类似于对有限域的乘法群或椭圆曲线离散对数的攻击,不过一些特殊的超椭圆曲线的离散对数有特殊的计算方法.在过去的十多年里,HCDLP 受到了全世界前沿数学家和密码学家的极大关注,不过目前对于低亏格(≤ 4)的 HCDLP 还没有发现有什么特别大的弱点,除了极少特殊的情况外,低亏格的 HCDLP 的攻击都是指数时间的.目前对超椭圆曲线离散对数的攻击,主要有下列方法:

穷搜索;Shanks 的小步大步法和 Pohlig-Hellman 方法;Pollard-Rho 方法;这些都是求解离散对数问题的通用方法,都是指数时间的.

Index 算法:

Adleman-DeMarrais-Huang[24]在 1994 年找到了,解有限域上大亏格超椭圆曲线的 Jacobian 中的离散对数的亚指数时间算法.下面介绍几个相关概念:一个除子 $D=[u,v]$,如果 u 在 F_q 上是不可约的,则称 D 是素的;超椭圆曲线的 Jacobian 中的除子 $D=[u,v]$ 等于素除子 $[u_i,v_i]$ 的和,这里 u_i 是 u 的素因式.一个除子称为 S 光滑的,如果它的所有素除子的次数至多是 S.1 - 光滑的($S=1$)除子是它的多项式 u 在 F_q 上完全分解的除子.记所有除子的次数至多是 S 的除子集合为 G_S,称为因式基(factor basis),有了光滑除子和因式基,就可以运用 index 的思想.

当亏格较小时,Index 算法就不再是亚指数时间算法,但仍然可以用.在 Eurocrypt 2000 上,P. Gaudry[25]讨论了较低亏格的超椭圆曲线离散对数问题的 Index 算法.

下面是 P. Gaudry 解较低亏格的超椭圆曲线离散对数问题的算法:(H 是 Hash 函数)

输入:有限域 F_q 上亏格 g 的曲线的一个除子 D_1,具有素数阶 n,一个除子 D_2,一个参数 r.

输出:一个整数 d,使得 $D_2=dD_1$.

(1)(构造因子基 G)对 F_q 上每一个次数为 1 的首一不可约多项式 u_i 找 v_i,使得 $[u_i,v_i]$ 是曲线的一个除子.如果有一个解,就将 $g_i=[u_i,v_i]$ 保存在 G 中(在两个互反的除子中我们只取其中一个).

(2)(随机 walk 的初始化)j 从 1 到 r,随机从 $[1,\cdots,n]$ 中选取 $a^{(j)}$,$b^{(j)}$,计算 $T^{(j)}:=a^{(j)}D_1+b^{(j)}D_2$,从 $[1,\cdots,n]$ 中随机选取 a_0,b_0,计算 $R_0:=a_0D_1+b_0D_2$.

令 $k=1$

(3)(a)计算 $j=H(R_0)$,$R_0:=R_0+T^{(j)}$,$a_0=a_0+a^{(j)} \bmod n$,$b_0=b_0+b^{(j)} \bmod n$.重复上面步骤,直到 $R_0=[u_0(z),v_0(z)]$ 是一个光滑除子.

(b)在 F_q 上分解 $u_0(z)$,并确定因式在基 G 中的位置,将结果作为矩阵 $M=(m_{ik})$ 的一行,$R_k=\sum m_{ik}g_i$.

存储系数 $a_k=a_0$,$b_k=b_0$.

如果 $k<\#G+1$,令 $k=k+1$,返回(1).

(4)找矩阵 M 的转置的核中的一个非零向量(e_k).

(5)输出 $d=-(\sum a_ke_k)/(\sum b_ke_k) \bmod n$.如果分母为 0,返回(2).

这个算法的计算复杂度是 $O(q^2+g!\,q)$.从而可看出,当亏格 $g>4$ 时,这个方法要比 pollard-Rho 方法好.下表给出了这个算法与 pollard-Rho 方法的对比[25]:

G	1	2	3	4	5	6	7
Rho	$q^{1/2}$	q	$q^{3/2}$	q^2	$q^{5/2}$	q^3	$q^{7/2}$
Index	q^2	q^2	q^2	q^2	q^2	q^2	q^2

超奇异超椭圆曲线:Frey 和 Ruck[26]利用 Tate 对,推广了椭圆曲线的 MOV 攻击,对超奇异超椭圆曲线离散对数提出了一个快速攻击方法(简称 FR 归约).

大素数域 $GF(p)$ 上的超椭圆曲线的 Jacobian 中不能有 p 阶子群:这类似于 Frobenius 变换的迹为 1 的椭圆曲线的 SSSA 攻击,是由 Ruck[27]推广的.

