软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2013,24(Suppl.(2)):200−206

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

4 次复乘域上的 GLV 分解*

胡 志[1], 徐茂智[2], 张国良[2]

[1](北京大学 北京国际数学研究中心,北京 100871)

[2](北京大学 数学科学学院 数学及其应用教育部重点实验室,北京 100871)

通讯作者: 徐茂智, E-mail: mzxu@math.pku.edu.cn

摘 要: 4 维 Gallant-Lambert-Vanstone(GLV)方法可用于加速一些定义在 $\mathbb{F}_{p^2}$ 上椭圆曲线的标量乘法计算,如 Longa-Sica 型具有特殊复乘结构的 GLS 曲线以及 Guillevic-Ionica 利用 Weil 限制得到的椭圆曲线.推广了 Longa-Sica 的 4 维 GLV 分解方法,并在 4 次复乘域中给出显式且有效的 4 维分解方法,且对分解系数的界做出理论估计.结果行之有效,很好地支持了 GLV 方法以用于这些椭圆曲线上的快速标量乘法运算的实现.

关键词: 椭圆曲线;GLV 方法;标量乘法;自同态;复乘

中文引用格式: 胡志,徐茂智,张国良.4 次复乘域上的 GLV 分解.软件学报,2013,24(Suppl.(2)):200−206. http://www.jos.org.cn/1000-9825/13037.htm

英文引用格式: Hu Z, Xu MZ, Zhang GL. GLV decomposition in quartic CM fields. Ruan Jian Xue Bao/Journal of Software, 2013,24(Suppl.(2)):200−206 (in Chinese). http://www.jos.org.cn/1000-9825/13037.htm

GLV Decomposition in Quartic CM Fields

HU Zhi[1], XU Mao-Zhi[2], ZHANG Guo-Liang[2]

[1](Beijing International Center for Mathematical Research, Peking University, Beijing 100871, China)

[2](LMAM, School of Mathematical Sciences, Peking University, Beijing 100871, China)

Corresponding author: XU Mao-Zhi, E-mail: mzxu@math.pku.edu.cn

Abstract: Four dimensional Gallant-Lambert-Vanstone (GLV) method can be applied for faster scalar multiplication on some elliptic curves over $\mathbb{F}_{p^2}$, such as the Longa-Sica GLS curves with special complex multiplication (CM), and the Guillevic-Ionica's curves via Weil restriction. This study generalizes Long-Sica four dimensional GLV decomposition methods, and gives explicit and efficient decompositions in quartic CM fields for such elliptic curves as well as the bound for the decomposed coefficients. The presented results well support the GLV method for faster implementations of scalar multiplications on desired curves.

Key words: elliptic curve; GLV method; scalar multiplication; endomorphism; complex multiplication

Gallant-Lambert-Vanstone(GLV)方法[1]是一种用于加速大素数特征域 $\mathbb{F}_q$ 上椭圆曲线 E 的标量乘法计算的方法,在椭圆曲线密码系统实现中发挥了重要作用.设 $P\in E(\mathbb{F}_q)$ 是阶为大素数 r 的点,假设 $E/\mathbb{F}_q$ 有一个阶为 d 的可有效计算的自同态 ϕ 使得 $\phi(P)=[\lambda]P$, 其中, $\lambda\in\mathbb{Z}/(r)$. 设 k 是在[0,r−1]中均匀随机选取的整数,为了计算 $[k]P$,GLV 方法的基本思想是:若可分解 $k=\sum_{j=0}^{d-1}k_j\lambda^j \bmod r$,则 $[k]P=\sum_{j=0}^{d-1}[k_j]\phi^j(P)$, 于是可利用 Straus-Shamir 技巧来计算维数为 d 的多重标量乘法.如果分解的系数满足 $\max_j \log_2\left|k_j\right|\approx(\log_2|k|)/d$, 那么二倍点运算的数量将减少到约为原来的 1/$d$.一些 GLV 分解方法已在文献[1−3]中被提出.

2009 年,Galbraith,Lin 和 Scott(GLS)[4]给出了一种构造 $\mathbb{F}_{p^2}$ 上椭圆曲线 E'中有效可计算自同态的方法,这里,E'是 $\mathbb{F}_p$ 上椭圆曲线 E 在 $\mathbb{F}_{p^2}$ 上的二次扭曲线.这个快速自同态 ϕ 由 Frobenius 映射和扭映射得到,并且满足极

* 基金项目: 国家自然科学基金(61272499, 10990011); 信息保障技术重点实验室(KJ-11-02)
收稿时间: 2013-07-17; 定稿时间: 2013-10-16

小多项式 $h_1(x)=x^2+1$. 2012 年,Longa 和 Sica[5]结合复乘推广了 GLS 构造方法,同时得到另一个有效自同态 ψ,满足极小多项式 $h_2(x)=x^2+bx+c$,于是基于 $\{1,\phi,\psi,\phi\psi\}$ 的 4 维标量乘法有了可能.Longa 和 Sica 还给出了分解 $[k]P=[k_0]P+[k_1]\phi(P)+[k_2]\psi(P)+[k_3]\phi\psi(P)$ 的有效算法,并且估计出分解系数 $|k_i|<C\cdot r^{1/4}$,其中,C 为某个常数.

