Advanced Studies in Contemporary Mathematics
30 (2020), No. 1, pp. 135 – 143

www.jangjeon.or.kr
http://dx.doi.org/10.17777/ascm2020.30.1.135

EFFICIENT COMPUTABLE HOMOMORPHISMS ON HESSIAN CURVES

GYOYONG SOHN

Abstract. This paper presents Frobenius endomorphisms on generalized Hessian curves and twisted Hessian curves. It gives an efficient computable homomorphism to compute the point multiplication on Hessian curve over a finite field. As an application, we describe the GLV method combied with the Frobenius endomorphism over the curve to speed up the scalar multiplication.

2010 Mathematics Subject Classification. 94A55, 11T71.

Keywords and phrases. Hessian Curve, Frobenius Endomorphism, Scalar Multiplication

1. Introduction

Elliptic curve cryptography was independently proposed by Koblitz [14] and Miller [15] 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[20, 8].

There are numerous investigations of fast scalar point multiplication on elliptic curves over large prime fields or binary fields [1, 11, 7, 17, 18]. For elliptic curves, the scalar multiplication can be done with various methods(a good reference is [1]). If an elliptic curve admits an efficient endomorphism, it can be used to speed up scalar multiplication. In [11], Iijima, Matsuo, Chao and Tsujii presented an efficiently computable homomorphism on elliptic curves using the Frobenius 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 [7].

There are several models of elliptic curves to provide the efficient computation and implement for cryptography in recent years [4, 10]. In [12], Joye and Quisquater proposed Hessian elliptic curves with the formulae of point addition and dubling. Farashahi and Joye presented the efficient arithmetic on generalized Hessian curves[5]. The arithmetic formulae of twised Hessian curve is presented in [2].

In this paper, we present the Frobenius endomorphisms on generalized Hessian curves and twisted Hessian curves. It gives a scalar multiplication algorithm on Hessian curves using Frobenius expansion. Applying the Frobenius endomorphism on Hessian curve, we construct a Frobenius map defined on the quadratic twist of a Hessian curve. To speed up the scalar multiplication on Hessian curves, we use the GLV method combined with the Frobenius endomorphism over the curve.

This paper is organized as follows. Section 1 illustrates some basic notions on Hessian curves and twisted Hessian curves. Second section gives the birational equivalence between Hessian curve and Weierstrass equation of elliptic curve. We also describe Frobenius endomorphism for Hessian curves and some basic properties.

2. Premiminaries

2.1. **Hessian Curves.** Let K be a field with $char(K) \neq 2$ and $\overline{K}$ its algebraic closure. A *Hessian curve* over K is defined by the symmetric cubic equation

$$H_d \ : \ x^3 + y^3 + 1 = dxy,$$

where $d \in K$ and $d^3 \neq 27$ in [9]. Furthermore, the generalized form of Hessian curves, called twisted Hessian as well, has been studied in [2, 5]. A *generalized Hessian curve* $H_{c,d}$ over K is defined by the equation

$$H_{c,d} \ : \ x^3 + y^3 + c = dxy,$$

where $c, d \in K$ with $c \neq 0$ and $d^3 \neq 27c$. A Hessian curve is a generalized Hessian curve with $c = 1$. The j-invariant is given by $j = \frac{1}{c}\left(\frac{d(d^3+36c)}{d^3-9c}\right)^3$.

Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two finite points on $H_{c,d}$. The addition formula denoted by $P + Q = (x_3, y_3)$ with

$$x_3 = \frac{y_1^2 x_2 - y_2^2 x_1}{x_2 y_2 - x_1 y_1} \text{ and } y_3 = \frac{x_1^2 y_2 - x_2 y_1}{x_2 y_2 - x_1 y_1}.$$

If $P = Q$ and $[2]P = (x_3, y_3)$, then

$$x_3 = \frac{y_1(c - x_1^3)}{x_1^3 - y_1^3} \text{ and } y_3 = \frac{x_1(c - y_1^3)}{x_1^3 - y_1^3}.$$

Moreover, the additive inverse of a point (x_1, y_1) on $H_{c,d}$ is the point (y_1, x_1).

