Proceedings of the Jangjeon Mathematical Society
22 (2019), No. 1. pp. 7 – 14

www.jangjeon.or.kr
http://dx.doi.org/10.17777/pjms2019.22.1.7

SCALAR MULTIPLICATION ON JACOBI CURVES USING THE FROBENIUS MAP

GYOYONG SOHN

Abstract. In this paper, we consider the scalar multiplication on Jacobi curves over a finite field using the Frobenius expansion. Applying the Frobenius endomorphism on Jacobi curves, we construct a Frobenius map defined on the quadratic twist of Jacobi curves. To speed up the scalar multiplication on Jacobi curves, we use the GLV method combined with the Frobenius endomorphism over the curves.

2010 Mathematics Subject Classification. 94A55, 11T71.

Keywords and phrases. twisted Jacobi intersection, Jacobi quartic, scalar multiplication, Frobenius map.

1. Introduction

Elliptic curve cryptography was independently proposed by Koblitz [11] and Miller [12] in 1985. The elliptic curve cryptosystem is a public key cryptosystem based on the discrete logarithm problem in the group of points on a curve. In elliptic curve cryptosystems, the efficiency depends essentially on the fundamental operation of the scalar multiplication $[n]P$ for a given point P on an elliptic curve E and an integer n. In general, the computational speed of a scalar multiplication $[n]P$ depends on finite field operations, curve point operations, and representation of the scalar n[13, 7].

There is a vast literature on efficient methods for computational speeding up scalar multipliclation. For elliptic curves, the scalar multiplication can be done with various methods. If an elliptic curve admits an efficient endomorphism, its use can speed up scalar multiplication. In [9], Iijima, Matsuo, Chao and Tsujii presented an efficiently computable homomorphism on elliptic curves using the Frobnius map on the quadratic twists of an elliptic curve. The Gallant-Lambert-Vanstone (GLV) gave suitable efficiently computable endomorphisms on elliptic curves for speeding up point multiplication [6].

Recently, there are several models of elliptic curves to provide the efficient computation, such as Edwards curves [3], Huff curves [8], Jacobi quartics[1], Hessian curve [10], and Jacobi intersections [2]. Chudnovsky and Chudnovsky [2] presented the Jacobi intersections curve $u^2+v^2=1$, $bu^2+w^2=1$ and efficient doubling and addition formulae in projective coordinates. The Jacobi intersections is the intersection of two quadratic surfaces in three dimensional space with a point on it. R. Feng et al.[4] introduced the twisted Jacobi intersections curve $au^2+v^2=1$, $bu^2+w^2=1$ for $a,b\in K$ with $ab(a-b)\neq 0$.

This work was supported by the research fund of Daegu National University of Education in 2017.

In this paper, we present the Frobenius endomorphism on Jacobi curves over a finite field and the scalar multiplication on Jacobi curves using Frobenius expansion. We focus our interest on Jacobi intersections curve and Jacobi quartic curve in Jacobi curves. Applying the Frobenius endomorphism on Jacobi curves, we construct a Frobenius map defined on the quadratic twist of Jacobi curves. To speed up the scalar multiplication on Jacobi curves, we use the GLV method combined with the Frobenius endomorphism over the curves.

This paper is organized as follows. Section 1 illustrate some basic notions on twisted Jacobi intersections, Jacobi quartic curves and Frobenius endomorphism. We also give expression of the group law and the birational equivalence between twisted Jacobi intersection and Weierstrass equation of elliptic curve. Second section describe Frobenius endomorphism for Jacobi intersections, Jacobi quartic curves and some basic properties.

2. Premiminaries

This section recall some basic notions for twisted Jacobi intersections curve, Jacobi quartic curves and Frobenius maps on elliptic curves.

2.1. **Twisted Jacobi intersections curve.** Let K be a field with $char(K) \neq 2$ and $\overline{K}$ its algebraic closure. A Jacobi intersections curve is defined by $u^2 + v^2 = 1$, $bu^2 + w^2 = 1$ where $b \in K$ and $b(1-b) \neq 0$. The Jacobi intersections curve is the intersection of two quadratic surfaces in three dimensional space with a point on it. The point $(0, 1, 1)$ is the neutral element of the addition law. The negative of the point (u, v, w) is $(-u, v, w)$. The addition and doubling formula for Jacobi intersections can be found in [2].