Freeman 和 Satoh[6],Guillevic 和 Vergnaud[7]研究将 $\mathbb{F}_p$ 上两族亏格为 2 的超椭圆曲线应用于密码学,它们对应的 Jacobians 在扩域上(2,2)同源于定义在 $\mathbb{F}_{p^2}$ 上椭圆曲线的乘积.Guillevic 和 Ionica[8]研究了同源阿贝尔簇上自同态环的关系,并利用这种关系构造出亏格为 2 的 Jacobians 与椭圆曲线上有效可计算自同态,由此引出了 Freeman 和 Satoh 的 Jacobians 与两族定义在 $\mathbb{F}_{p^2}$ 的新椭圆曲线上的 4 维 GLV 方法.

本文将 Longa-Sica 的 4 维 GLV 分解方法推广到以上定义在 $\mathbb{F}_{p^2}$ 的椭圆曲线上,并在 4 次复乘域中给出显式且有效分解方法,同时还对分解系数的界做出理论估计.已有方法在做 4 维 GLV 分解时,需要 4 个 Round 操作和 20 次乘法,而本文方法通常可以节省 8 次乘法.本文的研究结果表明,复乘通常蕴含了好的 GLV 分解性质,且实验数据也表明,利用复乘得到的分解很好地支持了 GLV 方法以用于加速椭圆曲线标量乘法计算.

本文第 1 节回顾复乘椭圆曲线的必要背景知识.第 2 节将 Longa-Sica 分解方法推广到范数-欧几里德的整环上.第 3 节给出了 $\mathbb{F}_{p^2}$ 上 Longa-Sica 曲线和 Guillevic-Ionica 曲线在 4 次复乘域中的显式分解方法.第 4 节给出若干例子和实验结果.

1 背景知识

1.1 基于复乘的自同态

设 E 为 $\mathbb{F}_q$ 上通常的椭圆曲线,其中,q 为某一大于 3 的素数的幂.记 $End(E)$是该椭圆曲线的自同态环,那么它是$\mathbb{Q}$的某虚二次扩域的序模.复乘方法[9]是一种用于构造椭圆曲线非常重要的方法.设 D 是一个负整数,$4q=t^2-Ds^2$,其中 $t,s\in\mathbb{Z}$.那么,复乘方法生成一条椭圆曲线 $E/\mathbb{F}_q$,其 Frobenius 映射 $\pi_q=(t+s\sqrt{D})/2$,$\#E(\mathbb{F}_q)=(1-\pi_q)(1-\bar{\pi}_q)$. 记 $K=End(E)\otimes\mathbb{Q}$,并且 $\mathcal{O}_K$ 是它的代数整数环,那么 $D=m^2Disc(K)$,其中,m 是某一整数,$Disc(K)$是 K 的判别式.

如果一个自同态 $\psi\in End(E)$可以在时间 $O(1)$计算,那么它被称作有效可计算.Gallant 等人利用复乘给出了一些椭圆曲线上的非常有效的自同态[1].这些自同态的具体形式可通过 Stark 算法[10]或者 Velu 公式计算得到.将 $\psi\in End(E)$视为一个复数,根据文献[11],有

$$\psi(x,y)=\left(\psi^{-2}\frac{f(x)}{g(x)},y\psi^{-3}\left(\frac{f(x)}{g(x)}\right)'\right) \tag{1.1}$$

其中 f,g 是$\mathbb{Q}$上的多项式函数,$\deg f=N_{\mathbb{Q}}^K(\psi),\deg g=N_{\mathbb{Q}}^K(\psi)-1$,通常选择 $\psi=(1+\sqrt{D})/2$ (若 $D\equiv 1 \bmod 4$)或者 $\sqrt{D}/2$ (若 $D\equiv 0 \bmod 4$),由于这样的 $\psi\in End(E)\setminus\mathbb{Z}$ 有最小的范数,因此很容易计算.

1.2 $\mathbb{F}_{p^2}$ 上椭圆曲线

Galbraith,Lin 和 Scott[4]给出了一种方法构造一大类二次扩域上的带有有效可计算自同态的椭圆曲线.记 E' 是 E 在 $\mathbb{F}_{p^2}$ 上的 $m(m=2,4,6)$次扭曲线,令 ψ_m 为 m 次扭映射,π_p 为 p 次 Frobenius 映射,那么我们得到 $E'/\mathbb{F}_{p^2}$ 上的一个有效自同态:

$$\phi: E'/\mathbb{F}_{p^2}\xrightarrow{\psi_m^{-1}}E/\mathbb{F}_{p^{2m}}\xrightarrow{\pi}E/\mathbb{F}_{p^{2m}}\xrightarrow{\psi_m}E'/\mathbb{F}_{p^2} \tag{1.2}$$