A *generalized Hessian curve* in projective coordinate is defined by the equation

$$\mathcal{H}_{c,d} \ : \ X^3 + Y^3 + cZ^3 = dXYZ,$$

where $c, d \in K$ with $c \neq 0$ and $d^3 \neq 27c$. The curve $\mathcal{H}_{c,d}$ has the points $(1 : -\omega : 0)$ of order 3, where ω is a primitive cube root of 1 in K. The neutral element of the group K-rational points of $\mathcal{H}_{c,d}$ is the point at infinity $(1 : -1 : 0)$ that we denote by $\mathcal{O}_{\mathcal{H}_{c,d}}$. For the point $P = (X_1 : Y_1 : Z_1)$ on $\mathcal{H}_{c,d}$, we have $-P = (Y_1 : X_1 : Z_1)$.

The obtained point addition and doubling formulae on generalized Hessian curves in projective coordinates as follows: Let $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$ be two points on $\mathcal{H}_{c,d}$, then $P + Q = R = (X_3 : Y_3 : Z_3)$, where

$$X_3 = X_2 Z_2 Y_1^2 - X_1 Z_1 Y_2^2, Y_3 = Y_2 Z_2 X_1^2 - Y_1 Z_1 X_2^2, Z_3 = X_2 Y_2 Z_1^2 - X_1 Y_1 Z_2^2$$

and $[2]P = R = (X_3 : Y_3 : Z_3)$, where

$$X_3 = Y_1(cZ_1^3 - X_1^3),\ Y_3 = X_1(Y_1^3 - cZ_1^3),\ Z_3 = Z_1(X_1^3 - Y_1^3).$$

The cost of point addition algorithms is 12**M** [3, 12, 19]. In this case, the computational cost of point addition is 4**M**, 3**M**, or 2**M** correspond to use of 3, 4 or 6 processors, respectively. The point addition formulae are complete if the difference of all pairs of points on $H_{c,d}$ is not equal the identity. In [3], the cost of point doubling is 6**M**+3**S**+1**D**, where **D** is the cost of a multiplication by the constant c.

2.2. **Twisted Hessian Curves.** A *twist Hessian curve* over a field K is defined by the equation

$$H_{a,d}^t\ :\ ax^3 + y^3 + 1 = dxy,$$

where $a, d \in K$. It has a specified point $(0, -1)$. The sum of two finite points (x_1, y_1) and (x_2, y_2) on $H_{a,d}^t$ is given by (x_3, y_3), where

$$x_3 = \frac{x_1 - y_1^3 x_1}{a y_1 x_1^3 - y_1} \text{ and } y_3 = \frac{y_1^3 - a x_1^3}{a y_1 x_1^3 - y_1}.$$

A twisted Hessian curve in projective coordinate over K is defined by

$$\mathcal{H}_{a,d}^t\ :\ aX^3 + Y^3 + Z^3 = dXYZ,$$

where $a, d \in K$ and $a(27a - d^3) \neq 0$. The neutral element of $\mathcal{H}_{a,d}^t(K)$ is the point at infinity $(0 : -1 : 1)$ that we denote by $\mathcal{O}_{\mathcal{H}_{a,d}^t}$. The special case $a = 1$ of a twisted Hessian curve is simply a Hessian curve. For the point $P = (X_1 : Y_1 : Z_1)$ on $\mathcal{H}_{a,d}^t$, we have $-P = (X_1 : Z_1 : Y_1)$.

The point addition on twisted Hessian curves in projective coordinate as follows: Let $P = (X_1, Y_1, Z_1)$ and $Q = (X_2, Y_2, Z_2)$ be two points on $\mathcal{H}_{a,d}^t$, then $P + Q = R = (X_3, Y_3, Z_3)$ where,

$$X_3 = Z_2^2 X_1 Z_1 - Y_1^2 X_2 Y_2,\ Y_3 = Y_2^2 Y_1 Z_1 - a X_1^2 X_2 Z_2,$$
$$Z_3 = a X_2^2 X_1 Y_1 - Z_1^2 Y_2 Z_2.$$

The above formula is described by the rotated addition law in [2]. The cost of point addition algorithm is 12**M** [2].

3. Frobenius Endomorphism on (twisted) Hessian curves

In this section, we construct the Frobenius endomorphisms on a generalized Hessian curve and twisted Hessian curve. It gives an efficient computable homomorphism to compute the point multiplication elliptic curve.

