Jacobi Quartic曲线上GLV/GLS标量乘算法

翁 江[1,2],姬伟峰[1],吴 玄[1],李映岐[1],张林锋[3],孟 浩[3]
(1. 西安电子科技大学网络与信息安全学院,陕西西安 710071;2. 空军工程大学信息与导航学院,陕西西安 710077;
3. 北京市海淀区复兴路14号院10分队,北京 100089)

摘 要: 目前GLV/GLS (Gallant, Lambert, Vanstone / Galbraith, Lin, Scott)标量乘算法的研究主要集中在Weierstrass曲线上,尝试寻找和构造更多或者更高次数的可有效计算的自同态.本文主要研究了Jacobi Quartic曲线上GLV/GLS标量乘算法.首先利用曲线之间的双有理等价,给出了该类曲线在素域上可有效计算自同态的具体构造,得到2维GLV方法.然后考虑椭圆曲线的二次扭曲线,利用曲线之间双有理等价和Frobenius映射,给出了该类曲线在二次扩域上可有效计算自同态的具体构造,得到2维GLS方法.将上述GLV和GLS方法结合起来,同时利用曲线在二次扩域上的两个不同的自同态,得到4维GLV方法.最后针对j不变量为0或1728两类特殊形式的椭圆曲线,利用更高次的扭曲线,得到4维GLV方法.实验结果表明:对于Jacobi Quartic曲线,2维GLV方法和4维GLV方法比5-NAF方法分别提速37.2%和109.4%以上.同时,在三种不同的实现方式下,Jacobi Quartic曲线上标量乘效率都优于Weierstrass曲线.

关键词: 椭圆曲线; Jacobi Quartic曲线; 标量乘; GLV方法; GLS方法; 可有效计算的自同态
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112(2021)09-1783-07
电子学报URL: http://www.ejournal.org.cn DOI: 10.12263/DZXB.20191005

GLV/GLS Scalar Multiplication on Jacobi Quartic Curves

WENG Jiang[1,2], JI Wei-feng[1], WU Xuan[1], LI Ying-qi[1], ZHANG Lin-feng[3], MENG Hao[3]
(1. *School of Network and Information Security, Xidian University, Xi'an, Shaanxi* 710071, *China*;
2. *Information and Navigation College, Air Force Engineering University, Xi'an, Shaanxi* 710077, *China*;
3. *Unit* 10, *Courtyard* 14, *Fuxing Road, Beijing* 100089, *China*)

Abstract: At present, GLV/GLS scalar multiplication mainly focuses on the Weierstrass curves, attempting to find and construct more and more efficient computable endomorphism. In this paper, we study the applications of GLV/GLS method on Jacobi Quartic curve. Firstly, we present the concrete construction of efficiently computable endomorphism for this type of curves over prime field by exploiting birational equivalence between curves, and obtain 2-dimensional GLV method. Secondly, we consider the quadratic twists of elliptic curves. By using birational equivalence and Frobenius mapping between curves, we present methods to construct efficiently computable endomorphisms of this type of curves over the quadratic extension field, and obtain a 2-dimensional GLS method. Finally, we obtain the 4-dimensional GLV method on elliptic curves with j-invariant 0 or 1728 by using higher degree twists. The experimental results show that the speedups of 2-dimensional GLV method and 4-dimensional GLV method than 5-NAF method exceed 37.2% and 109.4% for Jacobi Quartic curves respectively. At the same time, under the three implementations above, the scalar multiplication on the Jacobi Quartic curves is always more efficient than that on the Weierstrass curves.

Key words: elliptic curve; Jacobi Quartic curve; scalar multiplication; GLV method; GLS method; efficiently computable endomorphism

1 引言

在过去的三十年里,椭圆曲线公钥密码(Elliptic Curve Cryptography, ECC)受到了广泛的关注.椭圆曲线密码体制以计算速度快、存储空间少、通信带宽要求低、计算参数少等特点、更适合在计算能力和存储空间受限的系统(如智能卡和无线设备)中使用.特别是随

收稿日期:2019-09-03;修回日期:2021-01-24;责任编辑:梅志强
基金项目:国家自然科学基金(No.61902426);中国博士后科学基金第69批面上项目(No.2021M692502)

着物联网、无线传感器网络的普及应用,对椭圆曲线密码算法的效率提出了更高的要求.作为椭圆曲线密码算法中最核心、最耗时的运算,标量乘运算的计算速度决定着椭圆曲线密码方案的实现效率.