并且,ϕ有特征多项式 $h(x)=\Psi_{2m}(x)$,Ψ_{2m}为 $2m$ 次分圆多项式.于是,ϕ给出了一个 $\varphi(2m)$维 GLV 方法,其中,φ是欧拉函数.Longa 和 Sica 在文献[5]中研究了 $\mathbb{F}_{p^2}$ 上有特殊复乘 D 的 GLS 曲线(这里,$D\neq -3,-4$):

$$E'\left(\mathbb{F}_{p^2}\right): y^2=x^3+3cu^4x+2cu^6, c=\frac{j}{1728-j}, u\in\mathbb{F}_{p^2}/\mathbb{F}_p \tag{1.3}$$

类似方程(1.1),可以通过复乘计算出自同态 ψ.另一个自同态 ϕ(相当于 $i=\sqrt{-1}$)可由方程(1.2)得到.

Guillevic 和 Ionica 对判别式 $D<-2$ 的特殊复乘,构造了两类 $\mathbb{F}_{p^2}$ 上的椭圆曲线:

$$E_{1,c}\left(\mathbb{F}_{p^2}\right): y^2=(x-12)\left(x^2+12x+81\cdot c-126\right) \tag{1.4}$$

$$E_{2,c}\left(\mathbb{F}_{p^2}\right): y^2=x^3+3(2c-5)x+c^2-14c+22 \tag{1.5}$$

对于曲线 $E_{1,c}\left(\mathbb{F}_{p^2}\right)$,文献[8]给出了 ϕ 相当于 $\sqrt{\pm 2}$ 时的有效自同态,以及 ψ 相当于 $\sqrt{\pm D/2}$ 时的有效自同态.对于曲线 $E_{2,c}\left(\mathbb{F}_{p^2}\right)$,文献[8]给出了 ϕ 相当于 $\sqrt{-3}$ 时的有效自同态,以及 ψ 相当于 $\sqrt{-D/3}$ 时的有效自同态.

注意到 $\mathbb{F}_{p^2}$ 上曲线 E 在某些条件下(例如有 m 阶扭点,m=2,3),可以与 $\mathbb{F}_p$ 上亏格为 2 的超椭圆曲线 H 同源[7,8].换句话说,这些 $\mathbb{F}_{p^2}$ 上的亏格为 2 的超椭圆曲线 H 有分裂的 Jacobians.在这些情况下,m $End(Jac(H))\subseteq End(E\times E))$ 且 m $End(E\times E))\subseteq End(Jac(H))$,可将自同态 ϕ,ψ 看作是 4 次复乘域的代数数.

2 Longa-Sica 分解的推广

考虑标量乘法基于 $\Phi=\{1,\phi,\psi,\phi\psi\}$ 的 4 维分解,其中,ϕ 和 ψ 如上节中定义.设 $\phi(P)=[\lambda_1]P,\psi(P)=[\lambda_2]P$, $\lambda_i\in\mathbb{Z}/(r)$,$\phi$ 有极小多项式 $h_1(x)=x^2+b_1x+c_1$,并且 ψ 有极小多项式 $h_2(x)=x^2+b_2x+c_2$. 若标量 k 可分解为 $k\equiv k_0+k_1\lambda_1+k_2\lambda_2+k_3\lambda_1\lambda_2 \bmod r$, $k_i\in\mathbb{Z}$,则 $[k]P=[k_0]P+[k_1]\phi(P)+[k_2]\psi(P)+[k_3]\phi\psi(P)$. 设

$$f:\mathbb{Z}^4\to\mathbb{Z}/(r),\left(k_0,k_1,k_2,k_3\right)\to k_0+k_1\lambda_1+k_2\lambda_2+k_3\lambda_1\lambda_2 \bmod r,\ g_1:\mathbb{Z}[\phi,\psi]\to\mathbb{Z}^4,\ k_0+k_1\phi+k_2\psi+k_3\phi\psi$$
$$\to\left(k_0,k_1,k_2,k_3\right),\ g_2:\mathbb{Z}[\phi]\times\mathbb{Z}[\phi]\to\mathbb{Z}[\phi,\psi],(k_0+k_1\phi,k_2+k_3\phi)\to k_0+k_1\phi+(k_2+k_3\phi)\psi.$$

由于 f 是到 $\mathbb{Z}/(r)$ 的满同态映射,所以 ker f 是 $\mathbb{Z}^4$ 的指标为 r 的子格.假设 $\{v_0,v_1,v_2,v_3\}$ 是 ker f 的一组格基,那么 $\{v_j\}$ 就得到了一个分解如 $\left(k_0,k_1,k_2,k_3\right)=\left(k,0,0,0\right)-\left(\sum_{j=0}^{3}[a_j]\boldsymbol{v}_j\right)$,其中,$a_j\in\mathbb{Q}$ 且 $(k,0,0,0)=\sum_{j=0}^{3}a_j\boldsymbol{v}_j$,[·]表示取整操作.易见,分解的系数满足 $\max_j\left|k_j\right|\leqslant\left(\sum_{j=0}^{3}\|\boldsymbol{v}_j\|\right)\Big/2\leqslant 2\max_j\|\boldsymbol{v}_j\|$,其中,||·||是 $\mathbb{Q}^4$ 上的欧几里德范数.