A twisted Jacobi intersections curve is an elliptic curve over a field K defined by

$$J_{a,b} : \begin{cases} au^2 + v^2 = 1 \\ bu^2 + w^2 = 1 \end{cases}$$

for $a, b \in K$ with $ab(a-b) \neq 0$. A Jacobi intersections elliptic curve is a twisted Jacobi intersections curve with $a = 1$. This curve is non-singular if and only if $ab(a-b) \neq 0$. The j-invariant is given by $j = 2^8 \frac{(a^2-ab+b^2)^3}{a^2b^2(a-b)^2}$.

Let $P = (u_1, v_1, w_1)$ and $Q = (u_2, v_2, w_2)$ be two finite points on $J_{a,b}$. The addition formula denoted by $P + Q = (u_3, v_3, w_3)$ with

$$u_3 = \frac{u_1v_2w_2 + u_2v_1w_1}{v_2^2 + au_2^2w_1^2},\ v_3 = \frac{v_1v_2 - au_1w_1u_2w_2}{v_2^2 + au_2^2w_1^2},\ w_3 = \frac{w_1w_2 - bu_1v_1u_2v_2}{v_2^2 + au_2^2w_1^2}.$$

If $P = Q$ and $[2]P = (u_3, v_3, w_3)$, then

$$u_3 = \frac{2u_1v_1w_1}{v_1^2 + au_1^2w_1^2},\ v_3 = \frac{v_1^2 - au_1^2w_1^2}{v_1^2 + au_1^2w_1^2},\ w_3 = \frac{w_1^2 - bu_1^2v_1^2}{v_1^2 + au_1^2w_1^2}.$$

The identity element is $(0, 1, 1)$. The additive inverse of a point $P = (u, v, w)$ is the point $-P = (-u, v, w)$.

2.2. **Jacobi quartic curve.** A Jacobi quartic curve over a field K is defined by

$$J_{d,\mu} \ : \ y^2 = dx^4 + 2\mu x^2 + 1$$

where $d, \mu \in K$ and discriminant $\Delta = 256(\mu^2 - d)^2 \neq 0$.

Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points on $J_{d,\mu}$, then $P + Q = R = (x_3, y_3)$, where

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 - dx_1^2x_2^2}, \ y_3 = \frac{(y_1y_2 + 2\mu x_1x_2)(1 + dx_1^2x_2^2)}{(1 - dx_1^2x_2^2)^2} + \frac{2dx_1x_2(x_1^2 + x_2^2)}{(1 - dx_1^2x_2^2)^2}$$

and $2P = R = (x_3, y_3)$, where

$$x_3 = \delta x_1, \ y_3 = \delta(\delta - y_1) - 1$$

where $\delta = 2y_1/(2 + 2\mu x_1^2 - y_1^2)$. The inverse of the point (x_1, y_1) on $J_{d,\mu}$ is $(-x_1, y_1)$.

2.3. **Frobenius map on elliptic curves.** Let $\mathbb{F}_q$ be a finite field with $char(\mathbb{F}_q) \neq 2$ and $\overline{\mathbb{F}}_q$ its algebraic closure. An elliptic curve E over $\mathbb{F}_q$ is defined as

$$E \ : \ y^2 = x^3 + a_2x^2 + a_4x + a_6$$

with the point at infinity O_E where $a_2, a_4, a_6 \in \mathbb{F}_q$. The q-th power Frobenius map π of E is defined as

$$\begin{aligned} \pi \ &: \ E \to E \\ &(x, y) \mapsto (x^q, y^q). \end{aligned}$$

By the Hasse's Theorem, the number of $\mathbb{F}_{q^k}$-rational points on E satisfieds $|\sharp E(\mathbb{F}_{q^k}) - q^k - 1| \leq 2\sqrt{q^k}$.

