East Asian Math. J.
Vol. 39 (2023), No. 5, pp. 529–536
http://dx.doi.org/10.7858/eamj.2023.039

FROBENIUS ENDOMORPHISMS OF BINARY HESSIAN CURVES

Gyoyong Sohn

Abstract. This paper introduces the Frobenius endomophisms 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 implementaion 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 enomorphism [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.

(pISSN 1226-6973, eISSN 2287-2833)

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 ti.

2. Premiminaries

2.1. Binary Hessian Curves

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

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

for some $d \in \mathbb{F}_q$ 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 $\mathbb{F}_q$ is defined by the equation

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

where $c, d \in \mathbb{F}_q$ 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 $j = \frac{d^{12}}{c(c+d^3)^3}$.

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

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

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 $c, d \in \mathbb{F}_q$ 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 $\mathcal{O}_{H_{c,d}}$. 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 formulae of twised Hessian curve is presented in [2]. The doubling formula is $(x_3, y_3) = 2(x_1, y_1)$, where

$$x_3 = \frac{x_1 - y_1^3 x_1}{ay_1x_1^3 - y_1} \text{ and } y_3 = \frac{y_1^3 - ax_1^3}{ay_1x_1^3 - y_1}.$$

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 $\mathcal{O}_{H^t_{a,d}}$. 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 $\mathcal{O}_{E_{a,b}}$. The j-invariant is given by $\frac{1}{b}$.

The q-th power Frobenius map π_q is defined as

$$\begin{aligned} \pi_q \ : \ E_{a,b} &\longrightarrow E_{a,b} \\ (x, y) &\longmapsto (x^q, y^q). \end{aligned}$$

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

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

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

which satisfies

$$(\pi_q^2 - t\pi_q + q)P = \mathcal{O}_{E_{a,b}}$$

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] □

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

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

where

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

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

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

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 $\sharp E_{a,b}(\mathbb{F}_q) = q + 1 - t$, $|t| \leq 2\sqrt{q}$ and let σ be the birational map defined as above. Let π_q be the q-th power Frobenius endomorphism over $E_{a,b}$. Define $\psi_{H_{c,d}} = \sigma^{-1}\pi_q\sigma$. Then*

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

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

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

Proof. First note that σ is an isomorphism defined over a finite field $\mathbb{F}_q$, that π_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 $P \in H_{c,d}(\overline{\mathbb{F}}_q)$, let's denote $\sigma(P) = Q \in E_{a,b}(\overline{\mathbb{F}}_q)$. Then the characteristic polynomial $\chi_q(x) = x^2 - tx + q$, $|t| \leq 2\sqrt{q}$ of the q-th power Frobenius map π_q of $E_{a,b}$ satisfies

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

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

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

Therefore

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

□

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 ϕ_q of $H_{c,d}$ satisfies*

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

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

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 $P = (x, y) \in H_{c,d}(\overline{\mathbb{F}}_q)$, we have

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

Hence we have for all $P \in H_{c,d}(\overline{\mathbb{F}}_q)$, $\psi_{H_{c,d}}(P) = \pi_q(P)$ 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 $\mu \ : \ H_{a,d}^t \longrightarrow E_{a,b}$ defined by

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

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

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

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 $\sharp E_{a,b}(\mathbb{F}_q) = q + 1 - t$, $|t| \leq 2\sqrt{q}$ and let μ be the birational map defined as above. Let π_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. *$\psi_{H_{a,d}^t} \in End(H_{a,d}^t)$, (i.e., $\psi_{H_{a,d}^t}$ is an endomorphism of $H_{a,d}^t$).*
2. *For all $P \in H_{a,d}^t(\overline{\mathbb{F}}_q)$ we have*

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

Proof. The proof is similar to that of Lemma 3.4, we omit it here. □

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 $\sharp H_{a,d}^t(\mathbb{F}_q) = q+1-t$. Then the Frobenius endomorphism φ of $H_{a,d}^t$ satisfies*

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

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

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

$$\begin{aligned}\psi_{H^t_{a,b}}(x,y) =&(\mu^{-1}\pi_q\mu)(x,y)\\ =&(\mu^{-1}\pi_q)\Big(\frac{a^{\frac{2}{3}}x^2+y^2+a^{\frac{1}{3}}xy+a^{\frac{1}{3}}d(a^{\frac{1}{3}}x+y)+1/a^{\frac{1}{3}}d}{a^{\frac{3}{2}}d^2},\\ &\frac{a^{\frac{1}{3}}(x+d)(a^{\frac{1}{3}}xy+y^2)+y(y+a^{\frac{1}{3}}d)^2+(1+ad^3)/ad^3}{ad^3}\Big)\\ =&\mu^{-1}\Big(\frac{a^{\frac{2}{3}q}x^{2q}+y^{2q}+a^{\frac{1}{3}q}x^qy^q+a^{\frac{1}{3}q}d^q(a^{\frac{1}{3}q}x^q+y^q)+1/a^{\frac{1}{3}q}d^q}{a^{\frac{2}{3}q}d^{2q}},\\ &\frac{a^{\frac{1}{3}q}(x^q+d^q)(a^{\frac{1}{3}q}x^qy^q+y^{2q})+y^q(y^q+a^{\frac{1}{3}q}d^q)^2+1+1/a^qd^{3q}}{a^qd^{3q}}\Big)\\ =&(x^q,y^q),\end{aligned}$$

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

Hence we have for all $P\in H^t_{a,b}(\overline{\mathbb{F}}_q)$, $\psi_{H^t_{a,b}(\overline{\mathbb{F}}_q)}(P)=\varphi(P)$ 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

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

[4] R. R. Farashahi and S. G. Hosseini, Differential addition on binary elliptic curves, Finite fields and their applications 87 (2023), pp. 102141.

[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] 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] 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.

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

[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. -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.

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

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

Gyoyong Sohn

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

Email address: gysohn@dnue.ac.kr