Longa 和 Sica[5]在 Gauss 整环 $\mathbb{Z}[i]$ 中给出有效算法计算标量 k 的分解,且分解系数满足 $\left|k_i\right|<C\cdot r^{1/4}$,$C$ 为某一常数.其基本想法是,首先找到 $v=v_0+v_1i\in\mathbb{Z}[i]$ 使得 $v\overline{v}\equiv 0 \bmod r$ 并且 $v_0^2+v_1^2\leqslant r$,然后利用 v 找到 $u_j=u_{j0}+u_{j1}\psi\in\mathbb{Z}[i,\psi],u_{j0},u_{j1}\in\mathbb{Z}[i],j=0,1,2,3$, 使得 $u_j\overline{u_j}\equiv 0 \bmod r$.在第 1 步中,$v$ 可以利用$\mathbb{Z}$中 Cornacchia 算法[12]寻找,第 2 步中,u_j 可以使用 $\mathbb{Z}[i]$ 上的扩展欧几里德算法进行计算.

考虑在更一般的情况下推广 Longa-Sica 方法,记 $v=v_0+v_1\phi\in\mathbb{Z}[\phi]$, 使得 $v\overline{v}\equiv 0 \bmod r$ 并且 $v_0^2+v_1^2\leqslant r$ (同样可用 Cornacchia 算法计算).设 $f_1:\mathbb{Z}[\phi]\times\mathbb{Z}[\phi]\to\mathbb{Z}[\phi]/(v)\cong\mathbb{Z}/(r),(z_1,z_2)\to z_1+z_2\lambda_2 \bmod r$.我们希望找到非零向量 $\boldsymbol{u}\in\ker f_1$,使得 $g_1\cdot g_2(\boldsymbol{u})$尽可能地短.注意到,扩展欧几里德算法可被应用在 $\mathbb{Z}[\phi]$ 当且仅当 $\mathbb{Z}[\phi]$ 是范数-欧几里德的(环 R 上的欧几里德函数 e 满足下面这种拥有余数性质的基本除法:如果 $a,b\in R$ 并且 b 非零,那么存在 $q,s\in R$, 使得 $a=bq+s$ 并且有 $s=0$ 或者 $e(s)<e(b)$.如果 R 上的范数是一个欧几里德函数,那么 R 称为是范数-欧几里德的).这里列举一些无平方因子数 n,使得环 $\mathbb{Z}[\sqrt{n}]$ 是范数-欧几里德的[13]:−1,±2,±3,5,6,±7,±11,13,17,19,21,29,33,37,41,57,73.

注意到,对于 Longa-Sica 曲线和 Guillevic-Ionica 曲线,我们可以选择合适的 ϕ,使得 $\mathbb{Z}[\phi]$ 是范数-欧几里德的,那么 Longa-Sica 分解方法可推广为如下算法,这里,$\{v_0,v_1,v_2,v_3\}$ 构成了 ker f 的一组基.

算法 1. $\mathbb{Z}[\phi]$中的 Cornacchia 算法.

输入: $v=v_o+v_1\phi$,λ满足 $\lambda^2+b_2\lambda+c_2\equiv 0 \bmod r$.

输出:4 个线性无关向量 $\{\boldsymbol{v}_j:j=0,1,2,3\}\subset\ker f$.

1. 初始化: $r_0\leftarrow\lambda+\left(1-\frac{\lambda^2}{2r}\right)\cdot r,r_1\leftarrow v,r_2\leftarrow r,s_0\leftarrow 1,s_1\leftarrow 0,s_2\leftarrow 0,q\leftarrow 0.$

2. 主循环:当 $\|r_1\|^4\left(1+\left|b_2\right|+c_2\right)^2\geqslant r$ 时,重复如下操作:

$q \leftarrow \mathbb{Z}[\phi]$ 中最接近 r_0/r_1 的代数整数, $r_2 \leftarrow r_0 - q \cdot r_1, r_0 \leftarrow r_1, r_1 \leftarrow r_2, s_2 \leftarrow s_0 - q \cdot s_1, s_0 \leftarrow s_1, s_1 \leftarrow s_2$.

3. 返回值:计算 $\boldsymbol{u}_0 = (r_0, -s_0), \boldsymbol{u}_1 = (r_1, -s_1), \boldsymbol{u}_2 = \phi u_1, \boldsymbol{u}_3 = \phi u_2$.

返回 $\boldsymbol{v}_j = g_1 \cdot g_2(\boldsymbol{u}_j), j = 0,1,2,3$.