Every elliptic curve can be written in Weierstrass form, only those that contain poins of order 3 can be written in Hessian curve and twisted Hessian curve.

Theorem 3.1. *Let E be an elliptic curve over a field K. If the group $E(K)$ has a point of order 3 then E is isomorphism over $\overline{K}$ to a generalized Hessian curve. Moreover, if K has an element ω with $\omega^2 + \omega + 1 = 0$, then the group $E(K)$ has a point of order 3 if and only if E is isomorphic over K to a generalized Hessian curve.*

Proof. See [5]. □

We note that the elliptic curve E over a field K has a point of order 3 if and only if it has a Weierstrass model

$$E_{a_1,a_3} : y^2z + a_1xyz + a_3yz^2 = x^3. \tag{1}$$

For this, see [13]. In [2], E_{a_1,a_3} is called *triangular curve* because its Newton polygon is a triangle of minimum area.

From Theorem 3.1, if the characteristic of a field K is not 3, the generalized Hessian curve $\mathcal{H}_{c,d}$ is isomorphic over $K(\omega)$ to the Weierstrass curve E_{a_1,a_2} with $a_1 = d/3$, $a_3 = (d^3 - 27c)/3^6$.

Every elliptic curve in Weierstrass form E_{a_1,a_2} via the map $(x, y, z) \mapsto (X, Y, Z)$ defined by

$$X = \omega a_1x + (\omega - 1)y + (2\omega + 1)a_3z,$$
$$Y = -(\omega + 1)a_1x - (\omega + 2)y - (2\omega + 1)a_3z, \; Z = x.$$

is birationally isomorphic to the generalized Hessian curve $\mathcal{H}_{c,d}$ over $K(\omega)$. The inverse map $\mathcal{H}_{c,d} \to E_{a_1,a_3}$, $(X, Y, Z) \mapsto (x, y, z)$ is given by

$$x = Z, \; y = -\frac{1}{3}(X + Y + a_1Z), \; z = -\frac{1}{3a_3}\Big(wX + \frac{1}{w}Y + a_1Z\Big). \tag{2}$$

Now we denote the map $\mathcal{H}_{c,d} \to E_{a_1,a_3}$ by σ and σ^{-1} denotes its inverse transformation.

Remark 3.2. Consider the elliptic curve E_{a_1,a_3} defined in (1). If $p \neq 3$ and $a_1^3 - 27a_3$ is a cube in K, we let $c = 1$ and $d = 3(a_1 + 2\delta)/(a_1 - \delta)$, where $\delta^3 = a_1^3 - 27a_3$. Then the map $(x, y, z) \mapsto (X, Y, Z)$ given by

$$X = (2a_1 + \delta)x + 3y + 3a_3z, \; Y = -(a_1 - \delta)x - 3y,$$
$$Z = -(a_1 - \delta)x - 3a_3z$$

is an isomorphism over K between E_{a_1,a_3} and $\mathcal{H}_{c,d}$. The map $\sigma : (X, Y, Z) \mapsto (x, y, z)$ is given by

$$x = \frac{1}{3\delta}(X + Y + Z), \; y = -\frac{(a_1 - \delta)}{9\delta}\Big(X + \frac{d}{3}Y + Z\Big),$$
$$z = -\frac{(a_1 - \delta)}{9a_3\delta}\Big(X + Y + \frac{d}{3}Z\Big).$$

Now we define the q-power Frobenius endomorphism π of E_{a_1,a_3}

$$\pi \; : \; E_{a_1,a_3} \to E_{a_1,a_3}, \; (x, y) \mapsto (x^q, y^q).$$

We construct an endomorphism of the generalized Hessian curve over a finite field.

