·开发研究与工程应用· 文章编号:1000-3428(2015)01-0270-05 文献标识码:A 中图分类号:TP391

扭曲雅可比相交曲线上的斜-Frobenius 映射

曹鸿钰,王鲲鹏

(中国科学院信息工程研究所,北京 100093)

摘 要:利用扭曲的雅可比相交曲线上的 Frobenius 自同态映射,构造在扭曲的雅可比相交曲线二次扭曲线上的一个斜-Frobenius 映射,可用于制定扭曲的雅可比相交曲线的快速点乘算法,而不需要使用任何倍点。采用 GLV 方法加快扭曲的雅可比相交曲线上的点乘运算,给出斜的 Frobenius 映射的特征多项式。实例结果表明,该映射能够加速扭曲雅可比相交曲线上的标量乘运算。

关键词:雅可比相交曲线;双有理等价;扭曲曲线;斜-Frobenius 映射;τ-展开;GLV 方法

中文引用格式:曹鸿钰,王鲲鹏. 扭曲雅可比相交曲线上的斜-Frobenius 映射[J]. 计算机工程,2015,41(1):270-274.

英文引用格式:Cao Hongyu, Wang Kunpeng. Skew-Frobenius Mapping on Twisted Jacobi Intersection Curve[J]. Computer Engineering,2015,41(1):270-274.

Skew-Frobenius Mapping on Twisted Jacobi Intersection Curve

CAO Hongyu, WANG Kunpeng

(Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China)

【Abstract】 Using the Frobenius endomorphism on twisted Jacobi intersection curve, this paper constructs a skew-Frobenius mapping which is defined on the quadratic twist of twisted Jacobi intersection curve. It can be exploited to devise fast point multiplication algorithm on twisted Jacobi intersection curve that does not use any point doubling. The Gallant-Lamber-Vanstone(GLV) method can be used for speeding up point multiplication on twisted Jacobi intersection curve. The characteristic polynomial of the mapping is given. Example results show that the mapping can speed up the scalar multiplication of twisted Jacobi intersection curve.

【Key words】 Jacobi intersection curve; birationally equivalent; twist curve; skew-Frobenius mapping; τ-expansion; Gallant-Lamber-Vanstone(GLV) method

DOI:10.3969/j.issn.1000-3428.2015.01.051

1 概述

早在 1829 年,Jacobi 研究了雅可比相交(Jacobi intersection)形式的椭圆曲线(简称雅可比相交曲线),给出了其上的群律。雅可比相交曲线在 1986 年被 Chudnovsky 和 Chudnovsky[1]引入椭圆曲线密码学。

雅可比相交曲线是一种三维空间中 2 个曲面的交,其上不仅可以有一般的标量乘,还可以实现配对计算。文献[2]给出了雅可比相交曲线上雅可比相交曲线上配对的具体计算方法。

本文回顾扭曲雅可比相交曲线和椭圆曲线上的 Frobenius 映射。介绍扭曲雅可比相交曲线上的 Frobenius 映射。引入斜-Frobenius 映射,并应用 Frobenius 映射和斜-Frobenius 映射来加速扭曲雅可比相交曲线上的的标量乘运算。

2 预备知识

2.1 背景介绍

雅可比相交曲线上的标量乘速度是比较有竞争力的,例如在其上可以进行快速倍点和三倍点计算。其中,文献[1]给出了射影坐标中雅可比相交曲线上的快速倍点和点加公式。文献[3-4]对快速倍点和点加公式给出了一些改进。文献[5]给出了雅可比相交曲线上的快速三倍点公式。文献[6]给出了更快速的公式。另外,文献[7]的分析表明特征 3 的域

基金项目:国家“973”计划基金资助项目(2013CB338001);国家自然科学基金资助项目(61272040);中国科学院战略性先导科技专项基金资助项目(XDA06010702)。

作者简介:曹鸿钰(1988-),男,硕士研究生,主研方向:信息安全;王鲲鹏,教授。

收稿日期:2014-02-18 **修回日期**:2014-03-20 **E-mail**:feng_896@163.com

上雅可比相交曲线上的标量乘计算得更快。

由于计算 Frobenius 映射比计算倍点效率高,文献[8]提出了利用二次 twised 椭圆曲线上的 Frobenius 映射替代倍点。文献[9]称这种映射为斜-Frobenius 映射,并构造了亏格为 2 和 3 的超椭圆曲线上的斜-Frobenius 映射。