The characteristic polynomial $\chi_q \in \mathbb{Z}[x]$ of π is given by

$$\chi_q(x) = x^2 - tx + q, \ |t| \leq 2\sqrt{q},$$

which satisfies

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

for all $P \in E(\overline{\mathbb{F}}_q)$.

3. Frobenius map on Jacobi Curves

In this section, we introduce the Frobenius map on twisted Jacobi intersections curve and Jacobi quartic curve. At first, we consider a twisted Jacobi intersections curve $J_{a,b}$ over $\mathbb{F}_q$ with q elements. We define the q-power Frobenius endomorphism of $J_{a,b}$

$$\begin{aligned} \pi_{J_{a,b}} \ &: \ J_{a,b} \longrightarrow J_{a,b} \\ &(u, v, w) \longmapsto (u^q, v^q, w^q) \end{aligned}$$

Lemma 3.1. *Let K be a finite field with odd characteristic and $J_{a,b}$ be a twisted Jacobi intersections curve defined over K with $ab(a - b) \neq 0$. Then, every twisted Jacobi intersections curve $J_{a,b}$ is birationally equivalent over K to an elliptic curve E given by the Weierstrass equation*

$$E \ : \ y^2 = x(x - a)(x - b).$$

Proof. See [4] □

From lemma 3.1, one can see that there exists an elliptic curve E over $\mathbb{F}_q$ such that $J_{a,b}(\overline{\mathbb{F}}_q) \cong E(\overline{\mathbb{F}}_q)$. The isomorphism $\sigma : J_{a,b} \to E$ is definied to be

$$\sigma(u,v,w) = \Big(-\frac{a(w+1)}{v-1}, \frac{au}{v-1}(x-b)\Big).$$

The point $(u,v,w) = (0,1,1)$ on $J_{a,b}$ is mapped to the point at infinity O_E and $(u,v,w) = (0,-1,1)$ corresponds to $(x,y) = (b,0)$. The points $(u,v,w) = (0,-1,1)$ and $(u,v,w) = (0,-1,-1)$ correspond to the points $(x,y) = (a,0)$ and $(x,y) = (0,0)$ respectively.

The inverse transformation $\sigma^{-1} : E \to J_{a,b}$ is given by

$$\sigma^{-1}(x,y) = \Big(-\frac{2y}{x^2-ab}, \frac{x^2-2ax+ab}{x^2-ab}, \frac{x^2-2bx+ab}{x^2-ab}\Big).$$

Lemma 3.2. *Let $J_{a,b}$ be a twisted Jacobi intersections curve defined over $\mathbb{F}_q$ and E be the birational equivalent elliptic curve of $J_{a,b}$ over $\mathbb{F}_q$. Let $\sharp E(\mathbb{F}_q) = q+1-t$ and let σ be the birational map defined as above. Let π be the q-power Frobenius endomorphism over E. Define $\psi_{J_{a,b}} = \sigma^{-1}\pi\sigma$. Then*

(1) *$\psi_{J_{a,b}} \in End(J_{a,b})$, (i.e., $\psi_{J_{a,b}}$ is an endomorphism of $J_{a,b}$).*
(2) *For all $P \in J_{a,b}(\overline{\mathbb{F}}_q)$ we have*

$$\psi^2_{J_{a,b}}(P) - [t]\psi_{J_{a,b}}(P) + [q]P = O_{J_{a,b}}$$

Proof. First note that σ an isomorphism defined over $\mathbb{F}_q$, that π is an isogeny from E to itself defined over $\mathbb{F}_q$. Hence $\psi_{J_{a,b}}$ is an isogeny of $J_{a,b}$ to itself defined over $\mathbb{F}_q$. Therefore $\psi_{J_{a,b}}$ is a group homomorphism.

