FROBENIUS ENDOMORPHISMS OF BINARY HESSIAN CURVES

GYOYONG SOHN

Abstract. This paper introduces the Frobenius endomorphisms on the binary Hessian curves. It provides an efficient and computable homomorphism for computing point multiplication on binary Hessian curves. As an application, it is possible to construct the GLV method combined with the Frobenius endomorphism to accelerate scalar multiplication over the curve.

1. Introduction

Elliptic curve cryptography was first suggested by Koblitz [11] and Miller [12] in 1985. The security of these cryptosystems relies on the presumed intractability of the discrete logarithm problem on elliptic curves. In recent years, new models of elliptic curves have been discovered to provide cryptographic security, such as the Huff form, the Edwards form, the Hessian form and others [3, 8, 10]. Joye and Quisquater proposed Hessian elliptic curves [10], and Farashahi and Joye presented the efficient arithmetic on generalized Hessian curves [5]. Hessian curves can be represented by an equation of the form \( x^3 + y^3 + z^3 = dxyz \) in projective representation.

Scalar multiplication is the most critical operation in elliptic curve cryptography. It involves computing \([n]P\) for a given point \(P\) on an elliptic curve \(E\) defined over a finite field \(\mathbb{F}_q\) and a given integer \(n\). The speed and efficiency of elliptic curve cryptosystems rely heavily on the implementation of scalar multiplication. Various methods can be used for scalar multiplication on elliptic curves (a good reference is [1]). If an elliptic curve has an efficient endomorphism, it can be utilized to accelerate scalar multiplication. There have been investigations into fast scalar multiplication on elliptic curves over a finite field using endomorphism [1, 9, 6, 13, 14].

Received August 14, 2023; Revised September 27, 2023; Accepted September 30, 2023.
2010 Mathematics Subject Classification. 94A55, 11T71.
Key words and phrases. Binary Hessian Curve, Frobenius Endomorphism, Scalar Multiplication.
In this paper, we introduce the Frobenius endomorphisms on binary Hessian curves and binary twisted Hessian curves. We present an efficient homomorphism to accelerate scalar multiplication on these curves. To enhance the speed of scalar multiplication on binary Hessian curves, we utilize the GLV method combined with the Frobenius endomorphism over the curve.

This paper is organized as follows. Section 1 provides an introduction to binary Hessian curves, twisted Hessian curves, and the Frobenius map on Weierstrass equation of elliptic curve over a finite field with characteristic two. In the second section, we establish the birational equivalence between binary Hessian curve and Weierstrass equation of an elliptic curve over a finite field. Additionally, we describe the Frobenius endomorphism for binary Hessian curves and discuss some fundamental properties related to it.

2. Preliminaries

2.1. Binary Hessian Curves

Let $F_q$ be a finite field with even characteristic ($q = 2^n$) and $\overline{F}_q$ its algebraic closure. A binary Hessian curve over $F_q$ is defined by the symmetric cubic equation

$$H_d : x^3 + y^3 + 1 + dxy = 0,$$

for some $d \in F_q$ with $d^3 \neq 27$ [7]. 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 $F_q$ is defined by the equation

$$H_{c,d} : x^3 + y^3 + c + dxy = 0,$$

where $c, d \in F_q$ 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 $j = \frac{d^{12}}{c(c+d^3)x}.$

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

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

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

$$H_{c,d} : X^3 + Y^3 + cZ^3 = dXYZ,$$

where $c, d \in F_q$ with $c \neq 0$ and $d^3 \neq 27c$. It has the points $(1 : -\omega : 0)$ with $\omega^3 = 1$ at infinity. The neutral element of the group $\mathbb{F}_q$-rational points of $H_{c,d}$
is the point at infinity \((1 : -1 : 0)\) that we denote by \(O_{H_{a,d}}\). And, the negation of point \((X : Y : Z)\) is \((Y : X : Z)\).

2.2. Twisted Hessian Curves

A twisted Hessian curve over \(\mathbb{F}_q\) is defined by the equation

\[
H^t_{a,d} : ax^3 + y^3 + 1 = dxy,
\]

where \(a, d \in \mathbb{F}_q\). It has a specified point \((0, -1)\). The arithmetic formulæ of twisted Hessian curve is presented in [2]. The doubling formula is \((x_3, y_3) = 2(x_1, y_1)\), where

\[
\begin{align*}
x_3 &= x_1 - y_1^3 x_1 \quad \text{and} \\
y_3 &= y_1^3 - ax_1^3.
\end{align*}
\]

A twisted Hessian curve in projective coordinate over \(\mathbb{F}_q\) is defined by

\[
H^t_{a,d} : aX^3 + Y^3 + Z^3 = dXYZ,
\]

where \(a, d \in \mathbb{F}_q\) and \(a(27a - d^3) \neq 0\). The neutral element of \(H^t_{a,d}(\mathbb{F}_q)\) is the point at infinity \((0 : -1 : 1)\) that we denote by \(O_{H^t_{a,d}}\). The special case \(a = 1\) of a twisted Hessian curve is simply a Hessian curve. For the point \(P = (X : Y : Z)\) on \(H^t_{a,d}\), we have \(-P = (X : Z : Y)\).

