一种超椭圆曲线密码体制的快速求阶算法*)

李 彬 郝克刚
(西北大学计算机科学系软件工程研究所 西安 710000)

摘 要 本文基于代数方法阐述了 HCC 有关数学理论,给出关于一条超椭圆曲线的 Jacobian 求阶算法及其实例证明。基于 ECC 思想与国际标准规范,提出一种超椭圆曲线范围参数,讨论了适应于密码学的超椭圆曲线表示及其 Jacobian 上安全曲线的选择问题。

关键词 超椭圆曲线,离散对数

A Fast Exponent Arithmetic of Hyperelliptic Curves Cryptosystrm

LI Bin HAO Ke-Gang
(SEI,Computer Science Department,NorthWest University,Xi'an 710000)

Abstract The maths theory of hyperelliptic curves cryptosystem(HCC)is expatiated in this article while the arithmetic of HCC Jacobian addition is also set forth, and its correctness is proved by examples. A HC parameter is signed, and its strict express arithmetic is realized based on ECC and international standards which adapt to figure HC in cryptosystrm and count exponent of Jacobian. This arithmetic gives more aid for the selection of secure HC.

Keywords Hyperelliptic curves cryptosystem(HCC),Discrete logarithm

1 引言

超椭圆曲线密码是将古老且富有活力的深奥数学理论与工程技术领域中的密码技术结合在一起的一门综合、交叉的边缘学科,它涉及到代数数论、代数几何、解析数论、通信与信息理论、计算机软件、硬件、操作系统、计算机网络与应用等多门学科知识。目前,超椭圆曲线密码体制(HCC)已引起了国、内外学者的关注。超椭圆曲线是亏格 g≥1 时的一类特殊代数曲线,可以被看成是亏格 g=1 椭圆曲线的推广。1989 年,Neal Koblitz[1]基于有限域上超椭圆曲线的 Jacobian 群的计算离散对数问题困难性,提出了超椭圆曲线密码体制(HCC)。尽管近几年在理论与应用中取得了巨大的进展,新理论、新方法及新技术也不断涌现,但到目前为止尚未形成一个完整的理论体系,仍有许多问题等待解决[2]。一方面原因是因为 HCC 没有国际标准化;另一方面,确定 HCC 中的 Jacobian 群的阶比较困难,群运算规则也比椭圆曲线密码(ECC)复杂,使得其运算速度不如 ECC。

本文针对 HCC 计算 Jacobian 群的阶这一问题进行深入讨论,给出一种算法,并通过实例说明此算法的可行性。

2 HCC 基本数学理论

定义 1(超椭圆曲线) 设 K 是一个有限域,$\bar{K}$ 是它的代数闭包。一条定义在 K 上的亏格为 g 的超椭圆曲线(有时简称 HC)由下式给出:

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

其中 $f(u)\in K[u]$是次数为 $2g+1$ 的首一多项式,$h(u)\in K[u]$是次数至多为 g 的 $K[u]$中的多项式,并且没有解$(u,v)\in\bar{K}\times\bar{K}$ 同时满足方程 $v^2+h(u)v=f(u)$和偏微分方程 $2v+h(u)=0$ 和 $h'(u)v-f'(u)=0$。

让 L 是域 K 的一个扩域。在 C 上的 L-有理点,表示为 $C(L)$,是满足于曲线 C 的方程(1)中所有点的集合 $P=(x,y)\in L\times L$,伴随一个特殊的点,称为无穷远处点,表示为∞。点 $C(\bar{k})$的集合简单表示为 C。除了无穷远处的点∞,其它点被称为有限点。让 $P=(x,y)$是曲线 C 上的有限点,则点 P 的负元定义为 $\bar{P}=(x,-y-h(x))$,也是在 C 上。约定$\overline{\infty}=\infty$。如果一个有限点 P 满足 $P=\bar{P}$,则该点被称为一个特殊点;否则,该点为普通点。同时满足方程(1)和两个偏微分方程的点称为奇异点。要注意的是超椭圆曲线是没有奇异点的。