目前,利用可有效计算的自同态加速标量乘运算是椭圆曲线密码一个研究热点.2001年,Gallant等人[1]出了GLV方法来加速定义在大素数域上的椭圆曲线的标量乘运算.设$E(F_p)$为定义在有限域F_p上的椭圆曲线,点$P\in E(F_p)$的阶为大素数n.如果椭圆曲线E具有可有效计算的自同态ϕ使得$\phi(P)\in\langle P\rangle$,则可以将标量乘$kP$(其中$1\leqslant k\leqslant n$)分解成两个标量乘$k_1P+k_2\phi(P)$,其中$|k_1|,|k_2|\approx\sqrt{n}$,从而可以利用同时多标量乘的Straus-Shamir技巧将倍点运算数量减少一半.假设ϕ的特征多项式为X^2+rX+s,则存在$\lambda\in[0,n-1]$使得$\phi(P)=\lambda P$,其中λ为$X^2+rX+s \bmod n$的一个根.整数k_1和k_2可以通过在$L=\{(x,y)\in Z^2: x+y\lambda\equiv 0 \bmod n\}$中求解最近向量问题得到.文献[2,3]对如何有效地对标量k进行2维GLV分解进行了研究,并给出了分解系数k_1和k_2的上界.

GLV方法加速标量乘计算的关键在于椭圆曲线具有可有效计算的自同态,改进GLV方法主要有两个方向:(1)寻找更多的可有效计算的自同态,扩展GLV方法适用的范围;(2)将GLV方法推广到更高的维数,进一步地减少倍点运算的数量.目前,只有在几类常见的曲线上给出了可有效计算自同态的结果[1],并且寻找这种自同态并不容易.2009年,Galbraith等人[4]利用Frobenius自同态给出了一种构造椭圆曲线$E(F_{p^2})$上有效可计算自同态的方法,这里$E(F_{p^2})$为定义在F_{p^2}上椭圆曲线的二次扭曲线(称为GLS曲线).他们将这一构造结果与GLV方法结合在一起,从而将GLV方法推广到定义在F_{p^2}上一大类椭圆曲线上(称为GLS方法).

2010年,Zhou等人[5]针对一类特殊的GLS曲线利用LLL算法得到了3维GLV方法的一组基,并且得到很好的加速结果.2012年,Hu等人[6]针对j不变量为0的GLS曲线实现了4维GLV方法,实现结果表明在同一曲线上4维GLV方法比2维GLV方法效率提高了大约22%.同年,Longa和Sica[7]将GLS方法推广到所有的GLV曲线,利用F_{p^2}上的两个自同态Φ和Ψ对任意的标量$k\in[1,n]$得到一个4维GLV分解

$$kP=k_1P+k_2\Phi(P)+k_3\Psi(P)+k_4\Phi\Psi(P).$$

他们还利用整数环$\mathbb{Z}$和高斯整环$\mathbb{Z}[i]$上的扩展欧几里德算法给出了4维GLV分解的有效算法.

近年来,关于亏格为2的超椭圆曲线也有大量的研究工作.通常亏格为2曲线的Jacobian群具有比椭圆曲线更大的自同态环,所以在素域或者扩张次数相同的扩域上亏格为2曲线的GLV分解的维数是椭圆曲线的二倍.2013年,Bos等人[8]提出利用4维GLV方法来加速定义在素域F_p上亏格为2超椭圆曲线上的标量乘运算,他们考虑了Buhler-Koblitz(BK)曲线$y^2=x^5+b$[9]和Furukawa-Kawazoe-Takahashi(FKT)曲线$y^2=x^5+ax$[10].同年,Guillevic和Ionica[11]利用同源阿贝尔簇上的自同态环的关系构造出亏格为2曲线的Jacobian群与椭圆曲线上的可有效计算的自同态,从而得到两类定义在F_{p^2}上的椭圆曲线与定义在F_p上亏格为2曲线的Jacobian群上的4维GLV方法.Bos等人[12]考虑二次扩域F_{p^2}上亏格为2的超椭圆曲线,第一次研究和实现了8维的标量分解.近年来,国内学者于伟[13,14]、游林[15]等人针对特定的曲线加速了标量乘的运算效率.

近年来,不同形式的椭圆曲线被提出并受到学者们的广泛关注,如Montgomery曲线、Jacobi Quartic曲线、Edwards曲线等.这些曲线具有更强的抵抗侧信道攻击能力和更快的倍点运算公式,已经被考虑作为下一代椭圆曲线标准的候选方案.目前GLV/GLS方法的研究主要集中在Weierstrass曲线上,尝试寻找和构造更多或者更高次数的可有效计算的自同态,而在其他曲线形式上的研究还比较少.本文研究了GLV/GLS方法在Jacobi Quartic曲线上的应用及其效率评估.利用曲线之间的双有理等价、Frobenius映射、扭同构等,给出了上述两类曲线上可有效计算自同态的具体构造,并给出了一些曲线上可有效计算自同态的实例.将目前Weierstrass曲线上GLV/GLS主要研究结果推广到Jacobi Quartic曲线上,相应地得到2维和4维GLV方法,并通过实验对这类曲线上GLV标量乘算法进行评估,实验结果表明:对于Jacobi Quartic曲线,2维GLV方法和4维GLV方法比5-NAF方法分别提速37.2%和109.4%以上.并且在三种不同的实现方式下,Jacobi Quartic曲线上标量乘效率都优于Weierstrass曲线.