For $P \in J_{a,b}(\overline{\mathbb{F}}_q)$, let's denote $\sigma(P) = Q \in E(\overline{\mathbb{F}}_q)$. Then we have $(\pi^2 - t\pi + q)Q = O_E$. Hence,

$$\sigma^{-1}(\pi^2 - t\pi + q)\sigma(P) = O_{J_{a,b}}.$$

Therefore

$$\psi^2_{J_{a,b}}(P) - [t]\psi_{J_{a,b}}(P) + [q]P = O_{J_{a,b}}.$$

□

Theorem 3.3. *Let $J_{a,b}$ be a twisted Jacobi intersections defined over $\mathbb{F}_q$ with $\sharp J_{a,b}(\mathbb{F}_q) = q+1-t$. Then the Frobenius endomorphism of $J_{a,b}$ satisfies*

$$(\pi^2_{J_{a,b}} - t\pi_{J_{a,b}} + q)P = O_{J_{a,b}},$$

for all $P \in J_{a,b}(\overline{\mathbb{F}}_q)$.

Proof. Let E be the birational equivalent elliptic curve of $J_{a,b}$ defined over $\mathbb{F}_q$, and $\psi_{J_{a,b}}$ be the endomorphism of $J_{a,b}$ in lemma 3.2. By definition of $\psi_{J_{a,b}}$, for all $P = (u,v,w) \in J_{a,b}(\overline{\mathbb{F}}_q)$,

$$\begin{aligned}\psi(u,v,w) &= (\sigma^{-1}\pi)\Big(-\frac{a(w+1)}{v-1}, \frac{au}{v-1}(x-b)\Big) \\ &= \sigma^{-1}\Big(-\frac{a(w^q+1)}{(v^q-1)}, \frac{au^q}{(v^q-1)}(x^q-b)\Big) = (u^q, v^q, w^q),\end{aligned}$$

where $a, b \in \mathbb{F}_q$.

Hence we have for all $P \in J_{a,b}(\overline{\mathbb{F}}_q)$, $\psi_{J_{a,b}}(P) = \pi_{J_{a,b}}(P)$ and $\sharp E(\mathbb{F}_q) = \sharp J_{a,b}(\mathbb{F}_q) = q + 1 - t$. Hence by lemma 3.2, we can complete the proof of Theorem. □

Now we consider the Frobenius map on Jacobi quartic curve over a finite field $\mathbb{F}_q$. Let $J_{d,\mu}$ be a Jacobi quartic curve over $\mathbb{F}_q$. We define the q-th power Frobenius endomorhpism of $J_{d,\mu}$

$$\begin{aligned} \pi_{J_{d,\mu}} \ : \ J_{d,\mu} &\longrightarrow J_{d,\mu} \\ (x, y) &\longmapsto (x^q, y^q). \end{aligned}$$

In [1] if the Weierstrass elliptic curve $E : y^2 = x^3 + sx + t$ has a rational point of order 2 denoted $(\theta, 0)$, then it is birationally equivalent to the Jacobi quartic $J_{d,\mu}$ with $d = -(3\theta^2 + 4s)/16$ and $\mu = -3\theta/4$. The transformation $\tau : J_{d,\mu} \to E$ is given by

$$\tau(x, y) = \Big(\frac{2(y+1)}{x^2} - \frac{\theta}{2}, \frac{4(y+1)}{x^3} - \frac{3\theta}{x} \Big),$$

and the inverse transformation $\tau^{-1} : E \to J_{d,\mu}$ is given by

$$\tau^{-1}(x, y) = \Big(\frac{2(x-\theta)}{y}, \frac{(2x+\theta)(x-\theta)^2}{y^2} - 1 \Big).$$

The point $(0, 1)$ on $J_{d,\mu}$ is mapped to the point at infinity O_E and $(0, -1)$ corresponds to $(\theta, 1)$.