2.3. Frobenius map on elliptic curves

An elliptic curve \(E_{a,b}\) over \(\mathbb{F}_q\) with \(q = 2^n\) is defined by a Weierstrass equation

\[
E_{a,b} : y^2 + xy = x^3 + ax + b,
\]

with \(a, b \in \mathbb{F}_q\) and \(b \neq 0\) and the point at infinity \(O_{E_{a,b}}\). The \(j\)-invariant is given by \(\frac{1}{b}\).

The \(q\)-th power Frobenius map \(\pi_q\) is defined as

\[
\pi_q : E_{a,b} \to E_{a,b} \\
(x, y) \mapsto (x^q, y^q).
\]

By the Hasse’s theorem, the number of \(\mathbb{F}_{q^k}\)-rational points on \(E_{a,b}\) satisfies

\[
|\#E(\mathbb{F}_{q^k}) - q^k - 1| \leq 2\sqrt{q^k}.
\]

The characteristic polynomial \(\chi_q \in \mathbb{Z}[x]\) of \(\pi_q\) is given by

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

which satisfies

\[
(\pi_q^2 - t\pi_q + q)P = O_{E_{a,b}}
\]

for all \(P \in E_{a,b}(\overline{\mathbb{F}_q})\).
3. Frobenius map on binary (twisted) Hessian curves

In this section, we present the construction of the Frobenius maps on binary Hessian curves and binary twisted Hessian curves. We provide an efficient and computable homomorphism that facilitates the computation of point multiplication on elliptic curves over a finite field.

Let $\mathbb{F}_q$ be a finite field with even characteristic and $H_{c,d}$ be a binary Hessian curve over $\mathbb{F}_q$. We define the $q$-th power Frobenius map of $H_{c,d}$

$$\phi_q : H_{c,d} \to H_{c,d}, \ (x, y) \mapsto (x^q, y^q).$$

**Lemma 3.1.** Let $\mathbb{F}_q$ be a finite field with $q = 2^n$. Then, every binary Hessian curve $H_{c,d}$ is birationally equivalent over $\mathbb{F}_q$ to a binary elliptic curve $E_{a,b}$ given by the Weierstrass equation

$$E_{a,b} : v^2 + uv = u^3 + au^2 + b.$$

**Proof.** see [4] \qed

From the above, the map $\sigma : H_{c,d} \to E_{a,b}$ defined by

$$(x, y) \mapsto (u, v),$$

where

$$u = x^2 + y^2 + xy + d(x + y) + c/d,$$
$$v = \frac{(x + d)(xy + y^2) + y(y + d)^2 + (c^2 + cd^3)/d^3}{d^3}.$$

It is a birationally equivalence from binary Hessian curve $H_{c,d}$ to the binary Weierstrass curve $E_{a,b}$ with $a = c/d^3$ and $b = c(c + d^3)^3/d^{12}$. The inverse map is

$$x = \frac{d^6(u + v) + c(c + d^3)}{d^6u + d^2(c + d^3)}, \ y = \frac{d^6v + c(c + d^3)}{d^6u + d^2(c + d^3)}.$$

Now we construct the Frobenius endomorphism of binary Hessian curve over a finite field $\mathbb{F}_q$ with $q = 2^n$.

**Lemma 3.2.** Let $H_{c,d}$ be a binary Hessian curve defined over a finite field $\mathbb{F}_q$ with $q = 2^n$ and $E_{a,b}$ be the birational equivalent elliptic curve of $H_{c,d}$ over $\mathbb{F}_q$. Let $#E_{a,b}(\mathbb{F}_q) = q + 1 - t$, $|t| \leq 2\sqrt{q}$ and let $\sigma$ be the birational map defined as above. Let $\pi_q$ be the $q$-th power Frobenius endomorphism over $E_{a,b}$. Define $\psi_{H_{c,d}} = \sigma^{-1}\pi_q\sigma$. Then

1. $\psi_{H_{c,d}} \in \text{End}(H_{c,d})$, (i.e., $\psi_{H_{c,d}}$ is an endomorphism of $H_{c,d}$).
2. For all $P \in H_{c,d}(\mathbb{F}_q)$ we have

$$\psi_{H_{c,d}}^2(P) - [t]\psi_{H_{c,d}}(P) + [q]P = \mathcal{O}_{H_{c,d}}.$$
Proof. First note that $\sigma$ is an isomorphism defined over a finite field $\mathbb{F}_q$, that $\pi_q$ is an isogeny from $E_{a,b}$ to itself defined over $\mathbb{F}_q$. Hence $\psi_{H_{c,d}}$ is an isogeny of $H_{c,d}$ to itself defined over $\mathbb{F}_q$. Therefore $\psi_{H_{c,d}}$ is a group homomorphism.