2 基础知识

本节主要介绍与本文相关的基础知识,主要包括椭圆曲线的定义和同源映射的性质,更多详细内容可以参考文献[16~18].设有限域F_q的特征为p,$E: y^2=x^3+Ax+B$为定义在F_q上的椭圆曲线,称为Weierstrass曲线.其中存在两类特殊的椭圆曲线:$E_B: y^2=x^3+B$和$E_A: y^2=x^3+Ax$,其j不变量分别为0和1728.

2.1 同源映射

定义1[16] 设E_1和E_2为定义在域K上的椭圆曲线.若态射$\phi: E_1\rightarrow E_2$满足$\phi(\mathcal{O})=\mathcal{O}$,则称为$E_1$到$E_2$的同

源映射. 若E_1到E_2的同源映射满足$\phi(E_1)\neq\{\mathcal{O}\}$,则称$E_1$和$E_2$是同源的.

设$\mathrm{Hom}(E_1,E_2)$表示由E_1到E_2的所有同源映射构成的集合,则$\mathrm{Hom}(E_1,E_2)$形成一个群. 设$E_1=E_2=E$,则$\mathrm{Hom}(E,E)$是一个环,称为曲线E的自同态环(endomorphism ring),记作$\mathrm{End}(E)$. 对于任意$\phi,\varphi\in\mathrm{Hom}(E,E)$且点$P\in E$,则有$(\phi+\varphi)(P)=\phi(P)+\varphi(P)$,$(\phi\circ\varphi)(P)=\phi(\varphi(P))$. 自同态环$\mathrm{End}(E)$中所有可逆元构成曲线$E$的自同构群(automorphism group),记作$\mathrm{Aut}(E)$. 椭圆曲线E的自同态环是曲线E重要的不变量.

定理1[16]　设$\phi:E_1\to E_2$为同源映射,则有

(1) 设$m=\deg\phi$,则$\hat{\phi}\circ\phi=[m]$,在E_1上;$\phi\circ\hat{\phi}=[m]$,在E_2上.

(2) 设$\psi:E_2\to E_3$为一个同源映射,则$\widehat{\psi\circ\phi}=\hat{\phi}\circ\hat{\psi}$.

(3) 设$\varphi:E_1\to E_2$为另外一个同源映射,则$\widehat{\phi+\varphi}=\hat{\phi}+\hat{\varphi}$.

(4) 对于任意$m\in\mathbb{Z}$,有$\widehat{[m]}=[m]$且$\deg[m]=m^2$.

设E为定义在有限域F_q上的椭圆曲线,则对于任意定义在F_q上的椭圆曲线都有Frobenius自同态τ满足$\tau(x,y)=(x^q,y^q)$.

由Hasse定理可知,设$t=q+1-\#E(F_q)$,则Frobenius自同态τ满足特征方程$\tau^2-t\tau+q=0$且$|t|\leqslant 2\sqrt{q}$,其中t称为Frobenius自同态的迹(trace). 自同态τ还可以利用特征多项式的根来表示$\tau=\dfrac{t\pm\sqrt{t^2-4q}}{2}$.

2.2　Jacobi Quartic曲线

定义2　设域F_q的特征为奇素数,定义在域F_q上的Jacobi Quartic曲线方程[19]为

$$E_{J,d,a}:y^2=dx^4+2ax^2+1,$$

其中$a,d\in F_q$且$256(a^2-d)^2\neq 0$. Jacobi Quartic曲线上点加和倍点运算具有统一公式

$$(x_1,y_1)+(x_2,y_2)=\left(\frac{x_1y_2+y_1x_2}{1-dx_1^2x_2^2},\frac{(y_1y_2+2ax_1x_2)+2dx_1x_2(x_1^2+x_2^2)}{(1-dx_1^2x_2^2)^2}\right)$$

点$(0,1)$为单位元,点$(0,-1)$为二阶元,点(x,y)的负元为$(-x,y)$. 这种曲线具有更快的点运算公式,并且能够抵抗侧信道攻击. 该类曲线使用统一的点加和倍点公式,使得攻击者无法恢复出标量k的信息.

定义在域F_q上的Jacobi Quartic曲线$E_{J,d,a}:y^2=dx^4+2ax^2+1$双有理等价于Weierstrass曲线$E:v^2=u(u^2-4au+4a^2-4d)$,双有理映射为:

$$\varphi:E_{J,d,a}\to E,(x,y)\mapsto(u,v)=\left(\frac{2dx^2+2a(1+y)}{y-1},x\frac{4a(dx^2+2a)-4d(1-y)}{(1-y)^2}\right)$$

$$\psi:E\to E_{J,d,a},(u,v)\mapsto(x,y)=\left(\frac{2v}{(u-2a)^2-4d},\frac{u^2-4(a^2-d)}{(u-2a)^2-4d}\right)$$

2.3　GLS方法

本节简要介绍了GLS构造方法,详细内容可以参考文献[4].