Lemma 3.4. *Let $J_{d,\mu}$ be a Jacobi quartic curve defined over $\mathbb{F}_q$ and E be the birational equivalent elliptic curve of $J_{d,\mu}$ over $\mathbb{F}_q$. Let $\sharp E(\mathbb{F}_q) = q+1-t$ and let τ be the birational map $J_{d,\mu}$ to E. Let π be the q-power Frobenius endomorphism over E. Define $\psi_{J_{d,\mu}} = \tau^{-1}\pi\tau$. Then*

(1) *$\psi_{J_{d,\mu}} \in End(J_{d,\mu})$,*
(2) *For all $P \in J_{d,\mu}(\overline{\mathbb{F}}_q)$ we have*

$$\psi^2_{J_{d,\mu}}(P) - [t]\psi_{J_{d,\mu}}(P) + [q]P = O_{J_{d,\mu}}.$$

Proof. Since τ is an isomorphism and π is an isogeny from E to itself over $\mathbb{F}_q$, $\psi_{J_{d,\mu}}$ is an isogeny of $J_{d,\mu}$ to itself defined over $\mathbb{F}_q$. Therefore $\psi_{J_{d,\mu}}$ is a group homomorphism.

For $P \in J_{d,\mu}(\overline{\mathbb{F}}_q)$, let's denote $\tau(P) = Q \in E(\overline{\mathbb{F}}_q)$. Then we have $(\pi^2 - [t]\pi + [q])Q = O_E$. Hence,

$$\tau^{-1}(\pi^2 - t\pi + q)\tau(P) = O_{J_{d,\mu}}.$$

Therefore

$$\psi^2_{J_{d,\mu}}(P) - [t]\psi_{J_{d,\mu}}(P) + [q]P = O_{J_{d,\mu}}.$$

□

Theorem 3.5. *Let $J_{d,\mu}$ be a Jacobi quartic curve defined over $\mathbb{F}_q$ with $\sharp J_{d,\mu}(\mathbb{F}_q) = q + 1 - t$. Then the Frobenius endomorphism of $J_{d,\mu}$ satisfies*

$$(\pi^2_{J_{d,\mu}} - t\pi_{J_{d,\mu}} + q)P = O_{J_{d,\mu}},$$

for all $P \in J_{d,\mu}(\overline{\mathbb{F}}_q)$.

Proof. Let E be the birational equivalent elliptic curve of $J_{d,\mu}$ defined over $\mathbb{F}_q$, and $\psi_{J_{d,\mu}}$ be the endomorphism of $J_{d,\mu}$ in lemma 3.4. Then, for all $P = (x, y) \in J_{d,\mu}(\overline{\mathbb{F}}_q)$, we have

$$\begin{aligned}\psi_{J_{d,\mu}}(x,y) &= (\tau^{-1}\pi)\Big(\frac{2(y+1)}{x^2} - \frac{\theta}{2},\ \frac{4(y+1)}{x^3} - \frac{3\theta}{x}\Big)\\ &= \tau^{-1}\Big(\frac{2(y^q+1)}{x^2} - \frac{\theta}{2},\ \frac{4(y^q+1)}{x^3} - \frac{3\theta}{x^q}\Big) = (x^q, y^q),\end{aligned}$$

where $\theta \in \mathbb{F}_q$.

□

4. Frobenius map on quadratic twists of Jacobi curves

In this section, we construct a Frobenius map on quadratic twist of twisted Jacobi curves according to the Frobenius map on Jacobi curves and apply the GLV method.

In general, the twisted Jacobi intersections $J_{a,b}$ defined over $\mathbb{F}_q$ is a quadratic twisted Jacobi intersections $J_{\overline{a},\overline{b}}$ for any $\overline{a}$, $\overline{b}$ satisfying $\frac{\overline{b}}{\overline{a}} = \frac{b}{a}$. Let

$$\begin{aligned}\phi \ :\ J_{a,b} &\ \rightarrow\ J_{\overline{a},\overline{b}}\\ (u,v,w) &\mapsto (\sqrt{\alpha}u, v, w)\end{aligned}$$

where $\alpha = \frac{a}{\overline{a}}$. If α is not a square in the field $K = \mathbb{F}_q$, then the map ϕ is an isomorphism form $J_{a,b}$ to $J_{\overline{a},\overline{b}}$ over $K(\sqrt{\alpha})$. A quadratic twist Jacobi intersections of $J_{a,b}$ is denoted by $J^t_{a,b}$.

