一类 Koblitz 椭圆曲线的快速点乘*

胡 磊[1+], 冯登国[2], 文铁华[3]

[1](信息安全国家重点实验室(中国科学院 研究生院),北京 100039)

[2](中国科学院 软件研究所,北京 100080)

[3](中南大学 信息科学与工程学院,湖南 长沙 410083)

Fast Multiplication on a Family of Koblitz Elliptic Curves

HU Lei[1+], FENG Deng-Guo[2], WEN Tie-Hua[3]

[1](State Key Laboratory of Information Security (Graduate School, The Chinese Academy of Sciences), Beijing 100039, China)

[2](Institute of Software, The Chinese Academy of Sciences, Beijing 100080, China)

[3](School of Information Science and Technology, Central South University, Changsha 410083, China)

+ Corresponding author: Phn: 86-10-88256435, Fax: 86-10-88258317, E-mail: hu@is.ac.cn

http://home.is.ac.cn

Received 2002-09-12; Accepted 2002-12-31

Hu L, Feng DG, Wen TH. Fast multiplication on a family of Koblitz elliptic curves. *Journal of Software*, 2003,14(11):1907~1910.

http://www.jos.org.cn/1000-9825/14/1907.htm

Abstract: Fast point multiplication on a family of Koblitz elliptic curves in characteristic 3 is considered. Such curves are suitable for establishing provable secure cryptographic schemes with low bandwidth. By utilizing the complex multiplication property of the curves and using a modulo reduction and Frobenius expansion technique, it is shown that there is a fast point multiplication method without precomputation on the curves, which is 6 times faster than the ordinary repeated-double-add method. The idea of the fast method is independent of the optimization of finite field arithmetic and the choice of coordinate expression for points of the elliptic curves.

Key words: elliptic curve; point multiplication; Frobenius expansion; modulo reduction; fast algorithm

摘 要: 考虑一类特征 3 的 Koblitz 椭圆曲线的快速点乘算法.在这类曲线上适合建立低带宽的、可证明安全的密码体制.结果显示,利用这类曲线的复乘性质,使用模约减和 Frobenius 展开技巧,这类曲线上存在一种不带预计算的快速点乘算法,其运算速度是通常的重复加倍-点加算法的 6 倍.该算法的快速优化原理与有限域算术优化和椭圆曲线点的坐标表示的选取无关.

关键词: 椭圆曲线;点乘;Frobenius 展开式;模约减;快速算法

中图法分类号: TP309 **文献标识码**: A

* Supported by the National Natural Science Foundation of China under Grant No.90104034 (国家自然科学基金); the National High-Tech Research and Development Plan of China under Grant No.2002AA141020 (国家高技术研究发展计划(863))

第一作者简介: 胡磊(1967－),男,湖北麻城人,博士,教授,博士生导师,主要研究领域为密码学与信息安全.

超奇异椭圆曲线一直被排斥在椭圆曲线密码(ECC)的主流应用之外,这是因为通过使用所谓 Weil 配对或 Tate 配对的双线性型,存在著名的 MOV 攻击[1]和 FR 攻击方法[2],将 $GF(q)$上超奇异椭圆曲线上离散对数问题(DLP)约减到 $GF(q^l)$上离散对数问题($l\leq 6$),以降低由这类曲线构造的 ECC 系统的安全性.但最近 Joux 的先锋性工作[3]表明,使用同样的配对双线性型,超奇异椭圆曲线可以用来构造低带宽的、可证明安全的(provable secure)、基于双线性型的加密、签名和密钥协商方案[3~8].

基于复乘理论,Koblitz 提出了研究具有快速点乘优势的、现在国际密码学界通常统称为 Koblitz 曲线的椭圆曲线[9~11].由于应用需求的驱动,特征 2 的 Koblitz 曲线的点乘运算得以充分研究[12,13].