根据文献[5]的证明方法,类似地,有如下结论:

定理 1. 设 ϕ 有极小多项式 $h_1(x) = x^2 + c_1$, 且 $\mathbb{Z}[\phi]$ 是范数-欧几里德的, $v = v_0 + v_1\phi \in \mathbb{Z}[\phi]$, 使得 $v\bar{v} \equiv 0 \bmod r$, $v_0^2 + v_1^2 \leqslant r$, 则由算法 1 得到的格基 $\{v_0, v_1, v_2, v_3\}$ 可将 $k \in [0, r-1]$ 分解为 $(k_0, k_1, k_2, k_3) \in \mathbb{Z}^4$, $[k]P = [k_0]P + [k_1]\phi(P) + [k_2]\psi(P) + [k_3]\phi\psi(P)$, 其中, $\max_j |k_j| \leqslant (2 + 71\sqrt{1+|c_1|})\sqrt{1 + |b_2| + c_2} \cdot r^{1/4}$.

3 4 次复乘域上的显式分解

设 $End(E/\mathbb{F}_{p^2})$ 为 $E/\mathbb{F}_{p^2}$ 上的自同态环,这里将 ϕ, ψ 视为代数数,假设 $\mathbb{Q}(\phi) \cap \mathbb{Q}(\psi) = \mathbb{Q}$ 并且 $\mathbb{Z}[\pi_{p^2}] \subset \mathbb{Z}[\phi, \psi] \subset End(E/\mathbb{F}_{p^2})$. 令 $K = \mathbb{Q}(\phi, \psi)$, 对于 Longa-Sica 曲线而言, $K = \mathbb{Q}(i, \sqrt{D})$, 而对于 Guillevic-Ionica 曲线而言, $K = \mathbb{Q}(\sqrt{D_1}, \sqrt{D_2})$, 这里, $D_1 D_2 = D$. 注意到,存在一个二次子域 $K_0 \subset K$, 使得 K_0 是实的而 K 是 K_0 的虚二次域扩张,因此, K 是一个 4 次复乘域.

本节的基本想法是,利用 $\#E(\mathbb{F}_{p^2}) = hr = (1 - \pi_{p^2})(1 - \bar{\pi}_{p^2})$, 考虑在 $\mathbb{Z}[\phi, \psi]$ 中分解 $1 - \pi_{p^2}$. 在密码系统设定中,通常要求余因子 h 很小,则 $\log_2 r^{1/4} \approx \log_2 p^{1/2}$. 下面将展示如何利用复乘找到一组格基,并且格基的欧氏范数在界 $C\sqrt{p}$ 内,其中常数 $C > 0$. 下面,记 $M(d)$ 为 $\mathbb{Z}$ 上的全部 $d \times d$ 矩阵的集合, $\mathcal{O}_\infty$ 为无穷远点.

定理 2. 记 $E'/\mathbb{F}_{p^2}$ 为如方程(1.3)所定义的复乘判别式 $D < -4$ 的二次扭 GLS 椭圆曲线,其中, $D \equiv 0,1 \bmod 4$, 并且 $4p = t^2 - Ds^2$, $\pi_p = (t + s\sqrt{D})/2$. 令 ψ 与方程(1.1)中定义相同, ϕ(视为 $i = \sqrt{-1}$)与方程(1.2)中的定义相同.假设 $\psi \notin \mathbb{Q}(i)$, 并且对于任何 r 阶点 $P \in E'(\mathbb{F}_{p^2})$, 有 $[1 - i\pi_p]P = \mathcal{O}_\infty$. 考察利用 $\boldsymbol{\Phi} = (1, \phi, \psi, \phi\psi)$ 展开的 GLV 方法,令 $A_{m,n} \in M(4)$ 是满足 $\phi^m \psi^n \boldsymbol{\Phi}^T = A_{m,n} \boldsymbol{\Phi}^T$ 的矩阵, $\boldsymbol{v} \in \ker f$, 并定义 $\boldsymbol{v}_{m,n} = \boldsymbol{v} A_{m,n}, m = 0,1, n = 0,1$.

(1) 若 $D \equiv 1 \bmod 4$, 选择 ψ 为 $(1 + \sqrt{D})/2$, 且 $\boldsymbol{v} = (1, (s-t)/2, 0, -s)$. 那么, $\{\boldsymbol{v}_{m,n}\}$ 诱导出一个 4 维分解,且分解系数满足 $\max|k_j| \leqslant \left(1 + \sqrt{(5-D)/8}\right)\sqrt{2p}$;

(2) 若 $D \equiv 0 \bmod 4$, 选择 ψ 为 $\sqrt{D}/2$, 并且 $v = (1, -t/2, 0, -s)$. 那么, $\{\boldsymbol{v}_{m,n}\}$ 诱导出一个 4 维分解,且分解系数满足 $\max|k_j| \leqslant \left(1 + \sqrt{-D/4}\right)\sqrt{2p}$.