Theorem 4.1. *Let $J_{a,b}$ be a twisted Jacobi intersections curve defined over $\mathbb{F}_q$ and $J^t_{a,b}$ be a quadratic twist of $J_{a,b}$. Let $\sharp J_{a,b}(\mathbb{F}_q) = q + 1 - t$ and let ϕ is an isomorphism from $J_{a,b}$ to $J^t_{a,b}$ over $\mathbb{F}_q(\sqrt{\alpha})$. Let $\pi_{J_{a,b}}$ be the q-power frobenius map on $J_{a,b}$. Define $\psi_{J^t_{a,b}} = \phi\pi_{J_{a,b}}\phi^{-1}$. Then for all $P \in J^t_{a,b}(\overline{\mathbb{F}}_q)$, we have*

$$\psi^2_{J^t_{a,b}}(P) - [t]\psi_{J^t_{a,b}}(P) + [q]P = O_{J^t_{a,b}}.$$

Proof. The proof is similar to Theorem 3.3, we omit it here. □

The GLV method gave efficiently computable homomorphism of elliptic curve where E is defined over $\mathbb{F}_q$ with the large characteristic. The following map can be used for the GLV method to point multiplication on twisted Jacobi intersections by extending the method in Galbraith et. al. [5].

Theorem 4.2. *Let $J_{a,b}$ be a twisted Jacobi intersections over $\mathbb{F}_q$ with $q+1-t$ points. Let $\pi_{J_{a,b}}$ be the q-power Frobenius map on $J_{a,b}$. Write $J^t_{a,b}$ for the quadratic twist of $J_{a,b}$ over $\mathbb{F}_{q^2}$ and let $\phi : J_{a,b} \rightarrow J^t_{a,b}$ be the twisting isomorphism defined over $\mathbb{F}_{q^4}$. Let $\psi_{J^t_{a,b}} = \phi\pi_{J_{a,b}}\phi^{-1}$. Let $r|\sharp J^t_{a,b}(\mathbb{F}_{q^2})$ be a prime such that $r > 2q$. Let $P \in J^t_{a,b}(\mathbb{F}_{q^2})[r]$. Then $\psi_{J^t_{a,b}}(P) = [\lambda]P$ where $\lambda \in \mathbb{Z}/r\mathbb{Z}$ satisfies $\lambda^2 + 1 \equiv 0 \pmod r$. Also, we have $\psi_{J^t_{a,b}}(P)^2 + P = O_{J^t_{a,b}}$.*

Proof. Since ϕ and $\pi_{J_{a,b}}$ are group homomorphisms it follows that $\psi_{J^t_{a,b}}$ is too. We have $J_{a,b}(\mathbb{F}_{q^4}) \cong J^t_{a,b}(\mathbb{F}_{q^4})$ as groups.

If $r|\sharp J^t_{a,b}(\mathbb{F}_{q^2})$ is prime such that $r > 2q$, then $r \nmid \sharp J_{a,b}(\mathbb{F}_{q^2}) = (q+1-t)(q+1+t)$ and $r|\sharp J^t_{a,b}(\mathbb{F}_{q^4}) = \sharp J_{a,b}(\mathbb{F}_{q^2})\sharp J^t_{a,b}(\mathbb{F}_{q^2})$ but $r^2|\sharp J^t_{a,b}(\mathbb{F}_{q^4})$. This implies that for $P \in J^t_{a,b}(\mathbb{F}_{q^2})[r]$, $\psi_{J_{a,b}}(P)$ belongs to $J^t_{a,b}(\mathbb{F}_{q^2})[r]$. It follows that for for $P \in J^t_{a,b}(\mathbb{F}_{q^2})[r]$, there exists $\lambda \in \mathbb{Z}$ such that $\psi_{J^t_{a,b}}(P) = [\lambda]P$.