For $P \in H_{c,d}(\mathbb{F}_q)$, let’s denote $\sigma(P) = Q \in E_{a,b}(\mathbb{F}_q)$. Then the characteristic polynomial $\chi_q(x) = x^2 - tx + q$, $|t| \leq 2\sqrt{q}$ of the $q$-th power Frobenius map $\pi_q$ of $E_{a,b}$ satisfies

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

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

$$\sigma^{-1}(\pi_q^2 - [t]\pi_q + [q])\sigma(P) = O_{H_{c,d}}.$$

Therefore

$$\psi_{H_{c,d}}^2(P) - [t]\psi_{H_{c,d}}(P) + [q]P = O_{H_{c,d}}.$$  □

**Theorem 3.3.** Let $H_{c,d}$ be a binary Hessian curve defined over a finite field $\mathbb{F}_q$ with $q = 2^n$ and $\sharp H_{c,d}(\mathbb{F}_q) = q + 1 - t$. Then the Frobenius map $\phi_q$ of $H_{c,d}$ satisfies

$$(\phi_q^2 - [t]\phi_q + [q])P = O_{H_{c,d}},$$

for all $P \in H_{c,d}(\mathbb{F}_q)$.

**Proof.** Let $E_{a,b}$ be the birational equivalent elliptic curve of $H_{c,d}$ defined over $\mathbb{F}_q$ with $q = 2^n$, and $\psi_{H_{c,d}}$ be the endomorphism of $H_{c,d}$ in Lemma 3.2. By definition of $\psi_{H_{c,d}}$, for all $P = (x,y) \in H_{c,d}(\mathbb{F}_q)$, we have

$$\psi_{H_{c,d}}(x,y) = (\sigma^{-1}\pi_q\sigma)(x,y) = (\sigma^{-1}\pi)(x^2 + y^2 + xy + d(x + y) + c/d, (x + d)(xy + y^2) + y(y + d)^2 + (c^2 + cd^3)/d^3)) = \sigma^{-1}(x^{2q} + y^{2q} + (xy)^q + d^q(x + y)^q + c^q/d) = (x^q, y^q).$$

Hence we have for all $P \in H_{c,d}(\mathbb{F}_q)$, $\psi_{H_{c,d}}(P) = \pi_q(P)$ and $\sharp E_{a,b}(\mathbb{F}_q) = \sharp H_{c,b}(\mathbb{F}_q) = q + 1 - t$. Hence by Lemma 3.2, we can complete the proof of Theorem. □

Now we consider the Frobenius endomorphism on binary twisted Hessian curves over a finite field $\mathbb{F}_q$ with $q = 2^n$. We define the $q$-th power Frobenius
map of $H_{a,d}^t$

$$\varphi : H_{a,d}^t \to H_{a,d}^t, \ (x, y) \mapsto (x^q, y^q).$$

**Lemma 3.4.** Let $\mathbb{F}_q$ be a finite field of characteristic 2. Then, every binary twisted Hessian curve $H_{a,d}^t$ is birationally equivalent over $\mathbb{F}_q$ to a binary elliptic curve $E_{a,b}$ given by the Weierstrass equation

$$E_{a,b} : v^2 + uv = u^3 + au^2 + b.$$

The map $\mu : H_{a,d}^t \to E_{a,b}$ defined by

$$u = \frac{a^\frac{3}{2}x^2 + y^2 + a^\frac{3}{2}xy + a^\frac{3}{2}d(a^\frac{3}{2}x + y) + 1/a^\frac{3}{2}d}{a^\frac{3}{2}d^2},$$
$$v = \frac{a^\frac{3}{2}(x + d)(a^\frac{3}{2}xy + y^2) + y(y + a^\frac{3}{2}d)^2 + (1 + ad^3)/ad^3}{ad^3}$$

is a birationally equivalence from binary Hessian curve $H_{c,d}^t$ to the Weierstrass curve $E_{a,b}$ with $a = 1/ad^3$ and $b = (1 + ad^3)/a^{4}d^{12}$. The inverse map is

$$x = \frac{a^{2}d^{6}(u + v) + (1 + ad^3)}{a^{2}d^{5}u + ad^2(1 + ad^3)}, \ y = \frac{a^{2}d^{5}v + (1 + ad^3)}{a^{2}d^{5}u + a^{2}d^{2}(1 + ad^3)}.$$

The following lemma gives the Frobenius endomorphism of binary twisted Hessian curve over a finite field $\mathbb{F}_q$ with $q = 2^n$.