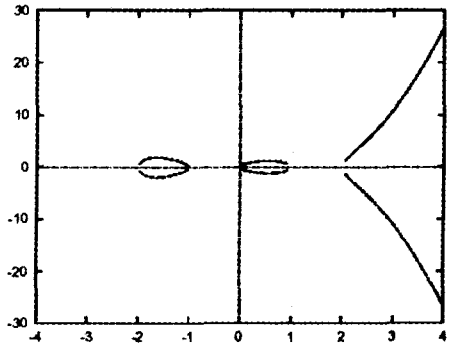


图 1 实数域上超椭圆曲线 $C_3: v^2=u^5-5u^3+4u$

考虑到一条具体曲线 $C: v^2+uv=u^5+5u^4+6u^2+u+3$ 是在有限整数域 Z_7 上。这里 $h(u)=u, f(u)=u^5+5u^4+6u^2+u+3$ 及亏格 $g=2$。由域相关知识,可以验证曲线 C 没有任何奇异点(除了无穷远点∞),因此 C 确实是一条超椭圆曲线其上的 Z_7 一有理点是 $C(Z_7)=\{\infty,(1,1),(1,5),(2,2),(2,3),(5,3),(5,6),(6,4)\}$,其中点(6,4)为一个特殊的点。

*)国家 863 计划资助项目,项目编号:2001AA115090。李 彬 博士生,主要研究方向:电子商务,网络安全。郝克刚 教授,博导,主要研究方向:软件工程,构件技术,电子商务,网络安全。

同样，对于有限域$=F_{2^5}=F_2[x]/(x^5+x^2+1)$上亏格为2的曲线$C:v^2+(u^2+u)v=u^5+u^3+1$。这里，$h(u)=u^2+u$，$f(u)=u^5+u^3+1$。可以验证曲线$C$没有任何奇异点(除了无穷远点$\infty$)。(0,1)和(1,1)是其上的特殊点。

例如下图就是在上述理论下的实数域上超椭圆曲线C_3：$v^2=u^5-5u^3+4u$。

3 超椭圆曲线密码的jacobian $J(K)$安全性要求

关于超椭圆曲线密码体制的安全性也是建立在超椭圆曲线离散对数问题(HCDLP)基础上的，即对于给定的约化除子D_1，D_2，确定一个正整数l使得$D_2=lD_1$，可以看作是有限域乘法群上或椭圆曲线有理点群上的密码体制的模拟。由于超椭圆曲线Jacobian自身所具有的特殊结构，使得其在密码学上的应用与其它基于离散对数问题的公钥密码体制有着许多不同的实现细节，如H-ElGamal加密算法、HDH密钥协商算法、HCDSA数字签名算法等[13]。

为选择安全的超椭圆曲线，必须选择一条合适的曲线C及凭借有限域K，即超椭圆曲线范围参数。在凭借有限域K的算法应具有实现上的有效性，特征为2的有限域似乎是最有吸引力的选择。C的jacobian $J(K)$的阶表示为$\#J(K)$，应能除以一个大的素数。按当前计算机技术水平，一个安全需求为$\#J(K)$除以一个大的素数r，至少应为45位十进制数。另外，为避免MOV约化攻击，r不应整除q^k-1，因为对于所有的小的k，在F_{q_k}上的离散对数问题是容易解的($1\leqslant k\leqslant 2000/\log_2 q$可满足安全要求)。因此，与ECC范围参数类似，超椭圆曲线密码体制范围参数有：曲线$C:v^2+h(u)v=f(u)$，其中，$\#J(C;F_q)=nh$为Jacobian除子类群的阶，其中n是160bit大素数(或更大)，$h=l$或$h<2^6$是较小数称为余因子，q约为g^{160}bit左右。

4 超椭圆曲线的求阶算法

目前国际上，计算超椭圆曲线的$\#J(C;F_q)$也已经有多项式时间算法，如Adleman，Huang[3]和Pila[4]推广的Schoof方法。从而使得计算椭圆曲线有理点群的阶已经可行，而且还可能会有更有效的算法被发明，就像在椭圆曲线情况，又提出了比SEA更有效的Satoh算法[5]。对于特征为2的有限域，P. Gaudry[6]等人在2000年提出了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。