Lemma 3.3. *Let $\mathcal{H}_{c,d}$ be a generalized Hessian curve defined over a finite field $\mathbb{F}_q$ and E_{a_1,a_3} be the birational equivalent elliptic curve of $\mathcal{H}_{c,d}$ over $\mathbb{F}_q$. Let $\sharp E_{a_1,a_3}(\mathbb{F}_q) = q+1-t$, $|t| \leq 2\sqrt{q}$ and let σ be the birational map defined as above. Let π be the q-power Frobenius endomorphism over E_{a_1,a_3}. Define $\psi_{\mathcal{H}_{c,d}} = \sigma^{-1}\pi\sigma$. Then*

(1) *$\psi_{\mathcal{H}_{c,d}} \in End(\mathcal{H}_{c,d})$, (i.e., $\psi_{\mathcal{H}_{c,d}}$ is an endomorphism of $\mathcal{H}_{c,d}$).*

(2) *For all $P \in \mathcal{H}_{c,d}(\overline{\mathbb{F}}_q)$ we have*

$$\psi^2_{\mathcal{H}_{c,d}}(P) - [t]\psi_{\mathcal{H}_{c,d}}(P) + [q]P = \mathcal{O}_{\mathcal{H}_{c,d}}.$$

Proof. First note that σ is an isomorphism defined over a finite field $\mathbb{F}_q$, that π is an isogeny from E_{a_1,a_3} to itself defined over $\mathbb{F}_q$. Hence $\psi_{\mathcal{H}_{c,d}}$ is an isogeny of $\mathcal{H}_{c,d}$ to itself defined over $\mathbb{F}_q$. Therefore $\psi_{\mathcal{H}_{c,d}}$ is a group homomorphism.

For $P \in \mathcal{H}_{c,d}(\overline{\mathbb{F}}_q)$, let's denote $\sigma(P) = Q \in E_{a_1,a_3}(\overline{\mathbb{F}}_q)$. Then the characteristic polynomial $\chi_q(x) = x^2 - tx + q$, $|t| \leq 2\sqrt{q}$ of the q-power Frobenius endomorphism π of E_{a_1,a_3} satisfies $(\pi^2 - [t]\pi + [q])P = \mathcal{O}_{E_{a_1,a_3}}$ for all $P \in E_{a_1,a_3}(\overline{\mathbb{F}}_q)$. Hence,

$$\sigma^{-1}(\pi^2 - [t]\pi + [q])\sigma(P) = \mathcal{O}_{\mathcal{H}_{c,d}}.$$

Therefore

$$\psi^2_{\mathcal{H}_{c,d}}(P) - [t]\psi_{\mathcal{H}_{c,d}}(P) + [q]P = \mathcal{O}_{\mathcal{H}_{c,d}}.$$

□

Now we define the q-power Frobenius endomorphism of $\mathcal{H}_{c,d}$

$$\widehat{\pi} \ : \ \mathcal{H}_{c,d} \to \mathcal{H}_{c,d}, \ (X, Y, Z) \mapsto (X^q, Y^q, Z^q).$$

Theorem 3.4. *Let $\mathcal{H}_{c,d}$ be a generalized Hessian curve defined over a finite field $\mathbb{F}_q$ and $\sharp\mathcal{H}_{c,d}(\mathbb{F}_q) = q + 1 - t$. Then the Frobenius endomorphism $\widehat{\pi}$ of $\mathcal{H}_{c,d}$ satisfies*

$$(\widehat{\pi}^2 - [t]\widehat{\pi} + [q])P = O_{\mathcal{H}_{c,d}},$$

for all $P \in \mathcal{H}_{c,d}(\overline{\mathbb{F}}_q)$.

Proof. Let E_{a_1,a_3} be the birational equivalent elliptic curve of $\mathcal{H}_{c,d}$ defined over $\mathbb{F}_q$, and $\psi_{\mathcal{H}_{c,d}}$ be the endomorphism of $\mathcal{H}_{c,d}$ in Lemma 3.3. By definition of $\psi_{\mathcal{H}_{c,d}}$, for all $P = (X, Y, Z) \in \mathcal{H}_{c,d}(\overline{\mathbb{F}}_q)$,

$$\begin{aligned}
\psi_{\mathcal{H}_{c,d}}(X, Y, Z) &= (\sigma^{-1}\pi\sigma)(X, Y, Z) \\
&= (\sigma^{-1}\pi)\Big(Z, -\frac{1}{3}(X + Y + a_1Z), -\frac{1}{3a_3}\Big(\omega X + \frac{1}{\omega}Y + a_1Z\Big)\Big) \\
&= \sigma^{-1}\Big(Z^q, -\frac{1}{3^q}(X^q + Y^q + a_1^qZ^q), -\frac{1}{3^q a_3^q}\Big(\omega^q X^q + \frac{1}{\omega^q}Y^q + a_1^q Z^q\Big)\Big) \\
&= (X^q, Y^q, Z^q),
\end{aligned}$$

where $a_1, a_3, \omega \in \mathbb{F}_q$.