文献[10]将雅可比相交曲线推广为扭曲雅可比相交形式的椭圆曲线(简称扭曲雅可比相交曲线)。在一个特征不为 2 的域 k 上,任一扭曲雅可比相交曲线双有理等价于一条椭圆曲线。利用扭曲雅可比相交曲线和椭圆曲线间的双有理映射,构造了域 k 上的扭曲雅可比相交曲线上的 Frobenius 映射,并给出这一 Frobenius 的特征方程。利用扭曲雅可比相交曲线上的 Frobenius 自同构映射可以构造快速标量乘算法。

利用扭曲雅可比相交曲线上的 Frobenius 映射和文献[8]中的方法,构造了扭曲雅可比相交曲线上的斜-Frobenius 映射。借鉴文献[11]中的方法,结果表明斜-Frobenius 映射可以用来加速扭曲雅可比相交曲线上的标量乘。扩展文献[12]的方法,文献[13]方法也可以应用在加速扭曲雅可比相交曲线的标量乘上。

2.2　雅可比相交曲线与扭曲雅可比相交曲线

特征不为 2 的域 k 上的雅可比相交曲线定义为:

$$\begin{cases} u^2+v^2=1 \\ bu^2+w^2=1 \end{cases}$$

其中,$b\in k,(1-b)b\neq 0,(0,1,1)$ 为零元。其上的群律由以下方程给出:

$$(u_1,v_1,w_1)+(u_2,v_2,w_2)=(u_3,v_3,w_3)$$

其中,$u_3=\dfrac{u_1v_2w_2+u_2v_1w_1}{v_2^2+u_2^2w_1^2}$;$v_3=\dfrac{v_1v_2-u_1w_1u_2w_2}{v_2^2+u_2^2w_1^2}$;

$w_3=\dfrac{w_1w_2-bu_1v_1u_2v_2}{v_2^2+u_2^2w_1^2}$。

文献[10]将雅可比相交曲线推广为广义形式的扭曲雅可比相交曲线 $E_{J,a,b}$,定义为:

$$\begin{cases} au^2+v^2=1 \\ bu^2+w^2=1 \end{cases}$$

其中,$a,b\in k,(a-b)ab\neq 0$。扭曲雅可比相交曲线的群律定义为[10]:

$$(u_1,v_1,w_1)+(u_2,v_2,w_2)=(u_3,v_3,w_3)$$

其中,$u_3=\dfrac{u_1v_2w_2+u_2v_1w_1}{v_2^2+au_2^2w_1^2}$;$v_3=\dfrac{v_1v_2-au_1w_1u_2w_2}{v_2^2+au_2^2w_1^2}$;

$w_3=\dfrac{w_1w_2-bu_1v_1u_2v_2}{v_2^2+au_2^2w_1^2}$。

更加完整的群律可以参考文献[14]。

扭曲雅可比相交曲线是光滑曲线并且双有理等价于椭圆曲线 $y^2=x(x-a)(x-b)$。

一条扭曲雅可比相交曲线 $E_{J,a,b}$ 是雅可比相交曲线 $E_{J,1,b/a}$ 的二次扭曲曲线。更一般地,$E_{J,a,b}$ 是 $E_{J,\bar{a},\bar{b}}$ 的二次扭曲曲线,其中 $b/a=\bar{b}/\bar{a}$。反过来,每个扭曲雅可比相交曲线的二次 twist 曲线是一个扭曲雅可比相交曲线。