本文研究一类特征 3 的超奇异 Koblitz 椭圆曲线的点乘算法.这类曲线被用作构造文献[5,6]的密码方案的几类首选曲线之一.由于这类曲线上 DLP 仅约减为 $GF(q^6)$上 DLP 离散对数问题($l=6$),这类曲线被 Koblitz 本人建议用在数字签名方案的实现中[11].在本文中,利用这类曲线的复乘性质,通过使用模约减和 Frobenius 展开技巧,我们显示这类曲线上存在一种不带预计算的快速点乘算法,其运算速度是通常的重复加倍-点加算法的 6 倍,而且该算法的快速优化原理与有限域算术优化和椭圆曲线点的坐标表示的选取无关.

1 算法的基本思想

设 n 是与 6 互素的整数,$a=1$ 或 -1.考虑椭圆曲线

$$E/GF(3^n):y^2=x^3-x+a, \tag{1}$$

该曲线 E 的阶和符合密码应用的 n 的选取可参见文献[5,6].由 E 的复乘性质,E 上的 Frobenius 映射

$$\Phi:(x,y)\to(x^3,y^3),\forall(x,y)\in E \tag{2}$$

满足[11]

$$(\Phi^2+3a\Phi+3)P=O,\forall P\in E. \tag{3}$$

由有限域知识可知,Φ的像可用与 E 上点加相比忽略不计的时间计算出.

设 $\varphi=(-3a+\sqrt{-3})/2$ 是多项式 $x^2+3ax+3$ 的一个实数根.设 k 是小于 E 的阶的正整数,P 是 E 上任意一点.为了计算点乘 kP,将 k 表示成一个表达式 $f(\varphi,\varphi)$,这里 $f(x,y)=\sum b_{ij}x^iy^j$ 是一个整系数多项式,使得 $k-f(x,x)$被 $x^2+3ax+3$ 整除,即使得 $k=f(\varphi,\varphi)$,则由式(3),$kP=f(\Phi,\Phi)P$.由 $\Phi(Q_1+Q_2)=\Phi(Q_1)+\Phi(Q_2)$对任意 $Q_1,Q_2\in E$ 成立的事实,我们有

$$kP=\sum_{i,j}b_{ij}\Phi^{i+j}P=\sum_i\Phi^i(\sum_j b_{ij}\Phi^jP)=\sum_i\Phi^i(P_i)\ , \tag{4}$$

这里,$P_i=\sum_j b_{ij}\Phi^jP$.设 N 为脚标 i 的最大值,则

$$kP=\sum_{i=0}^{N}\Phi^i(P_i)=\Phi(...\Phi(\Phi(\Phi(P_N)+P_{N-1})+P_{N-2})+...+P_1)+P_0\ . \tag{5}$$

关键想法是,如果 P_i 可以用忽略不计(相比于点加)的时间计算出来,则按照式(5)计算 kP 只需 r 个点的加法运算,即 $r-1$ 次加法运算,其中 r 是不等于无穷远点的 P_i 的个数.

以 $P(x,y)$表示 E 上坐标为(x,y)的点.由椭圆曲线的群律[14]和有限域特征为 3 的事实容易推出

$$(\Phi+a)P(x,y)=P(x^3,y^3)+aP(x,y)=P(x+a,ay), \tag{6}$$
$$(\Phi+a)^2P(x,y)=P(x+2a,a^2y)=P(x-a,y).$$

由于$-P(x,y)=P(x,-y)$,因此集合

$$\{O,\pm P,\pm(\Phi+a)P,\pm(\Phi+a)^2P\} \tag{7}$$

中的每个点的坐标表示可以由 P 立即计算得出.我们让 P_i取自式(7),即让 $\sum_j b_{ij}\varphi^j$ 取自集合

$$S=\{0,\pm1,\pm(\varphi+a),\pm(\varphi+a)^2\},$$

而将 k 表示成形如 $\sum_{i=0}^{N}a_i\varphi^i$ $(a_i\in S)$的表达式(称为φ-表达式),其中非零系数 a_i 的个数称为该φ-表达式的权,N 称为该φ-表达式的长度(假设 $a_N\neq0$),则以上方法计算 kP 的复杂度仅与 k 的φ-表达式的权成正比例.