Hence we have for all $P \in \mathcal{H}_{c,d}(\overline{\mathbb{F}}_q)$, $\psi_{\mathcal{H}_{c,d}}(P) = \widehat{\pi}(P)$ and $\sharp E_{a_1,a_3}(\mathbb{F}_q) = \sharp\mathcal{H}_{c,b}(\mathbb{F}_q) = q + 1 - t$. Hence by Lemma 3.3, we can complete the proof of Theorem. □

Now we consider the Frobenius endomorphism on twisted Hessian curves over a finite field $\mathbb{F}_q$. Each twisted Hessian curve over a finite field $\mathbb{F}_q$ has a rational point of order 3. Every elliptic curve over $\mathbb{F}_q$ with a point of order 3 is isomorphic to a twisted Hessian curve.

Lemma 3.5. *Let a, d be elements of a field K such that $a(27a - d^3) \neq 0$. Let K be a field with a primitive cube root of 1. Then every twisted Hessian curves $H^t_{\bar{a},\bar{d}}$ with $\bar{a} = d^3 - 27a, \bar{b} = 3d$ is birationally equivalent over K to an Weierstrass equation $E_{d,a}$ in* (1).

Proof. See Theorem 5.3 in [2]. □

From Lemma 3.5, one can see that there exists an Weierstrass equation $E_{d,a}$ over K such that $\mathcal{H}^t_{\bar{a},\bar{d}}(\overline{K}) \cong E_{d,a}(\overline{K})$. Let ω be a primitive root of 1 in K and μ be the isomorphism

$$\mu \ : \ E_{d,a} \to \mathcal{H}^t_{\bar{a},\bar{d}}, \ (x,y,z) \mapsto (X,Y,Z),$$

where

$$X = x, \ Y = \omega(y + dx + az) - \omega^2 y - az, \ Z = \omega^2(y + dx + az) - \omega y - az.$$

The netural point $(0,0,1)$ is mapped to $(0,-\omega,1)$. The inverse transformation is given by

$$\mu^{-1} \ : \ \mathcal{H}^t_{\bar{a},\bar{d}} \to E_{d,a}, \ (X,Y,Z) \mapsto (x,y,z),$$

where

$$x = X, \ y = -\frac{d}{3}(dX + \omega Y + \omega^2 Z), \ z = -\frac{1}{3a}(dX + Y + Z).$$

The following lemma gives an endomorphism of twisted Hessian curve over a finite field $\mathbb{F}_q$.

Lemma 3.6. *Let $\mathcal{H}^t_{\bar{a},\bar{d}}$ be a twisted Hessian curve defined over a finite field $\mathbb{F}_q$ and $E_{d,a}$ be the birational equivalent elliptic curve of $\mathcal{H}^t_{\bar{a},\bar{d}}$ over $\mathbb{F}_q$. Let $\sharp E_{d,a}(\mathbb{F}_q) = q + 1 - t$, $|t| \le 2\sqrt{q}$ and let μ be the birational map defined as above. Let π be the q-power Frobenius endomorphism over $E_{d,a}$. Define $\psi_{\mathcal{H}^t_{\bar{a},\bar{d}}} = \mu^{-1}\pi\mu$. Then*

(1) *$\psi_{\mathcal{H}^t_{\bar{a},\bar{d}}} \in End(\mathcal{H}^t_{\bar{a},\bar{d}})$, (i.e., ψ is an endomorphism of $\mathcal{H}^t_{\bar{a},\bar{d}}$).*

(2) *For all $P \in \mathcal{H}^t_{\bar{a},\bar{d}}(\overline{\mathbb{F}}_q)$ we have*

$$\psi^2_{\mathcal{H}^t_{\bar{a},\bar{d}}}(P) - [t]\psi_{\mathcal{H}^t_{\bar{a},\bar{d}}}(P) + [q]P = \mathcal{O}_{\mathcal{H}^t_{\bar{a},\bar{d}}}$$