2.3　椭圆曲线上的 Frobenius 映射

设 F_q 是一个特征大于 2 的有限域。F_q 上的椭圆曲线定义为:

$$E:\{(x,y)\mid y^2=x^3+a_2x^2+a_4x+a_6,a_2,a_4,a_6\in F_q\}\cup\{\infty\}$$

其中,∞ 为无穷远点。椭圆曲线 E 上的 q 次 Frobenius 映射 π_q 定义为:

$$\pi_q:E\to E$$
$$(x,y)\to(x^q,y^q)$$

记 $N=\#E(F_q)$,根据 Hasse 定理得到 $N=q+1-t$,这里 $t\leqslant\sqrt{q}$,且 π_q 的特征方程 $a_q(\lambda)$ 为:

$$a_q(\lambda)=\lambda^2-t\lambda+q$$

则对于任一 $P\in E(\bar{F}_q)$,π_q 满足方程:

$$(\pi_q^2-t\pi+q)P=\infty$$

其中,$\bar{F}_q$ 是 F_q 的代数闭包。

3　Frobenius 映射

设 F_q 是一个特征大于 2 的有限域且 $E_{J,a,b}$ 是定义在 F_q 的扭曲雅可比相交曲线。考虑如下的 $E_{J,a,b}$ 上的 q 次 Frobenius 映射:

$$\Pi_q:E_{J,a,b}\to E_{J,a,b}$$
$$(u,v,w)\to(u^q,v^q,w^q)$$

并且证明如下结论。

定理 1　$E_{J,a,b}$ 是定义在 F_q 上的扭曲雅可比相交曲线且 $\#E_{J,a,b}=q+1-t$。那么对于任一 $P\in E_{J,a,b}(F_q)$,$E_{J,a,b}$ 上的 Frobenius 映射 Π_q 满足:

$$(\Pi_q^2-t\Pi+q)P=\infty$$

为了证明这一定理,引入如下的引理。

引理 1　F_q 是一个特征大于 2 的有限域。任意一个 F_q 上的扭曲雅可比相交曲线在 F_q 中双有理等价于一个形式为 $y^2=x(x-a)(x-b)$ 的椭圆曲线[10]。

根据引理 1,存在 F_q 上的一个形式为 $y^2=x(x-a)(x-b)$ 的椭圆曲线 E,满足 $E_{J,a,b}(\bar{F}_q)\cong E(\bar{F}_q)$。设 ψ 是 $E_{J,a,b}$ 到 E 的同构映射,φ 是 ψ 的逆映射。由文献[10]中的定理 3.2,得到映射:

$$\psi:(u,v,w)\to(x,y)=\left(-\frac{a(w+1)}{v-1},\frac{au}{v-1}(x-b)\right)$$

是 $E_{J,a,b}$ 到 E 双有理等价映射,同时它的逆映射

φ 为：

$$\varphi:(x,y)\rightarrow(u,v,w)=\left(-\frac{2y}{x^2-ab},\frac{x^2-2ax+ab}{x^2-ab},\frac{x^2-2bx+ab}{x^2-ab}\right)$$

点$(u,v,w)=(0,1,1)$对应点$(x,y)=\infty$，点$(u,v,w)=(0,1,-1)$对应点$(x,y)=(b,0)$。

引理 2 $E_{J,a,b}$是定义在 F_q 上的扭曲雅可比相交曲线且 E 是形式为 $y^2=x(x-a)(x-b)$的椭圆曲线。设$\#E(F_q)=q+1-t$，ψ 是如上定义的双有理映射，π_q 是 E 上的 q 次 Frobenius 映射。定义$\Psi=\psi^{-1}\circ\pi_q\circ\psi$，那么：

(1) $\Psi\in End(E_{J,a,b})$(即 Ψ 是 $E_{J,a,b}$上的同源映射)；

(2)任一 $P\in E_{J,a,b}(F_q)$，Ψ 满足：

$$\Psi^2(P)-[t]\Psi(P)+[q](P)=\infty_{E_{J,a,b}}$$

证明：根据对引理 1 的讨论，ψ 是 $E_{J,a,b}$到 E 的 F_q 中的同构映射，π_q 是 E 上到自身的 F_q 中的同源映射。根据 Ψ 的定义，Ψ 是 $E_{J,a,b}$到自身的 F_q 中的同源映射。