下面，我们利用复数域上椭圆曲线有关理论，给出一种计算$\#J(K)$的算法。

让J为定义在域F_q上的超椭圆曲线C(由方程$v^2+h(u)v=f(u)$给出)的jacobian，F_{q^n}表示F_q上度-n的扩域，N_n表示有限Abelian群$J(F_{q^n})$的阶。M_n表示C上F_{q^n}-有理点的个数。对曲线C，关联一个zeta-函数。

定义2(zeta-函数) 让C为域F_q上的超椭圆曲线，对于$r\geqslant 1$让$M_r=\#C(F_{q^r})$。C上zeta-函数是幂级数

$$Z_C(t)=\exp\left(\sum_{r\geqslant 1}M_r\frac{t^r}{r}\right)$$

关于zeta-函数，有下列著名的属性。

定义3(zeta-函数属性) 让C为域F_q上亏格为g的超椭圆曲线，$Z_C(t)$是C的zeta-函数。

$Z_C(t)\in Z(t)$。更进一步，有$Z_C(t)=\dfrac{p(t)}{(1-t)(1-qt)}$ (2)

这里$P(t)$是一个具有整数系数且度为$2g$的多项式。此外$P(t)$具有下列形式：

$$P(t)=1+a_1t+\cdots+a_{g-1}t^{g-1}+a_gt^g+qa_{g-1}t^{g+1}+q^2a_{g-2}t^{g+2}+\cdots+q^{g-1}a_1t^{2g-1}+q^gt^{2g} \quad (3)$$

(ii)$P(t)$分解为

$$P(t)=\prod_{i=1}^{g}(1-a_i)(1-\bar{a}_i) \quad (4)$$

其中每个α_i是一个复数，其绝对值为$\sqrt{q}$，而$\bar{a}_i$表示α_i的复共轭。

(iii)$N_n=$分解为$\#J(F_{q^n})$满足

$$N_n=\prod_{i=1}^{g}|1-a_i^n|^2 \quad (5)$$

其中$\|$表示通常的复数绝对值。

为了计算N_n，只要(i)确定$P(t)$的系数$a_1,a_2,\cdots,a_g$，(ii)分解$P(t)$由此确定α_i；(iii)通过方程(5)计算N_n。现在方程(5)的二边乘以$(1-t)(1-qt)$生成$P(t)=(1-t)(1-qt)Z_C(t)$。

二边取对数及关于t的微分生成$\dfrac{p'(t)}{p(t)}=\sum_{r\geqslant 0}(M_{r+1}-1-q^{r+1})t^r$。根据方程二边的系数$t^0,t^1,\cdots,t^g$，我们看到第一个$g$值$M_1,M_2,\cdots,M_g$，足以确定出系数$a_1,a_2,\cdots,a_g$，由此得出$N_n$。

下面的过程总结了$g=2$情形下，计算N_n的技术。

算法1 N_n的算法

1. 通过穷举搜索，计算M_1,M_2；
2. $Z_C(t)$的系数由$a_1=M_1-1-q$及$a_2=(M_2-1-q^2+a_1^2)/2$；
3. 解二次方程$X^2+a_1X+(a_2-q)=0$，以得到二个解γ_1和γ_1；
4. 解$X^2-\gamma_1X-q=0$，获得一个解α_2；
5. $N_n=|1-a_1^n|^2\cdot|1-a_2^n|^2$。

下面是关于jacobian的N_n的边界的推论：

推论1 让C是一条定义在F_q上亏格为g的超椭圆曲线以及$N_n=\#J(F_{q^n})$，则$(q^{n/2}-1)^{2g}\leqslant N_n\leqslant(q^{n/2}+1)^{2g}$，因此，$N_n\approx q^{ng}$。