By definition,

$$\psi_{J^t_{a,b}}(u,v,w) = (\phi\pi_{J^t_{a,b}})(u/\sqrt{\alpha}, v, w) = \phi(u^q/\sqrt{\alpha}^q, v^q, w^q) = (\sqrt{\alpha}^{1-q}u^q, v^q, w^q)$$

for $P = (u,v,w) \in J^t_{a,b}(\overline{\mathbb{F}}_q)$. Also, since $u^{q^2} = u$, $v^{q^2} = v$, $w^{q^2} = w$ for $u, v, w \in \mathbb{F}_{q^2}$, we have

$$\psi^2_{J^t_{a,b}}(u,v,w) = \left(\alpha^{\frac{1-q^2}{2}}u, v, w\right) = (-u, v, w) = -(u,v,w).$$

where $\alpha \in \mathbb{F}_{q^2}$ (i.e., $\alpha^{q^2} = \alpha$) and $\sqrt{\alpha} \notin \mathbb{F}_{q^2}$ (and so, $\sqrt{\alpha}^{q^2} = -\sqrt{\alpha}$). Therefore,

$$\psi^2_{J^t_{a,b}}(P) + P = O_{J^t_{a,b}}.$$

□

Now we consider a Frobenius map on quadratic twist of Jacobi quartic curve and apply the GLV method. The quadratic twist of a Jacobi quartic curve $J_{d,\mu}$ is given by

$$J_{d,\mu,\delta} : y^2 = dx^4 + 2\mu\delta^2x^2 + \delta^4,$$

where $\delta \in \mathbb{F}_{q^m}$. The corresponding isomorphism $\rho : J_{d,\mu} \to J_{d,\mu,\delta}$ defined over $\mathbb{F}_{q^m}$ is give by $\rho(x,y) = (\delta x, \delta^2 y)$. A quadratic twist of a Jacobi quartic $J_{d,\mu,\delta}$ is denoted by $J^t_{d,\mu}$.

Theorem 4.3. *Let $J_{d,\mu}$ be a Jacobi quartic curve defined over $\mathbb{F}_q$ and $J^t_{d,\mu}$ be a quadratic twist of $J_{d,\mu}$. Let $\sharp J_{d,\mu}(\mathbb{F}_q) = q+1-t$ and let ρ is an isomorphism from $J_{d,\mu}$ to $J^t_{d,\mu}$. Let $\pi_{J_{d,\mu}}$ be the q-power frobenius map on $J_{d,\mu}$. Define $\psi_{J^t_{d,\mu}} = \rho\pi_{J_{d,\mu}}\rho^{-1}$. Then for all $P \in J^t_{d,\mu}(\overline{\mathbb{F}}_q)$, we have*

$$\psi^2_{J^t_{d,\mu}}(P) - [t]\psi_{J^t_{d,\mu}}(P) + [q]P = O_{J^t_{d,\mu}}.$$

Proof. The proof is similar to Theorem 3.5, we omit it here. □

Theorem 4.4. *Let $J_{d,\mu}$ be a Jacobi quartic curve over $\mathbb{F}_q$ with $q+1-t$ points. Let $\pi_{J_{d,\mu}}$ be the q-power Frobenius map on $J_{d,\mu}$. Write $J^t_{d,\mu}$ for the quadratic twist of $J_{d,\mu}$ over $\mathbb{F}_{q^2}$ and let $\rho : J_{d,\mu} \to J^t_{d,\mu}$ be the twisting isomorphism defined over $\mathbb{F}_{q^4}$. Let $\psi_{J_{d,\mu}} = \rho\pi_{J_{d,\mu}}\rho^{-1}$. Let $r|\sharp J^t_{d,\mu}(\mathbb{F}_{q^2})$ be a prime such that $r > 2q$. Let $P \in J^t_{d,\mu}(\mathbb{F}_{q^2})[r]$. Then $\psi_{J^t_{d,\mu}}(P) = [\lambda]P$ where $\lambda \in \mathbb{Z}/r\mathbb{Z}$ satisfies $\lambda^2+1 \equiv 0 \pmod r$. Also, we have $\psi_{J^t_{d,\mu}}(P)^2 + P = O_{J^t_{d,\mu}}$.*

Proof. The proof is similar to Theorem 4.2. Since ρ and $\pi_{J_{d,\mu}}$ are group homomorphisms it follows that $\psi_{J^t_{d,\mu}}$ is too. We have $J_{d,\mu}(\mathbb{F}_{q^4}) \cong J^t_{d,\mu}(\mathbb{F}_{q^4})$ as groups.