对于任一 $P\in E_{J,a,b}(F_q)$，记 $Q=\psi(P)\in E(F_q)$，则：

$$(\pi_q^2-t\pi+q)Q=\infty_E$$

所以：

$$\psi^{-1}(\pi_q^2-t\pi+q)\psi(P)=\infty_{E_{J,a,b}}$$

根据文献[15]的定理 4.8 得到：

$$\psi^{-1}\pi_q^2\psi(P)-[t]\psi^{-1}\pi\psi(P)+[q](P)=\infty_{E_{J,a,b}}$$

即：

$$\Psi^2(P)-[t]\Psi(P)+[q](P)=\infty_{E_{J,a,b}}$$

证毕。

定理 1 的证明：E 是 F_q 上的一个形式为 $y^2=x(x-a)(x-b)$的椭圆曲线，Ψ 是引理 2 中的 $E_{J,a,b}$自同构映射。根据 Ψ 的定义，对于任一 $P=(u,v,w)\in E_{J,a,b}(\bar{F}_q)$，有：

$$\Psi(u,v,w)=(\psi^{-1}\circ\pi_q\circ\psi)(u,v,w)=(\psi^{-1}\circ\pi_q)\left(-\frac{a(w+1)}{v-1},\frac{au}{v-1}(x-b)\right)=\psi^{-1}\left(-\frac{a(w^q+1)}{v^q-1},\frac{au^q}{v^q}(x-b)\right)=(u^q,v^q,w^q)$$

因此，对于任一 $P\in E_{J,a,b}(\bar{F}_q)$，能得到 $\Psi(P)=\Pi_q(P)$。那么根据引理 2，定理 1 得到证明。

可以用这样的 Frobenius 映射加速扭曲雅可比相交曲线上的标量乘。

4 斜-Frobenius 映射

利用第 3 节中的扭曲雅可比相交曲线上的 Frobenius 映射构造雅可比相交曲线的二次 twist 曲线上的斜-Frobenius 映射。这个构造是文献[8,11]中结果的扩展。

F_q 上的 $E_{J,a,b}$是 $E_{J,\bar{a},\bar{b}}$的二次扭曲曲线，其中$\bar{a}$，$\bar{b}$满足 $b/a=\bar{b}/\bar{a}$，令：

$$\phi:E_{J,a,b}\rightarrow E_{J,c,d}$$

$$(u,v,w)\mapsto(\sqrt{\alpha}u,v,w)$$

其中，$\alpha=a/\bar{a}$。若 α 是 $k=F_q$ 上的二次非剩余，则映射 ϕ 是在域 $k(\sqrt{\alpha})$上的 $E_{J,a,b}$到 $E_{J,\bar{a},\bar{b}}$的同构映射，记 $E^t_{J,a,b}$的二次 twist 曲线为 $E^t_{J,a,b}$。

下面开始构造 $E^t_{J,a,b}$上的斜-Frobenius 映射 Π^t_q。根据 $E_{J,a,b}$上的 Frobenius 映射 Π_q 的定义，$E^t_{J,a,b}$上的斜-Frobenius 映射 Π^t_q 可以定义为：

$$\Pi^t_q:E^t_{J,a,b}\xrightarrow{\phi^{-1}}E_{J,a,b}\xrightarrow{\Pi_q}E_{J,a,b}\xrightarrow{\phi}E^t_{J,a,b}$$

因此任一 $P=(u,v,w)\in E_{J,a,b}((F_q^2),\Pi^t_q$ 满足：

$$\Pi^t_q(P)=\phi\circ\Pi_q\circ\phi^{-1}(u,v,w)=(\sqrt{\alpha}^{1-q}u^q,v^q,w^q)$$

定理 2 $E_{J,a,b}$是 $k=F_q$ 上的扭曲雅可比相交曲线且 $E^t_{J,a,b}$是 $E_{J,a,b}$的二次扭曲曲线。设$\#E_{J,a,b}(F_q)=q+1-t$，映射 ϕ 是 $k(\sqrt{\alpha})$上的 $E^t_{J,a,b}$到 $E^t_{J,a,b}$的同构映射。设 Π_q 是 $E_{J,a,b}$上的 q 次 Frobenius 映射。定义 $\Pi^t_q=\phi\circ\Pi_q\circ\phi^{-1}$，则对于任一 $P\in E^t_{J,a,b}(\bar{F}_q^2)$，$\Pi^t_q$ 满足：