不难看出,当 k 换成形如 $c+d\varphi$的元素(c,d 为整数)时,上述思想可用于计算 $cP+d\Phi(P)$.

注意到,一个元素的φ-表达式不是惟一的,因为一个φ-表达式加上$\varphi^2+3a\varphi+3$ 的任意倍式仍表示原来的元素.在点乘计算的时候,应该使用极小权的φ-表达式.下节我们证明对一个元素 $c+d\varphi$,都存在惟一的φ-表达式满足$a_ia_{i+1}=0(\forall 0\le i\le N-1)$,并且这个$\varphi$-表达式(称为非连接$\varphi$-表达式)具有极小权.计算非连接$\varphi$-表达式的算法见文献[11],其计算量与椭圆曲线的点加运算相比可以忽略不计.

利用Φ^n-1 对椭圆曲线的作用为零的特性,我们可以进一步约减所用φ-表达式的长度和平均权,从而将上述点乘方法的计算速度再加快一倍.我们在第 3 节给出这个模Φ^n-1 约减的技巧.

2 非连接 Frobenius 展开式的权的极小性

记 $Z[\varphi]=\{c+d\varphi:c,d\in Z\}$, $s=(1+\sqrt{-3})/2$, $S'=\{s^i\varphi:i=0,1,\ldots,5\}$.$Z[\varphi]$的元素可惟一地写成 $c+ds$ 形式,其中 c,d 为整数.用复数的模的平方定义 $c+ds$ 的范,即 $N(c+ds)=c^2+cd+d^2$.它是一个整数.利用范保持乘法的特性和整数的因子分解性质,容易证明

引理 1. 设 $u,v,w\in Z[\varphi]$.

(i) 设 $u=v\varphi$.若$|u|<3$,则 $v\in S$.进一步地,若$|u|<1$,则 $u=v=0$.

(ii) 设 $u,v,w\in S$,则$|u+v+w|\le 3$,且$|u+v+w|=3$,当且仅当 $0\ne u=v=w\in S$.

(iii) 设 $u+v=w\varphi$且 $u,v\in S$,则 $w\in S$.

引理 2. $Z[\varphi]$的每个元素均存在惟一的非连接φ-表达式.

引理 3. 设 $\sum_{i=0}^{N}a_i\varphi^i$ 和 $\sum_{i=0}^{N}b_i\varphi^i$ 是同一个元素的两个φ-表达式,其中 $\sum_{i=0}^{N}a_i\varphi^i$ 是非连接的,则存在惟一确定的 $\varepsilon_{-1}=0,\varepsilon_0\in S,\varepsilon_1,\ldots,\varepsilon_N\in S\cup S'$,使得对任意 $0\le i\le N,b_i=a_i+\varepsilon_{i-1}-\varepsilon_i\varphi$.

证明:依次确定$\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_N$. □

定理 1. 设 $\sum_{i=0}^{N}a_i\varphi^i$ 和 $\sum_{i=0}^{N}b_i\varphi^i$ 是同一个元素的两个φ-表达式,其中前者是非连接的,后者不是非连接的,则 $\sum_{i=0}^{N}a_i\varphi^i$ 的权小于 $\sum_{i=0}^{N}b_i\varphi^i$ 的权.