子域超椭圆曲线的 Jacobian 的 Weil Decant 攻击:

利用 Weil 限制的想法去解椭圆曲线离散对数问题是由 Frey[28]首先提出的,之后 Smart 等人[21,29]又做了大量更深入的研究.Galbraith 推广了 Smart 等人的想法,将 Weil 限制的方法应用于有限域上亏格 $g>1$ 的曲线的 Jacobian 上[30].在文[31]中作者对适用于设计密码算法的超椭圆曲线进行了 Weil Descent 分析,同时对定义在 $GF(q^n)$ 上的形如 $y^2+xy=f(x)$ 的超椭圆曲线的离散对数问题能否用 Weil Descent 代数方法攻击作了详细讨论,得到结论:(1)Weil Descent 代数攻击法只能适用于极少部分这类超椭圆曲线;(2)当亏格或基域增大时,Weil Descent 方法攻击成功的概率趋向于 0.

6 超椭圆曲线密码体制实现现状

超椭圆曲线密码体制的实现工作也有许多学者在做,从已有的 HCC 的实现来看,超椭圆曲线密码的实现速度要比椭圆曲线密码实现速度慢,不过在同等安全水平下,低亏格的 HCDSA(DSA 的超椭圆曲线模拟)的实现签名和验证的综合速度仍然比 RSA 快.下面是 HP 实验室的 N. Smart[32]给出的有限域 $GF(2^n)$ 上型如 $y^2+y=f(x)$ 的超椭圆曲线的 HCDSA 的实现:在 Pentium Pro334MHz 上,Windows NT 下,利用 Microsoft Visual C++ 实现了 ECDSA 和 HCDSA(超椭圆曲线数字签名),下表中的时间都是 Ms,p 是 2^{161} 大小的素数.

	有限域	签名	验证
ECDSA	$GF(2^{161})$	4	19
ECDSA	$GF(p)$	3	17
HCDSA $g=5$	$GF(2^{31})$	18	71
HCDSA $g=6$	$GF(2^{31})$	26	98
HCDSA $g=7$	$GF(2^{31})$	40	156

日本的 Yasuyuki Sakai 等人[11,12,33]也对有限域 $GF(2^n)$ 和 $GF(p)$ 上的 HCC 进行了实现.

从 HCC 的实现可看出,超椭圆曲线密码的实现速度要比椭圆曲线密码实现速度慢.之所以这样的一个重要原因是超

椭圆曲线的 Jacobian 上的基本运算比椭圆曲线群的基本运算复杂得多. 所以如何减少超椭圆曲线的 Jacobian 的点加和标量乘的计算量,从而提高超椭圆曲线密码的实现速度是超椭圆曲线密码走向实用的一个非常重要的问题.

7 结束语

超椭圆曲线属于代数几何范畴,近几年被应用于许多领域,除了在本文中讲的超椭圆曲线公钥密码体制外,超椭圆曲线也是 Adleman 和 Huang 随机多项式算法素性证明[34]中的一个关键成分;超椭圆曲线还可以用来设计纠错码[35],这是一种代数几何码;超椭圆曲线还可用于大整数分解算法[36].

尽管超椭圆曲线的标量乘要比椭圆曲线的慢,但由于它在更小的域上运算,从而有许多 ECC 所不具备的优点,并且它的速度可能会得到提高. 超椭圆曲线密码目前在国内外都还处于理论研究阶段,还有很多具体问题没有很好的解决,是密码理论研究中国内外学者研究的热点课题之一. 超椭圆曲线密码要走向实用和成熟,还有许多问题需要解决. 下面列出目前 HCC 研究中急需解决和比较关注的的几个问题:

® 寻找计算超椭圆曲线 Jacobian 的点的个数(或 Frobenius 自同态的特征多项式 $P(T)$)的有效算法;

® 提高超椭圆曲线 Jacobian 上的基本运算的速度;

® 如何提高超椭圆曲线 Jacobian 上的标量乘运算,从而提高整个超椭圆曲线密码体制的实现速度;

® Jacobian 的 Weil Decant 攻击的进一步研究;

® 超椭圆曲线密码体制的标准化.

参考文献:

[1] N Koblitz. Elliptic curve cryptosystems [J]. Math. Comp. 1987, 48 (177): 203 - 209.

[2] V S Miller. Use of elliptic curve in cryptography [A]. In CRYPTO'85 (Santa Barbara, Calif., 1985), LNCS. 218 [C], Spring-Verlag. 1986: 417 - 426.