证明:由 $1 + \pi_{p^2} = (1 - i\pi_p)(1 + i\pi_p)$ 以及 $\boldsymbol{v}_{m,n} \cdot \boldsymbol{\Phi}^T = \phi^m \psi^n \boldsymbol{v} \cdot \boldsymbol{\Phi}^T = \phi^m \psi^n (1 - i\pi_p)$, 对于 $D \equiv 1 \bmod 4$ 的情况,可得到 $t \equiv s \bmod 2$, 并且,

$$
\begin{aligned}
\boldsymbol{v}_{0,0} &= (1, (s-t)/2, 0, -s),\\
\boldsymbol{v}_{1,0} &= (-(s-t)/2, 1, s, 0),\\
\boldsymbol{v}_{0,1} &= (0, (1-D)s/4, 1, -(s+t)/2),\\
\boldsymbol{v}_{1,1} &= (-(1-D)s/4, 0, (s+t)/2, 1).
\end{aligned}
$$

于是,由格基分解方法,有

$$\max|k_j| \leqslant (\sum_{i,j} \| \boldsymbol{v}_{i,j} \|)/2 \leqslant (2\sqrt{2p} + 2\sqrt{(5-D)/8}\sqrt{2p})/2 = (1 + \sqrt{(5-D)/8})\sqrt{2p}.$$

对于 $D \equiv 0 \bmod 4$ 的情况,可以得到 $t \equiv 0 \bmod 2$, 则,

$$
\begin{aligned}
\boldsymbol{v}_{0,0} &= (1, -t/2, 0, -s),\\
\boldsymbol{v}_{1,0} &= (t/2, 1, s, 0),\\
\boldsymbol{v}_{0,1} &= (0, -Ds/4, 1, -t/2),\\
\boldsymbol{v}_{1,1} &= (Ds/4, 0, t/2, 1),
\end{aligned}
$$

则由格基分解方法,有

$$\max\left|k_j\right| \leqslant (\Sigma_{i,j} \| \boldsymbol{v}_{i,j} \|)/2 \leqslant \left(2\sqrt{p} + 2\sqrt{-D/4}\sqrt{p}\right)/2 = \left(1+\sqrt{-D/4}\right)\sqrt{p}. \quad \square$$

对 D=–3,–4 的 GLS 曲线 4 维 GLV 分解,相关内容已在文献[14]中给出.

在复乘判别式 D<0 的 Guillevic-Ionica 曲线上,有 $4p^2 = t_2^2 - Ds_2^2$.对于 $E_{1,c}\left(\mathbb{F}_{p^2}\right)$,Guillevic 和 Vergnaud 在文献[7]中得到,若 $p \equiv 1 \bmod 8$, 则有 $t_2 + 2p = D's_1^2$ 且 $t_2 - 2p = -2t_1^2$; 若 $p \equiv 5 \bmod 8$, 则 $t_2 + 2p = 2s_1^2$ 且 $t_2 - 2p = -D't_1^2$, 这里, $t_1, s_1, D' \in \mathbb{Z}$, D=2D'.而对于 $E_{2,c}\left(\mathbb{F}_{p^2}\right)$ 有, $t_2 + 2p = D's_1^2$ 且 $t_2 - 2p = -3t_1^2$,其中, $t_1, s_1, D' \in \mathbb{Z}$,D=3D'.

定理 3. 令 $E_{k,c}\left(\mathbb{F}_{p^2}\right), k = 1,2$ 如方程(1.4)、方程(1.5)中所记,复乘判别式为 D.设 $4p^2 = t_2^2 - Ds_2^2$, $t_2 + 2p = D_1 t_1^2$ 以及 $t_2 - 2p = D_2 s_1^2$. $E_{k,c}\left(\mathbb{F}_{p^2}\right)$ 上存在两个有效自同态 ϕ(视为 $\sqrt{D_1}$)和 ψ(视为 $\sqrt{D_2}$),Frobenius 映射满足 $\pi_{p^2} = t_2 + s_2\sqrt{D} = (t_1\sqrt{D_1} + s_1\sqrt{D_2})^2/4$,记 $\pi_p = (t_1\sqrt{D_1} + s_1\sqrt{D_2})/2$,则 $1 - \pi_{p^2} = \left(1-\pi_p\right)\left(1+\pi_p\right)$. 假设对任意 r 阶点 $P \in E_{k,c}\left(\mathbb{F}_{p^2}\right)$ 有 $[1-\pi_p]P = \mathcal{O}_\infty$. 考虑利用 $\boldsymbol{\Phi} = (1, \phi, \psi, \phi\psi)$ 展开的 GLV 方法,记 $A_{m,n} \in M(4)$ 是满足 $\phi^m\psi^n\boldsymbol{\Phi}^T = A_{m,n}\boldsymbol{\Phi}^T$ 的矩阵, $\boldsymbol{v} = \left(2, -t_1, -s_1, 0\right)$, 定义 $\boldsymbol{v}_{m,n} = \boldsymbol{v}\, A_{m,n}, m = 0,1, n = 0,1$, 则 $\{\boldsymbol{v}_{m,n}\}$ 诱导出一个 4 维格基分解,分解系数满足 $\max\left|k_j\right| \leqslant (\sqrt{|D_1|} + \sqrt{|D_2|} + \sqrt{|D_1| + |D_2|})\sqrt{p}$.