定理2[17]　设E是定义在有限域F_q上的椭圆曲线,$\#E(F_q)=q+1-t$,设$\phi:E\to E'$是定义在F_{q^k}上的d次可分同源映射,其中E'为定义在F_{q^m}上的椭圆曲线且$m|k$. 令$r|\#E'(F_{q^m})$是一个素数使得$r>d$且$r\|\#E'(F_{q^k})$. 设π为E上的q-次Frobenuius映射,设$\hat{\phi}:E'\to E$为ϕ的对偶同源. 定义$\psi=\phi\pi\hat{\phi}$,则:

(1) $\psi\in End_{q^k}(E')$;

(2) 对于任意$P\in E'(F_{q^k})$,有$\psi^k(P)-[d^k]P=\mathcal{O}$和$\psi^2(P)-[dt]\psi(P)+[d^2q]P=\mathcal{O}$;

(3) 存在$\lambda\in Z$使得$\lambda^k-d^k\equiv 0\bmod r$,$\lambda^2-dt\lambda-d^2q\equiv 0\bmod r$,满足对于任意$P\in E'(F_{q^m})[r]$,$\psi(P)=[\lambda]P$.

推论1[17]　设$p>3$是一个素数,设E是定义在有限域F_p上的椭圆曲线,$\#E(F_p)=p+1-t$. 设E'为F_{p^2}上$E(F_{p^2})$的二次扭(quadratic twist)曲线,则$\#E'(F_{p^2})=(p-1)^2+t^2$. 设$\phi:E\to E'$为定义在$F_{p^4}$上的扭同构(twisting isomorphism). 设$r|\#E'(F_{p^2})$为素数且$r>2p$. 令$\psi=\phi\pi\phi^{-1}$,则

(1) 对任意的$P\in E'(F_{p^2})[r]$,$\psi^2(P)+P=\mathcal{O}$;

(2) $\psi(P)=[\lambda]P$,其中$\lambda=t^{-1}(p-1)\bmod r$.

推论2[17]　设$p>3$是一个素数,E是定义在有限域F_q上的椭圆曲线. 设E'为F_{p^2}上$E(F_{p^m})$的二次扭曲线,$\phi:E\to E'$为定义在$F_{p^{2m}}$上的扭同构. 设$r|\#E'(F_{p^m})$为素数且$r>2p^{m-1}$. 令$\psi=\phi\pi\phi^{-1}$. 则对任意的$P\in E'(F_{p^m})[r]$,$\psi^m(P)+P=\mathcal{O}$.

设$p\equiv 1\bmod 6$和$B\in F_p$,定义$E:y^2=x^3+B$. 选择$u\in F_{p^{12}}$使得$u^6\in F_{p^2}$,定义F_{p^2}上曲线$E':y^2=x^3+u^6B$. 重复地选取p,B,u直到$\#E'(F_{p^2})$为素数(或近似素数). 同构$\phi:E\to E'$定义在$F_{p^{12}}$上为$\phi(x,y)=(u^2,u^3y)$,同态$\psi=\phi\pi\phi^{-1}$,其中π为曲线E上的p-次Frobenuius映射,是定义在F_{p^2}上的. ψ满足特征方程:$\psi^4-\psi^2+1=0$,从而就得到了一个4维GLV.

3 GLV/GLS 方法 Jacobi Quartic 曲线上的应用

3.1 Jacobi Quartic 曲线上 GLV 方法

本节考虑 Jacobi Quartic 曲线上的 GLV 方法，给出该类曲线上可有效计算自同态具体的构造. 设素数 $p>3$，设 $E: y^2=x^3+Ax+B$ 为定义在有限域 F_p 上的椭圆曲线. 由文献[19]可知，椭圆曲线 E 与一个 Jacobi Quartic 曲线 E_J 双有理等价的充要条件是椭圆曲线 E 上存在阶为 2 的点.

定理 3 设素数 $p>3$，$E: y^2=x^3+Ax+B$ 为定义在域 F_p 上的椭圆曲线. 设 $n|\#E(F_p)$ 为素数，曲线 E 具有可有效计算的自同态 ψ，使得对任意点 $P\in E(F_p)[n]$，存在 $\lambda\in\mathbb{Z}$ 使得 $\psi(P)=\lambda P$. 若曲线 E 上存在阶为 2 的点，则存在 Jacobi Quartic 曲线 E_J 和相应的可有效计算的自同态 ψ_J 使得对任意的 $P\in E_J(F_p)[n]$，都有 $\psi_J(P)=\lambda P$.