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

[4] D G Cantor. Computing in the jacobian of a hyperelliptic curve [J]. Math. Comp., 1987, 48: 95 - 101.

[5] N Koblitz. Algebraic Aspects of Cryptography [M]. Algorithms and Computation in Math. 3, Springer-Verlag 1998.

[6] Mumford D. Tata Lectures on Theta II [M]. Birkhauser-Verlag, Boston. 1984.

[7] Paulus Ruck, H-G. Real and imaginary quadratic representations of hyperelliptic function fields logarithms [J]. Math. Comp., 1999, 68: 1233 - 1241.

[8] A Stein. Sharp upper bound for arithmetics in hyperelliptic function fields [R]. Techn. Report CORR # 99-23, University of Waterloo (2000), 68 pages. http://www.cacr.math.uwaterloo.ca.

[9] Andreas Enge. The extended euclidian algorithm on polynomials, and the computational efficiency of hyperelliptic cryptosystems. http://www.math.uni-augsburg.de/~enge/Publikationen.html.

[10] Robin Hartshorne. Algebraic Geometry [M]. GTM 52, Springer-Verlag, New York 1977.

[11] Y Sakai, K Sakurai, H Ishizuka. Secure hyperelliptic cryptosystems and their performance [A]. In PKC, Editors H. Imai and Y. Zheng, Springer-Verlag, , LNCS 1431 [C], 1998: 164 - 181.

[12] Y Sakai, K Sakurai. Design of hyperelliptic cryptosystems in small characteristic and a software implementation over $F(2^n)$ [A]. In ASIACRYPT 98, Editors K. Ohta and D. Pei, Springer-Verlag, , LNCS 1514 [C], 1998: 80 - 94.

[13] C Gunther, T Lange, A Stein. Speeding up the arithmetic on koblitz curves of genus two [R]. Techn. Report CORR # 2000-04, University of Waterloo (2000), 22 pages. http://www.cacr.math.uwaterloo.ca.

[14] R Schoof. Elliptic curves over finite fields and the computation of square roots mod p [J]. Math. Comp., 1985, 44: 483 - 494.

[15] L Adleman, M Huang. Counting rational points on curves and abelian varieties over finite fields [A]. In ANTS-2:, LNCS 1122 [C], Springer-Verlag, 1996: 1 - 16.

[16] J Pila. Frobenius maps of abelian varieties and finding roots of unity in finite fields [J]. Math. Comp., 1996, 55(192): 745 - 763.

[17] Pierrick Gaudry, Robert Harley. Counting points on hyperelliptic curves over finite fields [R]. http://www.cs.bris.ac.uk/Tools/Reports/Abstract/2000-gaudry.htm

[18] A-M Spallek. Kurven vom geschlecht 2 und ihre anwendung in public-key-kryptosystemen [D]. PhD thesis, Universitat Essen, 1994.

[19] Jinhui Chao, Kazuto Matsuo, Shigeo Tsujii. Fast construction of secure logarithm problems over Jacobian varieties [A]. in Information Security for Global Information Infrastructures [C], 461 - 470, Sihan Qing and Jan H. P. (Eds), IFIP TC-11 Working Conference on Information Security, Aug. 22 - 24, 2000. Beijing, China. Kluwer 2000.

[20] Annegret Weng. Constructing hyperelliptic curves of genus 2 suitable for cryptography. http://www.exp-math.uni-essen.de/~weng/.

[21] P Gaudry, F Hess, N P Smart. Constructive and destructive facets of weil descent on elliptic curves [R]. http://www.cs.bris.ac.uk/Tools/Reports/Abstract/2000-gaudry.htm.

[22] S D Galbraith. Limitation of constructive weil descent, http://www.cs.bris.ac.uk/~stenve.

[23] M Muller. Algorithmische konstruktion hyperelliptischer kurven mit kryptographischer relevanz und einem endomorphisenring echtgrosser als Z [D]. Phd-Thesis, Universitat Essen, 1996.

[24] L Adleman, J DeMarrais, M Huang. A subexponential algorithm for discrete logarithms over the rational subgroup of the jacobians of large genus hyperelliptic curves over finite fields [A]. in ANTS-1, LNCS 877 [C], Springer-Verlag, 1994: 28 - 40.

[25] P Gaudry. An algorithm for solving the discrete log problem on hyperelliptic curves [A]. In B. Preneel (ed.), Eurocrypt 2000, LNCS 1807 [C], Springer-Verlag, 2000: 19 - 34.

[26] Frey G, Rück H. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves [J]. Math. Comp, 1994, 62: 865 - 874.