For $P = (x,y) \in J^t_{d,\mu}(\overline{\mathbb{F}}_q)$, we have

$$\psi_{J^t_{d,\mu}}(x,y) = (\phi\pi_{J^t_{d,\mu}})(x/\delta, y/\delta^2) = \phi(x^q/\delta^q, y^q/\delta^q) = (\delta^{1-q}x^q, \delta^{2(1-q)}y^q).$$

Also, since $x^{q^2} = x$, $y^{q^2} = y$ for $x, y \in \mathbb{F}_{q^2}$, we have

$$\psi^2_{J^t_{d,\mu}}(x,y) = \left(\delta^{1-q^2}x^{q^2}, \delta^{2(1-q^2)}y^{q^2}\right) = (-x,y) = -(x,y).$$

where $\delta^2 \in \mathbb{F}_{q^2}$ and $\delta \notin \mathbb{F}_{q^2}$. Therefore, $\psi^2_{J^t_{d,\mu}}(P) + P = O_{J^t_{d,\mu}}$. □

5. Conclusion

This paper presented the Frobenius endomorphism of Jacobi curves over a finite field. In particular, we considered twisted Jacobi intersections curve and Jacobi quartic curve in Jacobi curves. Based on it, we constructed a Frobenius map defined on the quadratic twist of Jacobi curves and showed how to it to accelerate the scalar multiplication on curves.

References

[1] O. Billet, M. Joye, The jocobi model of an elliptic curve and side-channel analysis, AAEECC 2003, LNCS **2643**, 34–42, 2003.

[2] D. V. Chudnovsky, and G. V. Chudnovsky, Sequences of numbers gnerated by addition in formal groups and new primality and factorization tests, Advances in Applied Mathematics 7(1986), 385–434.

[3] H. M. Edwards, *A normal form for elliptic curves*, Bull. Am. Math. Soc., New Ser. 44(3) (2007), 393–422

[4] R. Feng, M. Nie and H. Wu, *Twisted Jacobi Intersections Curves*, Theoretical Computer Science **494**(8), 24–35, 2013.

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

[6] R. P. Gallant, R. J. Lambert and S. A. Vanstone, *Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms*, In J. Kilian (ed.), CRYPTO 2001, Springer LNCS 2139 (2001), 190–200.

[7] J. Guajardo and C. Paar, *Itoh-tusji version in standard basis and its applicaiton in cryptography and codes*, Design, Codes and Cryptography 25 (2002), no. 2, 207-216.

[8] G. B. Huff, *Diophantine problems in geometry and elliptic ternary forms*, Duke Math. J. 15 (1948), 443–453.

[9] T. Iijima, K. Matsuo, J. Chao and S. Tsujii, *Construction of Frobenius Maps of Twists Elliptic Curves and its Application to Elliptic Scalar Multiplication*, in SCIS 2002, IEICE Japan, January 2002, 699–702.

[10] M. Joye, and J. Quisquater, *Hessian elliptic curves and side-channel attacks*, In Workshop on Cryptographic Hardware and Embedded systems proceedings, LNCS vol 2162, pages 402–410, springer, 2001.

[11] N. Koblitz, *Elliptic curve cryptosystems*, Math. Comp. 48 (1987), 203–209.

[12] V. S. Miller, *Use of elliptic curves in cryptography*, In H. C. Williams, editor, Advances in Cryptology-CRYPTO'85, Lect. Notes Comput. Sci. 218 (1986), 417–426.

[13] D. Yong and G. Feng, *High speed modular divider based on GCD algorithm over GF(2m)*, Journal of communications 29 (2008), no. 10, 199–204.

Department of Mathematics Education, Daegu National University of Education, Daegu 705-715, Korea

E-mail address: gysohn@dnue.ac.kr