证明:去掉两个φ-表达式中的低次相同项,可设 $a_0\ne b_0$.设$\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_N$,由引理 3 确定.由于 $a_0-\varepsilon_0\varphi=b_0,\varepsilon_0\ne 0$,由引理 1 中的(i),$a_0\ne 0,b_0\ne 0$.由$\varphi$-表达式的非连接性,$a_1=0$.类似地,由$\varepsilon_0-\varepsilon_1\varphi=b_1$,有 $b_1\ne 0$.按同样方式将序列 $a_0a_1\ldots a_N$ 和序列 $b_0b_1\ldots b_N$ 剖分成连续的子序列,使得 $a_0a_1\ldots a_N$ 的每个子序列恰在第 1 个位置为非零元.由于 $b_1\ne 0$,我们仅需对 $i\ge 2$,证明 $b_0b_1\ldots b_N$ 的第 i 个子序列,设为 $b_ub_{u+1}\ldots$,不为全零子序列.若 $b_u\ne 0$,即证.设 $b_u=0$,则 $a_u+\varepsilon_{u-1}-\varepsilon_u\varphi=0$,由于 $0\ne a_u\in S$ 并且$|a_u+\varepsilon_{u-1}|\le 1+\sqrt{3}$,由引理 1(i),$\varepsilon_u\in S$.于是,$b_{u+1}=\varepsilon_u-\varepsilon_{u+1}\varphi\ne 0$.证毕. □

3 模φ^n-1 约减

本节我们将证明通过对 k 进行模φ^n-1 约减,可以将第 1 节的 kP 点乘的计算速度加快一倍.

引理 4. 设 N 为 $Z[\varphi]$中元素 u 的非连接φ–表达式的长度,则 $2\log_3(2|u|)-2<N<2\log_3(2|u|)$.

引理 5. 对任意 $u,v\in Z[\varphi],v\ne 0$,存在 $q,r\in Z[\varphi]$,使得 $u=vq+r$ 且 $N(r)\le N(v)/3$.

证明:利用复平面上由 v 和 vs 张成的格的性质.

由椭圆曲线的 Hasse 定理[14],$E/GF(3^n)$的阶小于 $3^n+1+2\cdot 3^{n/2}$ 而接近 3^n+1.对于椭圆曲线的密码应用,$3^n>2^{160}$,因此 $n>90$.而 k 通常比 E 的阶小一个小常量因子,因此可粗略认为 $k\approx 3^n$.由引理 4,k 的非连接φ-表达式长约 $2n$.

令 $v=\varphi^n-1$,则$|v|\approx|\varphi^n|=3^{n/2}$.由引理 5,将 k 除以 v 所得余式 r 的模小于 $3^{(n-1)/2}$,由引理 4,r 的非连接φ-表达式的长小于 n.另一方面,对于 E 上任意一点 $P(x,y)$,

$$\Phi^n(P(x,y))=P(x^{3^n},y^{3^n})=P(x,y),$$

即$(\Phi^n-1)P=O$,所以 $kP=rP$.文献[11]显示了长为 N 的非连接φ-表达式的平均权为 $2N/5$,因此平均地说,k 和 r 的非连接φ-表达式的权分别为 $4n/5$ 和不到 $2n/5$.这样我们得到如下定理:

定理 2. 平均地说,通过将 k 模φ^n-1 约减到余式 r,并通过计算 rP 代替 kP,我们将得到一个速度提高一倍的点乘算法.该算法计算一个点乘平均需要 $2n/5$ 个点的加法.

在本节最后,我们用整数的一个带余除法给出 k 的余式 r.为使表达式简洁,下面我们设 a=1 来加以讨论,a=−1 的情形可类似地进行讨论.

由于 n 是奇数,首先计算整数 q',r',使得 $k=3^{(n+1)/2}q'+r'$,且$|r'|<3^{(n+1)/2}/2$.因为 k 小于 $3^n+1+2\cdot 3^{n/2}$,所以 $q'\le 1+3^{(n-1)/2}$.由于$-\varphi 3^{-1/2}s^{1/2}=1$,我们有

$$k=3^{(n+1)/2}q'\varphi^n 3^{-n/2}s^{n/2}(-1)^n+r'$$
$$=(\varphi^n-1)(3^{1/2}s^{n/2}q'(-1)^n)+(3^{1/2}s^{n/2}q'(-1)^n+r'),$$

其中 $3^{1/2}s^{n/2}=(3+\varphi)s^{(n-1)/2}\in Z[\varphi]$,因而商 $3^{1/2}s^{n/2}q'(-1)^n$ 和余式 $3^{1/2}s^{n/2}q'(-1)^n+r'$ 都在 $Z[\varphi]$中.余式 $3^{1/2}s^{n/2}q'(-1)^n+r'$的模$\le 3^{1/2}q'+|r'|<2\cdot 3^{n/2}$.令 r 为此余式即可.