$$(\Pi^t_q)^2(P)-[t]\Pi^t_q(P)+[q](P)=\infty_{E^t_{J,a,b}}$$

证明：根据定理 1，得到 $\Pi_q^2-t\Pi+q=0$，进而可以推出 $\phi\circ(\Pi_q^2-t\Pi+q)\circ\phi^{-1}=0$，即对于任一 $P\in E^t_{J,a,b}(\bar{F}_q{}^2)$，$\Pi^t_q$ 满足：

$$(\Pi^t_q)^2(P)-[t]\Pi^t_q(P)+[q](P)=\infty_{E^t_{J,a,b}}$$

和 Frobenius 映射 Π_q 类似，$E^t_{J,a,b}$ 上的斜-Frobenius 映射 Π^t_q 可以用来加速扭曲雅可比相交曲线上的标量乘。

5 方法应用描述与实例

为了加速标量乘，文献[16-17]利用 Frobenius 自同构映射开发出了不利用倍点公式的标量乘算法。这种基于 Frobenius 自同构的特征方程的 nP 分解已经被用来计算标量乘：

$$nP=\sum_{i\geq 0}c_i\tau^iP$$

其中，c_i 是固定集合中的元素，例如$\{-q/2,\cdots,q/2\}$。

若 F_q 是一个小域时，标量乘可以使用不相邻形式以 τ 为基展开 nP 来加速[18-19]。当 F_q 非常大时，文献[13]设计了一种方法来加速标量乘。

5.1 τ-进制展开方法

$E_{J,a,b}$是 $k=F_q$ 上的扭曲雅可比相交曲线且

$E_{J,a,b}$是 $E_{J,a,b}$的二次扭曲曲线。根据定理 2,存在一个复数 τ 使得 $E^t_{J,a,b}$上的斜-Frobenius 映射可以被认为是 τ。τ 是一个由以下方程给出的复数:

$$\tau^2 - t\tau + q = 0$$

其中,$t = q + 1 - \#E_{J,a,b}(F_q)$。可以将 $k \in Z[\tau]$ 的 ω 宽窗口 τ 的不相邻形式(ω-τNAF)表示如下:

$$k = \sum_{i=0}^{t-1} c_i \tau^i$$

其中,$c_i \in \{-q/2, \cdots, q/2\}$,$i = 0, 1, \cdots, t-1$;如果 $c_i, c_{i+1}, \cdots, c_{i+\omega-1}$是 ω 个连续系数,那么它们当中至多一个非零。

对于 $P \in E^t_{J,a,b}(\overline{F}_q^2)$,$nP$ 可以被如下快速计算:

$$nP = \sum_{i=0}^{t-1} (\Pi_q^t)^i (c_i P)$$

$(\Pi_q^t)^i(c_i P)$可以按如下公式计算:

$$(\Pi_q^t)^i (c_i P) = (\sqrt{\alpha}^{1-q^i} u^{q^i}, v^{q^i}. w^{q^i})$$

利用 $E_{J,a,b}$上的 Frobenius 映射 Π_q,上述方法可以应用在扭曲雅可比相交曲线上。

虽然 Π_q^t 耗时比 Π_q 长得多,但是当$\#E^t_{J,a,b}(F_q^2)$和素数相差不大时,利用 Π_q^t 计算 $E^t_{J,a,b}$上的标量乘还是比过去的方法快。

5.2　GLV 方法

扩展文献[11]的方法,将 GLV 方法应用在扭曲雅可比相交曲线的标量乘上。

定理 3　设 F_q 的特征大于 3,$E_{J,a,b}$是 $k = F_q$ 上的扭曲雅可比相交曲线,且$\#E_{J,a,b}(F_q) = q + 1 - t$。令 $E^t_{J,a,b}$ 是 F_q^2 上的 $E_{J,a,b}$ 的二次扭曲曲线,则$\#E^t_{J,a,b}(F_q^2) = (q-1)^2 + t^2$。设 $r \mid \#E_{J,a,b}(F_q^2)$是一个素数且 $r > 2q$。$\phi: E_{J,a,b} \to E^t_{J,a,b}$是一个定义在 F_q^4 上的扭曲同构映射。令:

$$\Pi_q^t = \phi \circ \Pi_q \circ \phi^{-1}$$

则对于任一 $P \in Et\ J;a;b(F_q^2)[r]$,$\Pi_q^t$ 满足:

$$(\Pi_q^t)^2(P) + P = \infty_{E^t_{J,a,b}}$$

证明:由著名的 Weil 定理,得到$\#E_{J,a,b}(F_q^2) = (q+1)^2 - t^2$ 和$\#E_{J,a,b}(F_q^2) = (q-1)^2 + t^2$。