证明 由于椭圆曲线 E 上存在阶为 2 的点 R_1，设 $R_1=(r_1,0)$. 参考文献[19]中的方法，令 $d=-(3r_1^2+4A)/16$，$a=3r_1/4$，定义曲线 $E_J: Y^2=dX^4+2aX^2+1$，则 E 与 E_J 在域 F_p 上双有理等价，双有理映射为

$$\varphi: E\to E_J,(x,y)\mapsto(X,Y)=\left(\frac{2(x-r_1)}{y},\frac{(2x+r_1)(x-r_1)^2-y^2}{y^2}\right),$$

$$\varphi^{-1}: E_J\to E,(X,Y)\mapsto(x,y)=\left(\frac{2(Y+1)}{X^2}-\frac{r_1}{2},\frac{4(Y+1)-3r_1X^2}{X^3}\right)$$

故可以得到 E_J 上的自同态 $\psi_J=\varphi\psi\varphi^{-1}$.

设点 $P\in E(F_p)$ 的阶为素数 n，ψ 的特征多项式为 X^2+rX+s，则存在 $\lambda\in[0,n-1]$ 使得 $\phi(P)=\lambda P$，其中 λ 为 $X^2+rX+s \bmod n$ 的一个根. 由于 $\psi^2+r\psi+s=0$，则

$$\psi_J^2+r\psi_J+s=\varphi\psi^2\varphi^{-1}+r\varphi\psi\varphi^{-1}+s=\varphi(-r\psi-s)\varphi^{-1}+r\varphi\psi\varphi^{-1}+s=0$$

即 ψ_J 与 ψ 具有相同的特征多项式 X^2+rX+s.

故对任意的 $P\in E_J(F_p)[n]$，都有 $\psi_J(P)=\lambda P$. #

定理 4 将 Weierstrass 曲线上的自同态扩展到 Jacobi Quartic 曲线上，从而可以得到一个 Jacobi Quartic 曲线上的 2 维 GLV 标量乘算法.

例 1 设 $p\equiv 1 \bmod 4$ 是一个素数，考虑定义在有限域 F_p 上的椭圆曲线 $E_1: y^2=x^3+ax$.

设 $\alpha\in F_p$ 是一个 4 阶元，则映射 $\psi(x,y)\mapsto(-x,\alpha y)$ 是一个定义在 F_p 上的自同态，且满足 $\psi^2+1=0$. 曲线 E_1 上存在阶为 2 的点 $R_1=(0,0)$，根据定理 3 证明可知：存在 Jacobi Quartic 曲线 $E_J: Y^2=-\frac{a}{4}X^4+1$ 与曲线 E_1 双有理等价，双有理映射为

$$\varphi: E_1\to E_J,(x,y)\mapsto(X,Y)=\left(\frac{2x}{y},\frac{2x^3}{y^2}-1\right),$$

$$\varphi^{-1}: E_J\to E_1,(X,Y)\mapsto(x,y)=\left(\frac{2(Y+1)}{X^2},\frac{4(Y+1)}{X^3}\right),$$

曲线 E_J 上可有效计算的自同态 ψ_J 为

$$\psi_J(X,Y)=\left(-\frac{X}{\alpha},Y\right),$$

可以验证 $\psi_J^2+1=0$.

3.2 Jacobi Quartic 曲线上 GLS 方法

下面将 GLS 方法[4]推广到 Jacobi Quartic 曲线上，得到如下定理 5.

定理 5 设素数 $p>3$，$E: y^2=x^3+Ax+B$ 为定义在域 F_p 上的椭圆曲线且 $\#E_{a,d}(F_p)=p+1-t$. 设 E' 为 $E(F_{p^2})$ 的二次扭曲线，则 $\#E'(F_{p^2})=(p-1)^2+t^2$. 若 $2|\#E'(F_{p^2})$，$r|\#E'(F_{p^2})$ 是一个素数且满足 $r>2p$，则存在定义在 F_{p^2} 上的 Jacobi Quartic 曲线 E_J 及曲线上可有效计算的自同态 ψ_J，使得对任意的 $P\in E_J(F_{p^2})[r]$，都有 $\psi_J^2(P)+P=\mathcal{O}_{E_J}$.

证明 由 2.3 节推论 1 可知：设 u 为 F_{p^2} 中非二次剩余，曲线 E 的二次扭曲线为 $E': y^2=x^3+Au^2x+Bu^3$，且 $\#E'(F_{p^2})=(p-1)^2+t^2$. 设 π 为曲线 E 上的 p-次 Frobenuius 映射，则 $\psi=\phi\pi\phi^{-1}$ 为曲线 E' 的自同态，其中 $\phi: E\to E'$ 为定义在有限域 F_{p^4} 上的扭同构. 对于任意 $P\in E'(F_{p^2})[r]$，都有 $\psi^2(P)+P=\mathcal{O}_{E'}$.