**Lemma 3.5.** Let $H_{a,d}^t$ be a binary twisted Hessian curve defined over a finite field $\mathbb{F}_q$ with $q = 2^n$ and $E_{a,b}$ be the birational equivalent elliptic curve of $H_{a,d}^t$ over $\mathbb{F}_q$. Let $\psi_{E_{a,b}}(\mathbb{F}_q) = q + 1 - t$, $|t| \leq 2\sqrt{q}$ and let $\mu$ be the birational map defined as above. Let $\pi_q$ be the $q$-th power Frobenius map over $E_{a,b}$. Define $\psi_{H_{a,d}^t} = \mu^{-1}\pi_q\mu$. Then

1. $\psi_{H_{a,d}^t} \in \text{End}(H_{a,d}^t)$, (i.e., $\psi_{H_{a,d}^t}$ is an endomorphism of $H_{a,d}^t$).
2. For all $P \in H_{a,d}^t(\mathbb{F}_q)$ we have

$$\psi_{H_{a,d}^t}^2(P) - \lfloor t \rfloor \psi_{H_{a,d}^t}(P) + [q]P = \mathcal{O}_{H_{a,d}^t}.$$

**Proof.** The proof is similar to that of Lemma 3.4, we omit it here. \[\square\]

**Theorem 3.6.** Let $H_{a,d}^t$ be a binary twisted Hessian curve defined over a finite field $\mathbb{F}_q$ with $q = 2^n$ and $\psi_{H_{a,d}^t}(\mathbb{F}_q) = q + 1 - t$. Then the Frobenius endomorphism $\varphi$ of $H_{a,d}^t$ satisfies

$$\left(\varphi^2 - \lfloor t \rfloor \varphi + [q]\right)P = \mathcal{O}_{H_{a,d}^t},$$

for all $P \in H_{a,d}^t(\mathbb{F}_q)$.

**Proof.** Let $E_{a,b}$ be the birational equivalent elliptic curve of $H_{a,b}^t$ defined over $\mathbb{F}_q$ with $q = 2^n$, and $\psi_{H_{a,b}^t}$ be the endomorphism of $H_{a,d}^t$ in Lemma 3.4. By
HESSIAN CURVE

535
definition of $\psi_{H^t_{a,b}}$, for all $P = (x, y) \in H^t_{a,b}(\mathbb{F}_q)$, we have

$$
\psi_{H^t_{a,b}}(x, y) = (\mu^{-1} \pi_q \mu)(x, y)
$$

$$
= (\mu^{-1} \pi_q) \left( \frac{a^3 x^2 + y^2 + a^3 x y + a^3 d(a^3 x + y) + 1/a^2 d}{a^2 d^2}
\right)
$$

$$
= (\mu^{-1} \pi_q) \left( a^q (x + d)(a^q x y + y^2) + y(y + a^q d)^2 + (1 + ad^3)/ad^3 \right)
$$

$$
= \mu^{-1} \left( \frac{a^q x^2 + y^2 + a^q x y + a^q d^2 (a^q x + y^2) + 1/\mu^q d^2}{a^q d^2}
\right)
$$

$$
= \mu^{-1} \left( a^q (x^q + d^q)(a^q x^q y^q + y^2) + y^q(y^q + a^q d^q)^2 + 1/a^q d^q \right)
$$

$$
= (x^q, y^q),
$$

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

Hence we have for all $P \in H^t_{a,b}(\mathbb{F}_q)$, $\psi_{H^t_{a,b}}(P) = \varphi(P)$ and $\sharp E_{a,b}(\mathbb{F}_q) = \sharp H^t_{a,b}(\mathbb{F}_q) = q + 1 - t$. Hence by Lemma 3.5, we can complete the proof of Theorem.

□

4. Conclusion

In this paper, we have introduced the Frobenius endomorphisms on binary Hessian curves and twisted binary Hessian curves. These two endomorphisms can be utilized to accelerate scalar multiplication over binary (twisted) Hessian curves defined over finite fields with characteristic two.

References


Gyo Yong Sohn  
Department of Mathematics Education, Daegu National University of Education, Daegu 705-715, Korea  
Email address: gysohn@dnue.ac.kr