由于 r 是素数且 $r > 2q$,因此 $r \chi \#E_{J,a,b}(F_q^2) = (q+1-t)(q+1+t)$。根据定理假设,可以得到$r \mid \#E^t_{J,a,b}(F_q^4) = \#E_{J,a,b}(F_q^2)\ \#E_{J,a,b}(F_q^2)$,但是$r^2 \chi \#E_{J,a,b}(F_q^4)$。这意味着若 $\$P = (u,v,w) \in E^t_{J,a,b}(F_q^2)[r]$,则 $\Pi_q^t(P)$属于 $E^t_{J,a,b}(F_q^2)[r]$,那么就存在 $\lambda \in Z$ 满足 $\Pi_q^t(P) = \lambda P$。

根据定义,$\Pi_q^t(u,v,w) = (\alpha^{\frac{1-q}{2}} u^q, v^q, w^q)$,这里 $\alpha \in F_q^2$ 是 F_q^2 中的二次非剩余。同时得到:

$$(\Pi_q^t)^2(u,v,w) = (\alpha^{\frac{1-q^2}{2}} u^{q^2}, v^{q^2}, w^{q^2})$$

由于 $\alpha \in F_q^2$ 是 F_q^2 中的二次非剩余,则 $\alpha^{\frac{1-q^2}{2}} = -1$。又 $P = (u,v,w) \in E^t_{J,a,b}(F_q^2)$,那么有:

$$u^{q^2} = u, v^{q^2} = v, w^{q^2} = w$$

因此:

$$(\Pi_q^t)^2(u,v,w) = (-u,v,w) = -P$$

证毕。

例 1　$p = 2^{192} - 2^{64} - 1$ 是一个素数。$d = 2^{64} + 1$ 是 F_p 上的一个二次非剩余。则在 F_p^4 上,$E_{J,1,\lambda}$($\lambda = -421$)的二次扭曲曲线是 $E_{J,\sqrt{d},\sqrt{d}\lambda}$。在 F_p^4 上,$E_{J,1,\lambda}$到 $E_{J,\sqrt{d},\sqrt{d}\lambda}$的扭曲同构映射定义为:

$$\phi: E_{J,1,\lambda} \to E_{J,\sqrt{d},\sqrt{d}\lambda},\ (u,v,w) \mapsto (d^{-1/4} u.\ v.\ w)$$

$E_{J,\sqrt{d},\sqrt{d}\lambda}$上的斜-Frobenius 映射为:

$$\Pi_p^t(u,v,w) \mapsto (d^{\frac{1-p}{4}} u^p.\ v^p.\ w^p)$$

对于 $P \in E_{J,\sqrt{d},\sqrt{d}\lambda}(F_{p^2})$,有:

$$\Pi_p^t(u,v,w) \mapsto (d^{-1/4} u^{p^2}.\ v^{p^2}.\ w^{p^2}) = (d^{\frac{1-p^2}{4}} u, v, w)$$

由于 d 是 F_p 上的一个二次非剩余且 $p \equiv 1 \pmod 4$,因此在 F_p^2 上 $d^{\frac{1-p^2}{4}} = 1$。

对于任一 $P \in E_{J,\sqrt{d},\sqrt{d}\lambda}(F_{p^2})$,$\Pi_q^t$ 满足$(\Pi_q^t)^2(P) + P = \infty_{E_{J,\sqrt{d},\sqrt{d}\lambda}}$。

例 2　$p = 2^{255} - 19$ 是一个素数。$d = 121\ 665/121\ 666$ 是 F_p 上的一个二次非剩余,则 $E_{J,\sqrt{d},\sqrt{d}\lambda}$是 $E_{J,-1,\lambda}$($\lambda = -5\ 737$)在 F_p^4 上的二次扭曲曲线。可以定义 $E_{J,1,\lambda}$到 $E_{J,\sqrt{d},\sqrt{d}\lambda}$的 F_p^4 上的扭曲同构映射为:

$$\varphi: E_{J,1,\lambda} \to E_{J,\sqrt{d},\sqrt{d}\lambda},\ (u,v,w) \mapsto (d^{-1/4} u.\ v.\ w)$$