由于 $2|\#E'(F_{p^2})$，设曲线 $E'(F_{p^2})$ 上存在阶为 2 的点 $R_1=(r_1,0)$. 令 $d=-(3r_1^2+4Au^2)/16$，$a=3r_1/4$，定义曲线 $E_J: Y^2=dX^4+2aX^2+1$，则 E 与 E_J 在域 F_{p^2} 上双有理等价，双有理映射为

$$\varphi: E\to E_J,(x,y)\mapsto(X,Y)=\left(\frac{2(x-r_1)}{y},\frac{(2x+r_1)(x-r_1)^2-y^2}{y^2}\right),$$

$$\varphi^{-1}: E_J\to E,(X,Y)\mapsto(x,y)=\left(\frac{2(Y+1)}{X^2}-\frac{r_1}{2},\frac{4(Y+1)-3r_1X^2}{X^3}\right)$$

故可以得到 $E_J(F_{p^2})$ 上的自同态 $\psi_J=\varphi\psi\varphi^{-1}$.

由于 $\psi^2+1=0$，则

$$\psi_J^2+1=\varphi\psi^2\varphi^{-1}+1=-\varphi\varphi^{-1}+1=0$$

故对任意的 $P\in E_J(F_{p^2})[r]$，都有 $\psi_J^2(P)+P=\mathcal{O}_{E_J}$.

定理 5 的结果可以应用于任意定义在有限域 F_p

($p>3$)上Jacobi Quartic曲线,从而得到一个2维GLV标量乘算法.

3.3 Jacobi Quartic曲线上4维GLV方法

为了得到Jacobi Quartic曲线上的更高维GLV方法,主要有两种方法:(1)借鉴文献[7]的思想,将GLV与GLS方法结合起来,同时利用$E(F_{p^2})$上的两个不同的自同态.(2)借鉴文献[4,6]的思想,考虑具有更大自同构群的曲线,如j不变量为0或1728.

下面针对j不变量为1728的椭圆曲线给出具体的4维GLV方法构造. 设素数$p\equiv 1 \bmod 4$,曲线$E: y^2=x^3+Ax$为定义在F_p上的椭圆曲线. 根据2.3节推论1,选择$u\in F_{p^8}$使得$u^4\in F_{p^2}$,定义F_{p^2}上曲线$E_1: y^2=x^3+u^4Ax$. 重复地选取p,u,A直到$\#E_1(F_{p^2})=2r$,其中r为素数. 同构$\phi_1: E\to E_1$定义在F_{p^8}上为$\phi_1(x,y)=(u^2x,u^3y)$. 设π为曲线E上的p-次Frobenuius映射,则自同态

$$\psi(x,y)=\phi_1\pi\phi_1^{-1}(x,y)=((u/u^p)^2x^p,(u/u^p)^3y^p)$$

定义在F_{p^2}上,且满足$\psi^4+1=0$. 接下来,利用双有理等价将曲线E_1上自同态ψ转化到Jacobi Quartic曲线E_J上.

曲线E_1上存在阶为2的点$R_1=(0,0)$,根据例1可知:存在Jacobi Quartic曲线$E_J: Y^2=-\frac{u^4A}{4}X^4+1$与曲线$E_1$双有理等价,双有理映射为

$$\varphi: E_1\to E_J,(x,y)\mapsto(X,Y)=\left(\frac{2x}{y},\frac{2x^3}{y^2}-1\right),$$

$$\varphi^{-1}: E_J\to E_1,(X,Y)\mapsto(x,y)=\left(\frac{2(Y+1)}{X^2},\frac{4(Y+1)}{X^3}\right),$$

则曲线E_J上可有效计算的自同态ψ_J为

$$\psi_J(X,Y)=\varphi\psi\varphi^{-1}(X,Y)=(u^{p-1}X^p,Y^p),$$

可以验证$\psi_J^4+1=0$.

类似地,对于j不变量为0的椭圆曲线同样可以得到一个4维GLV方法构造,这里不再赘述.

4 效率分析

本节通过实验对Jacobi Quartic曲线上GLV/GLS标量乘算法的效率进行评估,并与Weierstrass曲线上的标量乘算法的效率进行比较. 为了体现比较结果的一般性,本节并没有给出具体的曲线参数选择. 针对大约128比特安全性,假设分别选择Weierstrass曲线E、Jacobi Quartic曲线的参数E_J,p_1和p_2表示256比特和128比特的某个素数,其中曲线和有限域参数并不是固定的,可以根据需要灵活选择.

为了评估算法的效率,我们在一台配置为Intel(R) Core(TM) i5-6200U CPU 2.30GHz的台式机上运行了实验,利用Magma软件[20]分别实现上述两类曲线上基于w-NAF方法、2维GLV和4维GLV标量乘算法,并比较它们的效率.

设M、S和I分别表示有限域F_{p_1}上的乘法、平方和求逆运算,忽略域上加法、减法、小系数乘法的计算. 相应地,m、s和i表示有限域$F_{p_2^2}$上的乘法、平方和求逆运算. 根据文献[7],这里假设1i=66m,1s=0.76m,1I=290M,1S=0.85M且M/m=0.91. 对于Jacobi quartic曲线,使用扩展射影坐标[21](简写为ExtJQuartic);对于Weierstrass曲线,使用Jacobian坐标(简写为Jacobian). 考虑如下基本运算:倍点($2P$)、点加($P+Q$)、混合坐标加法,分别表示为DBL、ADD和mADD. 表1给出了三类曲线上对应点运算的计算开销,其中M和S表示有限域上乘法和平方运算,而不特指有限域F_{p_1}.