例子(选择一条超椭圆曲线)考虑下列定义在F_2上亏格为2超椭圆曲线C：

$C:v^2+v=u^5+u^3+u$

通过穷举搜索，计算$M_1=3,M_2=9$；因此$a_1=0$及$a_2=2$。$X^2-2=0$的解$\gamma_1=\sqrt{2},\gamma_2=-\sqrt{2}$。解$X^2-\sqrt{2}X+2=0$，产生$\alpha_1=(\sqrt{2}+\sqrt{6}i)/2$；解$X^2+\sqrt{2}X+2=0$，产生$\alpha_1=(-\sqrt{2}+\sqrt{6}i)/2$。因此

$$N_n=|1-a_1^n|^2\cdot|1-a_2^n|^2=\begin{cases}2^{2n}+2^n+1,\text{if } n\equiv 1,5(\bmod 6),\\(2^n+2^{n/2}+1)^2,\text{if } n\equiv 2,4(\bmod 6),\\(2^n+2^{n/2}+1)^2,\text{if } n\equiv 2,4(\bmod 6),\\(2^n-1)^2,\text{if } n\equiv 3(\bmod 6),\\(2^{n/2}-1)^2,\text{if } n\equiv 0(\bmod 6)\end{cases}$$

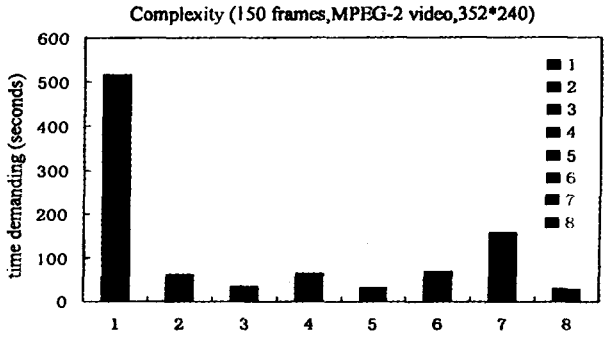
对于$n=101$，

$N_{101}=6427752177035961102167848369367185711289268443393416474761625 7$，

它的素因子为

$N_{10}=7\cdot 607\cdot 1512768222413735255864403005264105839324374778\ 520631853993$

(下转第152页)



1:完全解码和编码;2:Zou 的水印嵌入耗时;3:Zou 的水印检测耗时;4:Lu 的水印嵌入耗时;5:Lu 的水印检测耗时;6:Frank 的水印嵌入耗时;7:Frank 的水印检测耗时;8:解码到 VLC 域耗时

图 8 时间消耗比较

结论和未来展望 本文提出了一个使用扩展的 m-序作为水印模式的变长码域的实时视频水印算法。通过理论分析和试验验证表明,该算法在满足实时性和视频水印其它基本要求的前提下,同 Lu 和 Frank 提出的两种算法进行比较,能够获得更好鲁棒性,同时引起的视觉退化最小,即本算法性能更好。

本算法选用扩展的 m-序作为水印模式,充分利用其良好的均衡性获得了较好的性能。由于扩展 m-序有较好的自相关特性和交叉相关特性,利用该特性和码分复用技术可以提高水印系统的有效载荷,这将是以后进一步研究的内容。

参 考 文 献

1 Frank H, Bernd G. Watermarking of uncompressed and compressed video. Signal Processing, 1998, 66(3): 283～301

2 Langelaar G C, Lagendijk R L, Biemond J. Real-time labeling of MPEG-2 compressed video. Journal of Visual Communication and Image Representation, 1998, 9(4): 256～270

3 Langelaar G C, Lagendijk R L. Optimal differential energy watermarking of DCT encoded images and video. IEEE Transactions on Image Processing, 2001, 10(1): 148～158

4 Ling Hefei, Lu Zhengding, Zou Fuhao. New real-time watermarking algorithm for compressed video in VLC domain. In: Proc. of 2004 International Conference on Image Processing(ICIP). Piscataway, NJ, USA: IEEE, 2004. 2171～2174

5 Lu Chun-Shien, Chen Jan-Ru, Liao H-Y M, et al. Real-time MPEG video watermarking in the VLC domain. In: Proc. of 16th International Conference on Pattern Recognition. Los Alamitos, CA, USA: IEEE Comput. Soc, 2002. 552～555

6 Lu Chun-Shien, Huang Shih-Kun, Sze Chwen-Jye, et al. Cocktail watermarking for digital image protection. IEEE Transactions on Multimedia, 2000, 2(4): 209～224