证明:由于 $\boldsymbol{v}_{m,n} \cdot \boldsymbol{\Phi}^T = \phi^m\psi^n\boldsymbol{v} \cdot \boldsymbol{\Phi}^T = \phi^m\psi^n 2\left(1-\pi_p\right)$,且

$$\boldsymbol{v}_{0,0} = (2, -t_1, -s_1, 0),$$
$$v_{1,0} = (-t_1 D_1, 2, 0, -s_1),$$
$$\boldsymbol{v}_{0,1} = (-s_1 D_2, 0, 2, -t_1),$$
$$\boldsymbol{v}_{1,1} = (0, -s_1 D_2, -t_1 D_1, 2).$$

于是根据格基分解方法,可得

$$\max\left|k_j\right| \leqslant (\Sigma_{i,j} \| \boldsymbol{v}_{i,j} \|)/2 \leqslant (\sqrt{|D_1|} + \sqrt{|D_2|} + \sqrt{|D_1| + |D_2|})\sqrt{p}. \quad \square$$

注意到,若 $t_1 \equiv s_1 \equiv 0 \bmod 2$, 则可定义 $\boldsymbol{v}$ 如 $v = (1, -t_1/2, -s_1/2, 0)$.

4 示例及数据实验

4.1 曲线示例

LS 曲线-128:设素数

$$p = 2^{128} - 124217,$$
$$4p = t^2 + 11s^2,$$
$$t = 36817731368501993475,$$
$$s = 712493991080127739.$$

设 $\mathbb{F}_{p^2} = \mathbb{F}_p[z]/(z^2+1), u = z+5$, 则曲线 $E'/\mathbb{F}_{p^2} : y^2 = x^3 - 13824u^2x/539 - 27648u^3/539$ 的阶 $\#E'(\mathbb{F}_{p^2}) = r$, 其中,$r$ 是 256 比特素数.与第 1 节相同,在 $E'/\mathbb{F}_{p^2}$ 上定义 ϕ(视为 i)和 ψ(视为 $(1+\sqrt{-11})/2$).若对任意 r 阶点 $P \in E'(\mathbb{F}_{p^2})$, 有 $[1-\phi((s-t)/2 + s\psi)]P = \mathcal{O}_\infty$, 则由定理 2 可定义 $\boldsymbol{v} = (1, (s-t)/2, 0, -s)$. 而由算法 1 可得格基 $\{\boldsymbol{v}'_j\} \subset \ker f$.有趣的是,实验结果显示,两种方法均得到了同一组格基.

GI 曲线-128:设素数

$$p = 204922038868557842644133314527162339757 \equiv 5 \bmod 8,$$
$$4p = 2t_1^2 + 5s_1^2,$$

其中,

$$t_1 = 6184074368627374052,$$
$$s_1 = 12191821880923320482.$$

设 $z = 860166582905057611098831196780681426 18$, 取 $c = \sqrt{z} \in \mathbb{F}_{p^2}$, 那么,文献[8]给出了椭圆曲线 $E_{1,c}\left(\mathbb{F}_{p^2}\right)$,

群阶 $\#E_{1,c}\left(\mathbb{F}_{p^2}\right)=4r$,其中,$r$ 为 253 比特素数.与第 1 节相同,定义 $\phi(=\sqrt{2})$ 和 $\psi(=\sqrt{-5})$, 对于任意 r 阶点 $P\in E_{1,c}\left(\mathbb{F}_{p^2}\right)$,有 $[1-(t_1\phi+s_1\psi)/2]P=\mathcal{O}_\infty$.根据定理 3,可定义 $\boldsymbol{v}=(1,-t_1/2,-s_1/2,0)$.而由算法 1,可得到另一组格基 $\{\boldsymbol{v}'_j\}\subset\ker f$.

4.2 实验结果

实验统计了每种 GLV 方案中 10 000 000 次标量分解的情况.表 1 所示为分解所得最大的标量长度出现的频率百分比.在第 3.1 节所示两类曲线的 4 维 GLV 分解中,表 1 表示出显式分解与(推广)Longa-Sica 方法在分解系数 $\max_j\left|k_j\right|$ 比特长度基本相同.对于 GI 曲线-128,Longa-Sica 分解方法(使用 $\{\boldsymbol{v}'_j\}$)表现得稍好,显式分解方法(使用 $\boldsymbol{v}$)在分解速度方面更占优,因为 $\boldsymbol{v}_{m,n}$ 有一个分量为 1,一个分量为 0,从而可节省 8 次乘法.