Proof. The proof is similar to that of Lemma 3.3, we omit it here. □

Theorem 3.7. *Let $\mathcal{H}^t_{\bar{a},\bar{d}}$ be a twisted Hessian curve defined over a finite field $\mathbb{F}_q$ and $\sharp\mathcal{H}^t_{\bar{a},\bar{d}}(\mathbb{F}_q) = q + 1 - t$. Then the Frobenius endomorphism $\widetilde{\pi}$ of $\mathcal{H}^t_{\bar{a},\bar{d}}$ satisfies*

$$(\widetilde{\pi}^2 - [t]\widetilde{\pi} + [q])P = \mathcal{O}_{\mathcal{H}^t_{\bar{a},\bar{d}}},$$

for all $P \in \mathcal{H}^t_{\bar{a},\bar{d}}(\overline{\mathbb{F}}_q)$.

Proof. Let $E_{d,a}$ be the birational equivalent elliptic curve of $\mathcal{H}^t_{\bar{a},\bar{d}}$ defined over $\mathbb{F}_q$, and $\psi_{\mathcal{H}^t_{\bar{a},\bar{d}}}$ be the endomorphism of $\mathcal{H}^t_{\bar{a},\bar{d}}$ in Lemma 3.6. By definition of $\psi_{\mathcal{H}^t_{\bar{a},\bar{d}}}$, for all $P = (X,Y,Z) \in \mathcal{H}^t_{\bar{a},\bar{d}}(\overline{\mathbb{F}}_q)$,

$$\begin{aligned}
\psi_{\mathcal{H}^t_{a,d}}(X,Y,Z) &= (\mu^{-1}\pi\mu)(X,Y,Z) \\
&= (\mu^{-1}\pi)\Big(X, -\frac{d}{3}(dX + \omega Y + \omega^2 Z), -\frac{1}{3a}(dX + Y + Z)\Big) \\
&= \mu^{-1}\Big(X^q, -\frac{d^q}{3^q}(d^q X^q + \omega^q Y^q + \omega^{2q} Z^q), -\frac{1}{3^q a^q}(d^q X^q + Y^q + Z^q)\Big) \\
&= (X^q, Y^q, Z^q),
\end{aligned}$$

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

Hence we have for all $P \in \mathcal{H}^t_{\bar{a},\bar{d}}(\overline{\mathbb{F}}_q)$, $\psi_{\mathcal{H}^t_{\bar{a},\bar{d}}(\mathbb{F}_q)}(P) = \widetilde{\pi}(P)$ and $\sharp E_{d,a}(\mathbb{F}_q) = \sharp\mathcal{H}^t_{\bar{a},\bar{d}}(\mathbb{F}_q) = q + 1 - t$. Hence by Lemma 3.6, we can complete the proof of Theorem. □

We present scalar multiplication for special types of ellitpic curves with efficient computable endomorphism of generalized Hessian curves. The GLV method gave efficiently computable homomorphism of elliptic curve where E is defined over $\mathbb{F}_q$ with the large characteristic.

If the characteristic of $\mathbb{F}_q$ is not 2, we can simplify the equation by completing the square. Then the Weierstarss form of (1) gives an elliptic curve equation of the following form :

$$E' \ : \ y^2 = 4x^3 + a_1^2x^2 + 2a_1a_3x + a_3^2, \tag{3}$$

where $a_1, a_3 \in \mathbb{F}_q$. In order to give fast formulas for curve arithmetic, it is desirable for the curves that we consider to have twists. Let u be a nonsquare in $\mathbb{F}_{q^2}$. Define $A = ua_1^2$, $B = 2u^2a_1a_3$, and $C = u^3a_3^2$. The quadratic twist of (3) is

$$E^t \ : \ y^2 = 4x^3 + Ax^2 + Bx + C.$$

For $P = (x, y) \in E^t$, we have $-P = (x, -y)$. The corresponding isomorphism $\varphi : E' \to E^t$ defined over $\mathbb{F}_{q^2}$ is given by

$$\varphi(x, y, z) = (ux, \sqrt{u}^3 y, z) \tag{4}$$

and is defined over $\mathbb{F}_{q^4}$.