表1　两种不同形式椭圆曲线上点运算的开销

曲线形式	DBL	ADD	mADD
ExtJQuartic	2M+5S	7M+4S	6M+3S
Jacobian	1M+8S	11M+5S	7M+4S

标量乘的计算通常包括预计算、求值计算和坐标转换三个阶段. 根据分析结果选择最优的实现方式,对于w-NAF方法实现,使用5-NAF表示;对于2维GLV实现,使用4-NAF表示的交叉方法(简写为2GLV+INT(4-NAF));对于4维GLV实现,使用3-NAF表示的交叉方法(简写为4GLV+INT(3-NAF)). 假设利用文献[22]中LM预计算方案,它利用了统一Z坐标减少预计算的开销,并且只需要一个求逆运算. 对于ExtJQuartic曲线,需要$1I+(12L-4)M+(5L+7)S$,其中L为预计算点数的1/2. 由于自同态的计算开销随着曲线的不同而变化,它只在预计算中出现且对整个预计算过程的开销影响不大,这里我们忽略了自同态的计算开销. 最后将坐标转换为仿射坐标形式:对于ExtJQuartic曲线,需要1I+4M;对于Jacobian曲线,需要1I+3M+1S. 表2给出了两类曲线上不同标量乘实现方法计算开销的粗略估计.

表2中给出了不同实现方式下三种曲线上标量乘运算的开销:对于ExtJQuartic曲线,2维GLV方法和4维GLV方法比5-NAF方法分别提速大约37.2%和109.4%. 同时可以看出:在三种不同的实现方式下,ExtJQuartic曲线上标量乘效率都优于Jacobian曲线. 具体地,对于2维GLV方法,ExtJQuartic曲线比Jacobian曲线分别提速大约13.2%;对于4维GLV方法,ExtJQuartic曲线比Jacobian曲线分别提速大约13.8%.

表2 两类曲线上不同标量乘实现方法计算开销比较

曲线	实现方法	算个数	计算开销	加速
$E_J(F_{p_2^2})$	4GLV+INT(3-NAF)	2i + 608m + 559s	1164.8m	109.4%
$E_J(F_{p_1})$	2GLV+INT(4-NAF)	2I + 659.2M + 840.6S	1953.7M ≈ 1777.9m	37.2%
$E_J(F_{p_1})$	5-NAF	2I + 864M + 1455S	2680.8M ≈ 2439.5m	-
$E(F_{p_2^2})$	4GLV+INT(3-NAF)	2i + 587m + 798s	1325.5m	114.3%
$E(F_{p_1})$	2GLV+INT(4-NAF)	2I + 561.4M + 1258.8S	2211.4M ≈ 2012.4m	41.1%
$E(F_{p_1})$	5-NAF	2I + 629.7M + 2248.7S	3121.1M ≈ 2840.2m	–

5 结论

对于Weierstrass曲线上GLV/GLS方法已经有比较多的研究,而在其他曲线形式上的研究还比较少.本章主要研究了GLV/GLS方法在Jacobi Quartic曲线上的应用.利用曲线之间的双有理等价、Frobenius映射、扭同构等,给出了上述两类曲线上可有效计算自同态的具体构造,并给出了一些曲线上可有效计算自同态的实例.将目前Weierstrass曲线上GLV/GLS主要研究结果推广到Jacobi Quartic曲线上,相应地得到2维和4维GLV方法.最后还通过实验对两类曲线上标量乘算法的效率进行了评估.

参考文献

[1] Gallant R P, Lambert R J, Vanstone S A. Faster point multiplication on elliptic curves with efficient endomorphisms [A]. Advances in Cryptology-CRYPTO 2001, 21st Annual International Cryptology Conference[C]. Santa Barbara, California, USA: Proceedings, 2001. 19 – 23.

[2] Park Y H, Jeong S, Kim C H, et al. An alternate decomposition of an integer for faster point multiplication on certain elliptic curves[A]. International Workshop on Public Key Cryptosystems[C]. Paris, France: Springer, 2002. 323 – 334.

[3] Sica F, Ciet M, Quisquater J J. Analysis of the gallant-lambert-vanstone method based on efficient endomorphisms: elliptic and hyperelliptic curves[A]. International Workshop on Selected Areas in Cryptograph[C]. Newfoundland, Canada: Springer, 2002. 21 – 36.

[4] Galbraith S D, Lin X, Scott M. Endomorphisms for faster elliptic curve cryptography on a large class of curves[J]. Journal of Cryptology, 2011, 24(3): 446 – 469.