$E_{J,\sqrt{d},\sqrt{d}\lambda}$上的斜-Frobenius 映射为:

$$\Pi_p^t(u,v,w) \mapsto (d^{\frac{1-p}{4}} u^p.\ v^p.\ w^p)$$

对于 $P \in E_{J,\sqrt{d},\sqrt{d}\lambda}(F_{p^2})$,有:

$$\Pi_p^t(u,v,w) \mapsto (d^{-1/4} u^{p^2}.\ v^{p^2}.\ w^{p^2}) = (d^{\frac{1-p^2}{4}} u, v, w)$$

d 是 F_p 上的一个二次非剩余且 $p \equiv 1 \pmod 4$,则在 F_p^2 上 $d^{\frac{1-p^2}{4}} = 1$。

可以推出对于任一 $P \in E_{J,\sqrt{d},\sqrt{d}\lambda}(F_{p^2})$,$\Pi_p^t$ 满足$(\Pi_q^t)^2(P) + P = \infty_{E_{J,\sqrt{d},\sqrt{d}\lambda}}$。

同时由于 $E_{J,a,b}$是 $E_{J,\overline{a},\overline{b}}$的二次扭曲曲线,其中 $b/a = \overline{b}/\overline{a}$,这样可以选小一点的$\overline{a}, \overline{b}$,使得 $E_{J,\overline{a},\overline{b}}$是 $E_{J,a,b}$的二次扭曲曲线。

6　结束语

本文论述了定义在有限域 F_q 上的扭曲雅可比相交曲线中的自同构,介绍了扭曲雅可比相交曲线上 Frobenius 映射的性质并给出了这个 Frobenius 映射的特征方程。应用扭曲雅可比相交曲线上的 Frobenius 映射,构造了定义在扭曲雅可比相交曲线二次扭曲曲线上的斜-Frobenius 映射。结果表明,扭曲雅可比相交曲线的 Frobenius 映射和斜-Frobenius 映射可以加速扭曲雅可比相交曲线上的标量乘运算。

参考文献

[1] Chudnovsky D V, Chudnovsky G V. Sequences of Numbers Generated by Addition in Formal Groups and New Primality and Factorization Tests[J]. Advances in Applied Mathematics, 1986, 7(4): 385-434.

[2] 唐春明, 徐茂智, 亓延峰. Jacobi 交上的配对计算[J]. 计算机工程与科学, 2011, 33(10): 25-29.

[3] Liardet P Y, Smart N P. Preventing SPA/DPA in ECC Systems Using the Jacobi Form[C]//Proceedings of the 3rd International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Germany: Springer, 2001: 391-401.

[4] Bernstein D J, Lange T. Explicit-formulae Database [EB/OL]. (2008-03-12). http://www.hyperelliptic.org/EFD.

[5] Hisil H, Carter G, Dawson E. New Formulae for Efficient Elliptic Curve Arithmetic[C]//Proceedings of the 8th International Conference on Cryptology in India. Berlin, Germany: Springer, 2007: 138-151.

[6] Hisil H, Wong K K H, Carter G, et al. Faster Group Operations on Elliptic Curves[C]//Proceedings of the 7th Australasian Conference on Information Security. [S.l.]: Australian Computer Society Inc., 2009: 7-20.

[7] 端木庆峰, 张雄伟, 王衍波, 等. 3 特征域椭圆曲线群点的快速计算算法[J]. 解放军理工大学学报: 自然科学版, 2011, 12(1): 1-6.

[8] Iijima T, Matsuo K, Chao J, et al. Construction of Frobenius Maps of Twists Elliptic Curves and Its Application to Elliptic Scalar Multiplication [C]// Proceedings of Conference on Small Computer System Interface. Berlin, Germany: Springer, 2002: 699-702.

[9] Kozaki S, Matsuo K, Shimbara Y. Skew-Frobenius Maps on Hyperelliptic Curves [J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2008, 91(7): 1839-1843.