Theorem 3.8. *Let $\mathcal{H}_{c,d}$ be a generalized Hessian curve over $\mathbb{F}_q$ with $q + 1 - t$ points. Let $\hat{\pi}$ be the q-power Frobenius map on $\mathcal{H}_{c,d}$. Write E^t for the quadratic twist of E' over $\mathbb{F}_{q^2}$ and let $\phi : \mathcal{H}_{c,d} \to E^t$ be the twisting isomorphism defined over $\mathbb{F}_{q^4}$. Let $\psi = \phi\hat{\pi}\phi^{-1}$. Let $r|\sharp E^t(\mathbb{F}_{q^2})$ be a prime such that $r > 2q$. Let $P \in E^t(\mathbb{F}_{q^2})[r]$. Then $\psi(P) = [\lambda]P$ where $\lambda \in \mathbb{Z}/r\mathbb{Z}$ satisfies $\lambda^2 + 1 \equiv 0$ (mod r). Also, we have $\psi(P)^2 + P = \mathcal{O}_{E^t}$.*

Proof. Since ϕ and $\hat{\pi}$ are group homomorphisms it follows that ψ is too. We have $\mathcal{H}_{c,d}(\mathbb{F}_{q^4}) \cong E^t(\mathbb{F}_{q^4})$ as groups.

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

From (2), (4), we have that ϕ is

$$\phi(X, Y, Z) = \Big(uZ, -\frac{\sqrt{u}^3}{3}(X + Y + dZ), -\frac{1}{3a}(\omega X + \frac{1}{\omega}Y + dZ)\Big).$$

and the inverse map ϕ^{-1} is

$$\begin{aligned}\phi^{-1}(x, y, z) = \Big(&\frac{\omega d}{u}x + \frac{(w-1)}{\sqrt{u}^3}y + (2\omega + 1)az, -\frac{(\omega + 1)d}{u}x - \frac{(\omega + 2)}{\sqrt{u}^3}y \\ &- (2\omega + 1)az, \frac{x}{u}\Big).\end{aligned}$$

Then we have the map ψ is

$$\begin{aligned}
\psi(x,y,z) &= (\phi\pi\phi^{-1})(x,y,z)\\
&= (\phi\pi)\Big(\frac{\omega d}{u}x+\frac{(\omega-1)}{\sqrt{u}^3}y+(2\omega+1)az,-\frac{(\omega+1)d}{u}x-\frac{(\omega+2)}{\sqrt{u}^3}y\\
&\quad -(2\omega+1)az,\frac{x}{u}\Big)\\
&= \phi\Big(\frac{\omega^q d^q}{u^q}x^q+\frac{(\omega-1)^q}{(\sqrt{u}^3)^q}y^q+(2w+1)^q a^q z^q,-\frac{(\omega+1)^q d^q}{u^q}x^q\\
&\quad -\frac{(\omega+2)^q}{(\sqrt{u^3})^q}y^q-(2\omega+1)^q a^q z^q,\frac{x^q}{u^q}\Big)\\
&= \Big(\frac{u}{u^q}x^q,\frac{\sqrt{u}^3}{3u^q}(d^q-d)x^q+\frac{\sqrt{u}^3 y^q}{(\sqrt{u}^3)^q},-\frac{1}{3a}\Big((d^q(\omega^{q+1}-\omega^{q-1}-\omega^2)\\
&\quad +d)\frac{x^q}{u^q})+(\omega^{q+1}-\omega^{q-1}+\omega+2)\frac{y^q}{(\sqrt{u}^3)^q}+a^q(2\omega+1)^{q+1}z^q\Big)
\end{aligned}$$

for $P=(x,y,z)\in E^t(\overline{\mathbb{F}}_q)$. Also, since $x^{q^2}=x$, $y^{q^2}=y$ for $x,y\in\mathbb{F}_{q^2}$, we have

$$\psi^2(x,y)=\Big(\frac{u^{1-q}}{u^{q^2-q}}x^{q^2},\frac{(\sqrt{u}^3)^{1-q}}{(\sqrt{u}^3)^{q^2-q}}y^{q^2},(a^{q-1})^{2q}z^{q^2}\Big)=(x,-y,z)=-(x,y,z),$$

where $u\in\mathbb{F}_{q^2}$ (i.e., $u^{q^2}=d$) and $\sqrt{u}^3\notin\mathbb{F}_{q^2}$ (and so, $(\sqrt{u}^3)^{q^2}=-\sqrt{u}^3$). Therefore,

$$\psi^2(P)+P=\mathcal{O}_{E'}.$$

□

The following theorem is an application of GLV method to point multiplication of projective twisted Hessian curve.