4 结 论

为了计算本文研究的 Koblitz 椭圆曲线(基域为 $GF(3^n)$)上的点乘 kP,首先按照第 3 节的方法求出 k 模φ^n-1的余式 r,按照文献[11]的算法求出 r 的非连接φ-表达式,再由此φ-表达式按照第 1 节方法计算 rP,即得所需的 kP.该算法计算一个点乘平均需要 $2n/5$ 个点的加法,其速度是传统的重复加倍——点加算法(计算量为$(3n\log_2 3)/2$个点的加倍或加法)的大约 6 倍$(15\log_2 3/4\approx 6)$.该算法不带预计算,其快速优化原理仅利用了曲线的复乘性质,与有限域算术优化和椭圆曲线点的坐标表示的选取无关.因此,结合有限域算术的优化并选取适当的坐标表示,我们将得到非常有效的曲线上点乘算法.

References:

[1] Menezes AJ, Okamoto T, Vanstone SA. Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Transactions on Information Theory, 1993,39(5):1639~1646.

[2] Frey G, Rück HG. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. Mathematics of Computation, 1994,62(206):865~874.

[3] Joux A. A one round protocol for tripartite Diffie-Hellman. In: Bosma W, ed. Algorithmic Number Theory Symposium-ANTS-IV (2000). Berlin/Heidelberg: Springer-Verlag, 2000. 385~394.

[4] Boneh D, Franklin M. Identity-Based encryption from the Weil pairing. In: Kilian J, ed. Advance in Cryptology-CRYPTO 2001. Berlin/Heidelberg: Springer-Verlag, 2001. 213~229.

[5] Galbraith SD. Supersingular curves in cryptography. In: Boyd C, ed. Advance in Cryptology-ASIACRYPT 2001. Berlin/Heidelberg: Springer-Verlag, 2001. 495~513.

[6] Boneh D, Lynn B, Shacham H. Short signature from the Weil pairing. In: Boyd C, ed. Advance in Cryptology-ASIACRYPT 2001. Berlin/Heidelberg: Springer-Verlag, 2001. 515~532.

[7] Verheul ER. Self-Blindable credental certifications from the weil pairing. In: Boyd C, ed. Advance in Cryptology-ASIACRYPT 2001. Berlin/Heidelberg: Springer-Verlag, 2001. 533~551.

[8] Smart NP. Identity based authenticated key agreement protocol based on Weil pairing. IEE Electronic Letters, 2002,38:630~632.

[9] Koblitz N. CM-Curves with good cryptographic properties. In: Feigenbaum J, ed. Advance in Cryptology-CRYPTO 1991. Berlin/Heidelberg: Springer-Verlag, 1992. 279~287.

[10] Koblitz N. Constructing elliptic curve cryptosystems in characteristic 2. In: Menezes AJ, Vanstone SA, eds. Advance in Cryptology-CRYPTO 1990. Berlin/Heidelberg: Springer-Verlag, 1991. 156~167.

[11] Koblitz N. An elliptic curve implementation of the finite field digital signature algorithm. In: Krawczyk H, ed. Advance in Cryptology-CRYPTO 1998. Berlin/Heidelberg: Springer-Verlag, 1998. 327~337.

[12] Muller V. Fast multiplication on elliptic curves over small fields of characteristic 2. Journal of Cryptology, 1998,11(4):219~234.

[13] Solinas JA. An improved algorithm for arithmetic on a family of elliptic curves. In: Kaliski B, ed. Advance in Cryptology-CRYPTO 1997. Berlin/Heidelberg: Springer-Verlag, 1997. 357~371.

[14] Silverman JH. The Arithmetic of Elliptic Curves. New York: Springer-Verlag, 1986. 55~63; 130~132.