[10] Feng Rongquan, Nie Menglong, Wu Hongfeng. Twisted Jacobi Intersections Curves [J]. Theoretical Computer Science, 2013, 494: 24-35.

[11] Wang Mingqiang, Wang Xiaoyun, Zhan Tao, et al. Skew-Frobenius Map on Twisted Edwards Curve[C]// Proceedings of the 7th International Conference on Theory and Application of Models of Computation. Prague, Czech: [s.n.], 2010: 199-210.

[12] Gallant R P, Lambert R J, Vanstone S A. Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms[C]//Advances in Cryptology-CRYPTO'01. Berlin, Germany: Springer, 2001: 190-200.

[13] 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.

[14] Wu H, Feng R. A Complete Set of Addition Laws for Twisted Jacobi Intersection Curves [J]. Wuhan University Journal of Natural Sciences, 2011, 16(5): 435-438.

[15] Silverman J H. The Arithmetic of Elliptic Curves[M]. Dordrecht, the Netherlands: Springer, 2009.

[16] Solinas J A. Efficient Arithmetic on Koblitz Curves[J]. Designs, Codes and Cryptography, 2000, 19(2/3): 195-249.

[17] Solinas J A. An Improved Algorithm for Arithmetic on a Family of Elliptic Curves[C]//Proceedings of CRYPTO'97. Berlin, Germany: Springer, 1997: 357-371.

[18] Koblitz N. CM-curves with Good Cryptographic Properties[C]//Proceedings of CRYPTO'91. Berlin, Germany: Springer, 1992: 279-287.

[19] Blake I F, Kumar M V, Xu Guangwu. Efficient Algorithms for Koblitz Curves over Fields of Characteristic Three[J]. Journal of Discrete Algorithms, 2005, 3(1): 113-124.

编辑 顾逸斐

(上接第 269 页)

参考文献

[1] Vócking B. How Asymmetry Helps Load Balancing[J]. Journal of the ACM on Computer, 2003, 50(4): 568-589.

[2] Fall K R, Stevens W R. TCP/IP Illustrated[M]. [S.l.]: Addison-Wesley Professional, 2011.

[3] 刘舱强, 邓昌胜, 余 谅. 基于哈希表的最长前缀匹配算法改进[J]. 微计算机信息, 2009, (30): 143-144.

[4] 崔尚森, 张白一. 一种基于哈希表和 Trie 树的快速 IP 路由查找算法[J]. 计算机工程与应用, 2005, 41(9): 156-158.

[5] 赵国锋, 陈群丽. 基于 Hash 和 AQT 的类决策树包分类算法研究[J]. 通信技术, 2010, 43(2): 210-212.

[6] 李英毅, 贾 雨. 用 Hash 表技术实现快速流分类[J]. 成都理工大学学报: 自然科学版, 2008, 35(1): 108-112.

[7] 强士卿, 程 光. 基于流的哈希函数比较分析研究[J]. 南京师范大学学报: 工程技术版, 2008, 8(4): 25-28.

[8] 程 光, 龚 俭, 丁 伟, 等. 面向 IP 流测量的哈希算法研究[J]. 软件学报, 2005, 16(5): 652-658.

[9] Kumar S, Crowley P. Segmented Hash: An Efficient Hash Table Implementation for High Performance Networking Subsystems [C]//Proceedings of ACM Symposium on Architecture for Networking and Communications Systems. [S.l.]: ACM Press, 2005: 91-103.

[10] Kumar S, Turner J, Crowley P. Peacock Hashing: Deterministic and Updatable Hashing for High Performance Networking[C]//Proceedings of the 27th Conference on Computer Communications. [S.l.]: IEEE Press, 2008: 101-105.

[11] 张朝霞, 刘耀军. 有效的哈希冲突解决办法[J]. 计算机应用, 2010, 30(11): 2965-2966.

[12] MacKenzie P D, Plaxton C G, Rajaraman R. On Contention Resolution Protocols and Associated Probabilistic Phenomena[C]//Proceedings of the 26th Annual ACM Symposium on Theory of Computing. [S.l.]: ACM Press, 1994: 153-162.

[13] Cormen T H, Leiserson C E, Rivest R L, et al. Introduction to Algorithms[M]. Cambridge, USA: MIT Press, 2001.

编辑 顾逸斐