假设群阶的余因子满足 $\log_2 h<4w$, 并且域特征 $p=2^n-c$ 是比特长度为 n=64m,64m−1 的拟梅森素数($m\in\mathbb{Z}$),若对 k_j 使用宽度为 w 的非相邻形式表示(NAF)[15],那么两种方法(Longa-Sica 分解和复乘显式分解)一般得到相同的标量乘法循环长度.进一步地,若使用了预计算方案[16], $\max_j\left|k_j\right|$ 的频率对 $[k]P$ 的计算时间代价影响很小.因此,在上述参数设定的情形下,建议利用复乘显式分解的 GLV 方法来加速标量乘法计算.

表 1 四维 GLV 分解

曲线-格基向量	r	$\max_j\left\|k_j\right\|$ 比特/频率(%)		
LS 曲线-128-$\boldsymbol{v}$	256	64/7.77022 61/0.36410	63/85.98472 60/0.02372	62/5.85589 ≤59/0.00135
GI 曲线-128-$\boldsymbol{v}$	253	64/63.37428 61/1.01352	63/27.46788 60/0.06389	62/8.07617 ≤59/0.00426
GI 曲线-128-$\{\boldsymbol{v}'_j\}$	253	64/10.30556 61/2.49516	63/67.54093 60/0.24809	62/19.39339 ≤59/0.01687

References:

[1] Gallant RP, Lambert RJ, Vanstone SA. Faster point multiplication on elliptic curves with efficient endomorphisms. In: Kilian J, ed. Proc. of the CRYPTO 2001. Heidelberg: Springer-Verlag, LNCS 2139, 2001. 190−200.

[2] Park YH, Jeong S, Kim CH, Lim J. An alternate decomposition of an integer for faster point multiplication on certain elliptic curves. In: Naccache D, Paillier P, eds. Proc. of the PKC 2002. LNCS 2274, Heidelberg: Springer-Verlag, 2002. 323−334.

[3] Sica F, Ciet M, Quisquater JJ. Analysis of Gallant-Lambert-Vanstone method based on efficient endomophisms: Elliptic and hyperelliptic curves. In: Nyberg K, Heys HM, eds. Proc. of the SAC 2002. LNCS 2595, Heidelberg: Springe-Verlagr, 2003. 21−36.

[4] Galbraith SD, Lin XB, Scott M. Endomorphisms for faster elliptic curve cryptography on a large class of curves. In: Joux A, ed. Proc. of the EUROCRYPT 2009. LNCS 5479, Heidelberg: Springer-Verlag, 2009. 518−535.

[5] Longa P, Sica F. Four-Dimensional Gallant-Lambert-Vanstone scalar multiplication. In: Wang X, Sako K, eds. Proc. of the ASIACRYPT 2012. LNCS 7658, Heidelberg: Springer-Verlag, 2012. 718−739.

[6] Freeman D, Satoh T. Constructing pairing-friendly hyperelliptic curves using Weil restriction. J. Number Theory, 2011,131(5): 959−983.

[7] Guillevic A, Vergnaud D. Genus 2 hyperelliptic curve families with explicit Jacobian order evaluation and pairing-friendly constructions. In: Abdalla M, Lange T, eds. Proc. of the Pairing 2012. LNCS 7708, Heidelberg: Springer-Verlag, 2012. 234−253.

[8] Guillevic A, Ionica S. Four dimensional GLV via the Weil restriction. Cryptology ePrint Archive, Report, 2013/311.

[9] Atkin AOL, Morain F. Elliptic curves and primality proving. Math. Comput., 1993,61:29−68.

[10] Stark HM. Class numbers of complex quadratic fields. In: Kuyk W, ed. In: Modular Functions of One Variable I. New York: Springer-Verlag, Lecture Notes in Math., Vol.320, 1973. 153−174.

[11] Cox D. Primes of the Form x^2+ny^2. New York: Wiley, 1989.

[12] Cohen H. A Course in Computational Algebraic Number Theory. Berlin: Springer-Verlag, 1996.

[13] The On-Line Encyclopedia of Integer Sequences, A048981. http://oeis.org/A048981/internal

[14] Hu Z, Longa P, Xu MZ. Implementing the 4-dimensional GLV method on GLS elliptic curves with j-invariant 0. Des. Codes Cryptogr., 2012,63(3):331−343.

[15] Hankerson D, Menezes AJ, Vanstone S. Guide to Elliptic Curve Cryptography. Heidelberg: Springer-Verlag, 2004.

[16] Longa P, Miri A. Newcomposite operations and precomputation scheme for elliptic curve cryptosystems over prime fields. In: Cramer R, ed. Proc. of the PKC 2008. LNCS 4939, Heidelberg: Springer-Verlag, 2008. 229–247.

胡志(1985－),男,湖南湘潭人,博士,主要研究领域为密码学,信息安全理论.
E-mail: huzhi@math.pku.edu.cn

徐茂智(1962－),男,博士,教授,主要研究领域为代数学,密码学.
E-mail: mzxu@pku.edu.cn

张国良(1988－),男,博士生,主要研究领域为密码学,信息安全理论.
E-mail: guoliang_tj@126.com