[27] H G Ruck. On the discrete logarithms in the divosor class group of curves [J]. Math. Comp., 1999, 68: 805 - 806.

[28] G Frey. How to disguise an elliptic curve [A]. Talk at ECC'98, Waterloo [C], 1998. http://cacr.math.uwaterloo.ca/conferences/1998/ecc98/slides.html.

[29] S D Galbraith ,N P Smart. A cryptographic application of Weil descent [A]. Proceedings Cryptography and Coding ,Springer LNCS 1746 [C] , 1999 :191 - 200.

[30] S D Galbraith. Weil descent of Jacobians [OL] ,http :/ / www. cs. bris. ac. uk/ ～stenve.

[31] Fangguo Zhang , Yumin Wang. An analysis of weil descent attack on the hyperelliptic curves discrete logarithm. Accepted by ChinaCrgpt '02.

[32] Smart N. On the performance of hyperelliptic cryptosystems [A]. In EUROCRYPT'99 , Editors J. Stern , Springer-Verlag ,LNCS 1592 [C] , 1999 :165 - 175.

[33] Yasuyuki Sakai , Kouichi Sakurai. On the practical performance of hyperelliptic curve cryptosystems in software implementation [J]. IEICE , 2000 ,4 : E83-A.

[34] L Adleman ,M Huang. Primality testing and Abelian Varieties over Finite Fields [M]. Lecture Notes in Mathematics 1512 ,Springer-Verlag , berlin ,1992.

[35] D Le Brigand. Decoding of codes on hyperelliptic curves [A]. Eurocode '90 ,LNCS 514 [C] ,Springer-Verlag ,1991 :126 - 134.

[36] H W Lenstra ,J Pila , C Pomerance. A hyperelliptic smoothness test. I [A]. Philosophical Transactions of the Poyal Society of London A [C] , 1993 ,345 :397 - 408.

作者简介:

张方国　男. 生于 1972 年 12 月. 博士研究生. 1996 年在烟台师范学院数学系获得理学学士学位 ,1999 年在上海同济大学应用数学系获得理学硕士学位 ,现在西安电子科技大学通信工程学院攻读密码学博士学位 ,研究兴趣是电子商务 ,椭圆曲线和超椭圆曲线密码体制.

王育民　(见本期第 21 页)

2002 年中国 IT 技术趋势与产业发展高峰论坛
崇尚科学精神　激荡专业思维

"2002 年中国 IT 技术趋势与产业发展高峰论坛"于 2001 年 12 月 28 日在北京新世纪饭店举行. 此次论坛由中国电子信息产业发展研究院主办;北京赛迪信息技术评测有限公司承办;中国计算机用户协会协办;支持单位有:中国电子学报、中国计算机报、中国计算机用户、赛迪网.

论坛首先由中国电子信息产业研究院苟仲文院长致词并祝论坛成功举行. 论坛上特邀专家作了主题报告:中国工程院倪光南院士演讲报告的题为"中国 IT 核心技术的发展";中国人工智能学会理事长、北京邮电大学钟义信教授报告题为"网络技术的发展、面临的危机及解决方案";思科网络技术有限公司互联网商业解决方案执行经理隋成岩先生报告题为"互联网时代的 IT 理念";微软有限公司开发部软件开发首席专家蔡锟先生报告题为"Microsoft. NET Internet 发展方向";海军计算技术研究所、中国工程院沈昌祥院士报告题为"信息安全国家发展战略思考与对策";联想研究院研究员信息安全实验室主任韦卫博士报告题为"网络安全的关键技术";中网通信网络有限公司总裁罗与曾先生报告题为"2002 年网络安全展望". 上述 7 位专家和学者就 IT 技术、网络技术、信息安全技术等热点问题阐述了自己的观点 ,精彩的演讲受到了与会代表的欢迎.

此次高峰论坛还邀请了国家各部委信息中心主任和部分厂家代表以及研究所、大学的专家学者、IT 公司的技术人员和管理人员等 200 余人参加论坛. 论坛期间行业用户与厂家及技术专家之间还进行了充分的交流和沟通 ,为今后进一步合作和为 IT 技术的发展创造了条件.

代表们感谢本次论坛的承办单位赛迪评测组织此次高峰论坛 ,给大家提供了交流学习的机会. 赛迪评测作为赛迪集团所属的第三方专业评测机构 ,始终秉承"科学、权威、客观、公正"的服务宗旨 ,面向消费者、IT 企业、行业和媒体用户提供整机测试、外设测试、配件测试、网络通信测试、消费 IT 产品测试、软件测试等系列评测服务 ,旨在通过权威的评测服务为厂商和用户之间筑起沟通的桥梁.