[5] Zhou Z, Hu Z, Xu M, et al. Efficient 3-dimensional GLV method for faster point multiplication on some GLS elliptic curves[J]. Information Processing Letters, 2010, 110 (22): 1003 – 1006.

[6] Hu Z, Longa P, Xu M. Implementing the 4-dimensional GLV method on GLS elliptic curves with j-invariant 0[J]. Designs, Codes and Cryptography, 2012, 63(3): 331 – 343.

[7] Longa P, Sica F. Four-dimensional gallant-lambert-vanstone scalar multiplication[A]. Advances in Cryptology-ASIACRYPT 2012 [C]. Beijing, China: Springer, 2012. 718 – 739.

[8] Bos J W, Costello C, Hisil H, et al. Fast cryptography in genus 2[J]. Journal of Cryptology, 2016, 29(1): 28 – 60.

[9] Buhler J, Koblitz N. Lattice basis reduction, jacobi sums and hyperelliptic cryptosystems[J]. Bulletin of the Australian Mathematical Society, 1998, 58(01):147 – 154.

[10] Furukawa E, Kawazoe M, Takahashi T. Counting points for hyperelliptic curves of type $y^2=x^5+ax$ over finite prime fields[A]. International Workshop on Selected Areas in Cryptography[C]. Ottawa, Canada: Springer, 2003. 26 – 41.

[11] Guillevic A, Ionica S. Four-dimensional GLV via the weil restriction[A]. International Conference on the Theory and Application of Cryptology and Information Security[C]. Bengaluru, India: Springer, 2013. 79 – 96.

[12] Bos J W, Costello C, Hisil H, et al. High-performance scalar multiplication using 8-dimensional GLV/GLS decomposition[A]. International Conference on Cryptographic Hardware and Embedded Systems[C]. Santa Barbara, CA, USA: Springer, 2013. 331 – 348.

[13] 于伟, 李宝, 王鲲鹏, 等. 特征3有限域上椭圆曲线的co-Z Montgomery算法[J]. 计算机学报, 2017, 40(05):1121 – 1133.
Yu W, Li B, Wang K P, et al. Co-z montgomery algorithm for elliptic curves over finite fields of characteristic 3[J]. Chinese Journal of Computers, 2017, 40(05): 1121 – 1133. (in Chinese)

[14] Yu W, Wang K P, Li B, et al. Montgomery algorithm over a prime field[J]. Chinese Journal of Electronics, 2019, 28(01): 39 – 44.

[15] You L, Yang Y L, Gao S H. Divisor class halving algorithms for genus three hyperelliptic curves[J]. Chinese Journal of Electronics, 2020, 29(01): 97 – 105.

[16] Silverman. The Arithmetic of Elliptic Curves[M]. New

York, USA: Springer, 2009.
[17] Hankerson D, Menezes A J, Vanstone S. Guide to Elliptic Curve Cryptography[M]. New York, USA: Springer, 2004.
[18] Washington L C. Elliptic Curves Number Theory and Cryptography[M]. Florida, USA: CRC Press, 2008.
[19] Billet O , Joye M . The Jacobi model of an elliptic curve and side-channel analysis[A]. International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes[C]. Toulouse, France: Springer, 2003. 34 – 42.
[20] Magma. Magma Computational Algebra System[EB/OL]. http://magma.maths.usyd.edu.au/magma/, 2019.
[21] Hisil H, Carter G, Dawson E, et al. Jacobi quartic curves revisited[A]. Australasian Conference on Information Security and Privacy[C]. Brisbane, Australia: Springer, 2009. 452 – 468.
[22] Longa P, Miri A. New composite operations and precomputation scheme for elliptic curve cryptosystems over prime fields[A]. International Workshop on Public Key Cryptography[C]. Barcelona, Spain: Springer, 2008. 229 – 247.

作者简介

翁　江　男,1986 年 3 月出生,陕西西安人. 现为空军工程大学信息与导航学院讲师,主要研究方向为网络密码和椭圆曲线密码.
E-mail: wengjiang858@163.com

姬伟峰　男,1976 年 3 月出生,陕西西安人. 现为空军工程大学信息与导航学院副教授,主要从事网络安全方向的研究.
E-mail: jiwf@yeah.net

吴　玄　男,1998 年 9 月出生,安徽阜阳人. 现为空军工程大学信息与导航学院研究生,主要从事信息安全方向的研究.
E-mail: 1766300243@qq.com

李映岐　男,1999 年 1 月出生,河南南阳人. 现为空军工程大学信息与导航学院研究生,主要从事信息安全方向的研究.
E-mail: 1152007427@qq.com

张林锋　男,1981 年 9 月出生,江西玉山人. 2007 年毕业于空军工程大学,获得硕士学位,研究方向为网络安全技术.
E-mail: zhanglinfengmail@163.com

孟　浩　男,1978 年 7 月出生,吉林公主岭人. 2016 年毕业于空军工程大学,获得硕士学位,研究方向为网络安全技术.
E-mail: mofymofy@163.com