Theorem 3.9. *Let $\mathcal{H}^t_{\bar{a},\bar{d}}$ be a Hessian curve over $\mathbb{F}_q$ with $q+1-t$ points. Let $\widetilde{\pi}$ be the q-power Frobenius map on $\mathcal{H}^t_{\bar{a},\bar{d}}$. Write E^t for the quadratic twist of $\mathcal{H}^t_{\bar{a},\bar{d}}$ over $\mathbb{F}_{q^2}$ and let $\widetilde{\phi}:\mathcal{H}^t_{\bar{a},\bar{d}}\to E^t$ be the twisting isomorphism defined over $\mathbb{F}_{q^4}$. Let $\widetilde{\psi}=\widetilde{\phi}\widetilde{\pi}\widetilde{\phi}^{-1}$. Let $r|\sharp E^t(\mathbb{F}_{q^2})$ be a prime such that $r>2q$. Let $P\in E^t(\mathbb{F}_{q^2})[r]$. Then $\widetilde{\psi}(P)=[\lambda]P$ where $\lambda\in\mathbb{Z}/r\mathbb{Z}$ satisfies $\lambda^2+1\equiv 0$ (mod r). Also, we have $\widetilde{\psi}(P)^2+P=O_{E^t}$.*

Proof. The proof is similar to that of Theorem 3.8, we omit it here. □

4. Conclusion

In this paper, we presented the Frobenius endomorphisms on generalized Hessian curve and twisted Hessian curves. This leads to an efficient point multiplication on Hessian curve over a finite field. Moreover, we constructed a Frobenius map defined on the quadratic twist of a special type of elliptic curve and showed how to it to accelerate the scalar multiplication on this curve.

References

[1] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen and F. Vercauteren, *Handbook of Elliptic and Hyperelliptic Cryptography*, Chapman and Hall/CRC, 2006.

[2] D. Bernstein, C. Chuengsatiansup, D. Kohel and T. Lange, *Twisted Hessian Curves*, Proceedings of the 4th International Conference on Progress in Cryptology, LATINCRYPT 2015, vol 9230, 269–294, 2015.

[3] D. V. Chudnovsky and g. v. Chudnovsky. Sequences of numbers generated by addition in formal groups and new primality and factorizaation tests. Advances in Applied Mathematics, 7(4):385-434, 1986.

[4] H. M. Edwards, A normal form for elliptic curves, Bulletin of the American Mathematical Society 44(3) (2007), 393–422.

[5] R. R. Farashahi, M. Joye, *Efficient arithmetic on Hessian curves*, in: Public Key Cryptography-PKC 2010, 13th International Conference on Practice and Theory in Public Key Cryptography, Paris, France, May 26-28, 2010. Proceedings, 2010, pp. 243–260.

[6] 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.

[7] 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.

[8] 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.

[9] O. Hesse. Über die Elimination der variabeln aus drei algebraischen Gleichungen vom zweiten Grade mit zwei Vaiabeln. Journal für die reine und angewandte Mathematik. 10:68-96, 1844.

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

[11] 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.

[12] M. Joye and J. -J. Quisquater. Hessian elliptic curves and side-channel attacks. In C. K. Koc, D. Naccache, and C. Paar, editors, CHES 2001, volume 2162 of LNCS, pages 402-410, Springer, 2001.

[13] A. Knapp. *Elliptic Curves*, Princeton University Press, 1992.

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

[15] 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.

[16] J. H. Silverman, *The Arithmetic of Elliptic curves*, Springer, 1986.

[17] G. Sohn, *Scalar multiplication on Jacobi curves using the frobenius map*, Proceedings of the Jangjeon Mathematical Society 22(2019), No. 1, pp. 7-14.

[18] G. Sohn, *Scalar multiplication on Huff curves using the frobenius map*, Advanced Studies in Contemporary Mathematics 27(2017), No. 2, pp. 223-228.

[19] N. P. Smart, The Hessian form of an elliptic curve. In C. K. Koc, D. Naccahe, and C. Paar, editiors, CHES 2001, volume 2162 of LNCS, paes 118-125. Springer, 2001.

[20] 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