7 Cox I J, Kilian J, Leighton F T, et al. Secure spread spectrum watermarking for multimedia. IEEE Transactions on Image Processing, 1997, 6(12): 1673～1687

8 Huang Jiwu, Shi Y Q, Shi Yi. Embedding image watermarks in DC components. IEEE Transactions on Circuits and Systems for Video Technology, 2000, 10(6): 974～979

9 Watson A B. DCT quantization matrices visually optimized for individual images. In: Proc. of Conference of Human Vision, Visual Processing, and Digital Display IV. San Jose, CA, USA: SPIE, 1993. 202～216

10 Zou Fuhao, Lu Zhengding, Ling Hefei. A multiple watermarking algorithm based on CDMA technique. In: Proc. of the 12th ACM International Conference on Multimedia(ACM Multimedia 2004). New York, NY, USA: ACM, 2004. 424～427

11 Fiebig U-C G, Schnell M. Correlation properties of extended m-sequences. Electronics Letters, 1993, 29(20): 1753～1755

(上接第 144 页)

结论 超椭圆曲线密码尽管近几年在理论与应用中取得了巨大的进展,新理论、新方法及新技术也不断涌现,但到目前为止尚未形成一个完整的理论体系,仍有许多问题等待解决。本文给出关于一条超椭圆曲线的 jacobian J(K)的快速算法,可以快速有效地计算出超椭圆曲线 Jacobian 除子类群的阶,并通过实例证明该算法的有效性。超椭圆曲线密码体制(HCC)的标准化和实用化是一个亟待解决的问题,我们下一步的研究方向是如何提高超椭圆曲线 Jacobian 上的基本运算及其上标量乘运算的速度,从而使超椭圆曲线密码体制得以实际应用于密码安全方案中。

参 考 文 献

1 Koblitz N. Hyperelliptic cryptosystems. Journal of Cryptology, 1989(1): 139～150

2 Hess F, Seroussi G, Smart N. Two Topics in Hyperelliptic Cryptography: [HP Labs Technical Reports, HPL-2000-118]. 2000

3 Adleman L, Huang M. Counting rational points on curves and abelian varieties over finite fields. In ANTS-2, LNCS 1122, Springer-Verlag, 1996. 1～16

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

5 Satoh T. Canonical Lifting of Elliptic Curves and p-Adic Point Counting - Theoretical Background. Workshop on Elliptic Curve Cryptography - ECC'00, 2000. Available at: http://www.exp-math.uni-essen.de/～galbra/eccslides/eccsldes.html

6 Gaudry P, Hess F, Smart N. Constructive and destructive facets of Weil descent on elliptic curves. preprint, January 2000. Available at: http://www.hpl.hp.com/techreports/2000/HPL-2000-10.html

7 Kocher P, Jaffe J, Jun B. Differential power analysis. Advances in Cryptology - Crypto '99, Lecture Notes in Computer Science, Springer-Verlag, 1999, 1666: 388～397

8 Kelsey J, Schneier B, Wagner D, Hall C. Cryptanalytic attacks on pseudorandom number generators. Fast Software Encryption - FSE '98, Lecture Notes in Computer Science, Springer-Verlag, 1998, 1372: 168～188

9 Dobbertin H, Bosselaers A, Preneel B. RIPEMD-160: A strengthened version of RIPEMD. Fast Software Encryption - FSE '96, Lecture Notes in Computer Science, Springer-Verlag, 1996, 1039: 71～82

10 Vaudenay S. Hidden collisions on DSS, Advances in Cryptology - Crypto '96, Lecture Notes in Computer Science, Springer-Verlag, 1996, 1109: 83～88

11 Blake-Wilson S, Menezes A. Unknown key-share attacks on the station-to-station(STS) protocol. Public Key Cryptography - Proceedings of PKC '99, Lecture Notes in Computer Science, Springer=Verlag, 1560: 154～170

12 Kocher P. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems, Advances in Cryptology - Crypto '96, Lecture Notes in Computer Science, Springer-Verlag, 1996, 1109: 104～113

13 张方国,王育民. 超椭圆曲线密码体制的研究与进展. 电子学报, 2002, 30(1): 26～131