East Asian Math. J.
Vol. 40 (2024), No. 5, pp. 551–557
http://dx.doi.org/10.7858/eamj.2024.038

SCALAR MULTIPLICATION ON GENERALIZED HUFF CURVES USING THE SKEW-FROBENIUS MAP

Gyoyong Sohn

Abstract. This paper presents the Frobenius endomorphism on generalized Huff curve and provides the characteristic polynomial of the map. By applying the Frobenius endomorphism on generalized Huff curve, we construct a skew-Frobenius map defined on the quadratic twist of a generalized Huff curve. This map offers an efficiently computable homomorphism for performing scalar multiplication on the generalized Huff curve over a finite field. As an application, we describe the GLV method combined with the Frobenius endomorphism over the curve to speed up the scalar multiplication.

1. Introduction

Elliptic curves are a branch of mathematics that has been studied for almost a century. In 1985, Koblitz [8] and Miller [9] independently proposed the use of elliptic curves in cryptography. The elliptic curve cryptosystem is a public key cryptosystem based on the discrete logarithm problem in the group of points on a curve. In the elliptic curve cryptosystem, the efficiency essentially depends on the fundamental operation of scalar multiplication. Generally, the speed of scalar multiplication depends on finite field operations, curve point operations, and the representation of the scalar n[12, 5].

There is a vast literature on efficient methods for computationally speeding up scalar multiplication. For elliptic curves, scalar multiplication can be performed using various methods (a good reference is [1]). If an elliptic curve admits an efficient endomorphism, its use can speed up scalar multiplication. In [2], 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) method provides suitable, efficiently computable endomorphisms on elliptic curves for speeding up point multiplication [3].

To obtain faster scalar multiplications, several models of elliptic curves have been extensively studied, including Edward curves, Jacobi intersections, Jacobi

Received June 14, 2024; Accepted September 30, 2024.
2010 *Mathematics Subject Classification.* 94A55, 11T71.
Key words and phrases. Generalized Huff Curve, Scalar Multiplication, Frobenius Map.

quartics, Hessian curves, and others. In 1948, Huff introduced a new elliptic curve model while studying a Diophantine problem [6]. In [7], Joye, Tibouchi and Vergnaud studied Huff's model over fields of odd characteristic and introduced formulas for fast point arithmetic. Wu and Feng in [11] presented a general Huff form.

In this paper, we present the Frobenius endomorphism on generalized Huff curves over finite fields and the scalar multiplication using Frobenius expansion. By applying the Frobenius endomorphism to generalized Huff curves, we construct a skew-Frobenius map defined on the quadratic twist of a generalized Huff curve. To speed up scalar multiplication on these curves, we use the GLV method combined with the Frobenius endomorphism.

This paper is organized as follows. Section 1 illustrates some basic notions on generalized Huff curves and the Frobenius endomorphism. We also provide the expression of the group law and the birational equivalence between generalized Huff curve and the Weierstrass equation of an elliptic curve. The second section describes the Frobenius endomorphism for the curve and some basic properties.

2. Premiminaries

2.1. Generalized Huff Curves

Let K be a field with char(K)$\neq 2$ and $\overline{K}$ its algebraic closure. The generalized Huff curves over K proposed by Wu and Feng in [10] are of the form:

$$H_{a,b}\ :\ x(ay^2-1)=y(bx^2-1), \tag{1}$$

where $a,b\in K^*$ and $ab(a-b)\neq 0$. This model contains the ordinary Huff curves $ax(y^2-1)=by(x^2-1)$ as particular case. We know that every elliptic curve over the finite field with three points of order 2 is isomorphic to a general Huff curve.

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

$$x_3=\frac{(x_1+x_2)(ay_1y_2+1)}{(bx_1x_2+1)(ay_1y_2-1)} \text{ and } y_3=\frac{(y_1+y_2)(bx_1x_2+1)}{(bx_1x_2-1)(ay_1y_2+1)}.$$

In projective coordinates, the generalized Huff curves are defined by

$$\mathcal{H}_{a,b}\ :\ X(aY^2-Z^2)=Y(bX^2-Y^2),$$

where $a,b\in K^*$ and $ab(a-b)\neq 0$. We know that $O_{\mathcal{H}_{a,b}}=(0,0,1)$ is an inflection point of $\mathcal{H}_{a,b}$ and no inflection points with $Z=0$. The inverse of point $P=(X,Y,Z)$ is $-P=(X,Y,-Z)$. Generalized Huff curves has an additive group structure with $O_{\mathcal{H}_{a,b}}$. Hence, the three points at infinity $(1,0,0)$, $(0,1,0)$ and $(a,b,0)$ are exactly the three primitive 2-torsion points of $\mathcal{H}_{a,b}$. The sum of any two of them is equal to the third one.

2.2. Frobenius map on elliptic curves

Let $\mathbb{F}_q$ be a finite field with $\mathrm{char}(\mathbb{F}_q) \neq 2$ 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 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 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 Generalized Huff curves

Let $\mathbb{F}_q$ be a finite field of $\mathrm{char}(\mathbb{F}_q) \neq 2$ and let $H_{a,b}$ be a generalized Huff curve over $\mathbb{F}_q$ with the points at infinity $O_{H_{a,b}}$. We define the *q-th* power Frobenius map $\widehat{\pi}$ of $H_{a,b}$

$$\begin{aligned} \widehat{\pi} \ : \ & H_{a,b} \longrightarrow H_{a,b} \\ & (x, y) \longmapsto (x^q, y^q) \end{aligned}$$

Now we state the following lemmas to use the main result of this section.

Lemma 3.1. [10] *Let K be a field of char(K)$\neq 2$, let a and b be two elements of K, with $a \neq b$. Then, the curve*

$$X(aY^2 - Z^2) = Y(bX^2 - Z^2)$$

is isomorphic over K to the elliptic curve given by the Weierstrass equation

$$V^2W = U(U + aW)(U + bW)$$

via the transformations $\sigma(X, Y, Z) = (U, V, W)$, where $U = bX - aY$, $V = (b - a)Z$ and $W = Y - X$. The inverse application is given by $\sigma^{-1}(U, V, W) = (X, Y, Z)$, with $X = U + aW$, $Y = U + bW$, $Z = V$.

In affine coordintates, the generalized Huff curve $x(ay^2 - 1) = y(bx^2 - 1)$ defined over K is isomorphic to the elliptic curve $y^2 = x(x + a)(x + b)$ over K.

Lemma 3.2. *Let $H_{a,b}$ be a generalized Huff curve defined over $\mathbb{F}_q$ and E be the elliptic curve over $\mathbb{F}_q$ that is isomorphic to $H_{a,b}$. Let $\sharp E(\mathbb{F}_q) = q + 1 - t$ and let σ be the birational transformation defined as above. Let π be the q-th power Frobenius endomorphism over E. Define $\psi = \sigma^{-1}\pi\sigma$. Then*

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

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

Proof. First note that σ an isogeny from $H_{a,b}$ to E and is defined over $\mathbb{F}_q$, that π is an isogeny from E to itself defined over $\mathbb{F}_q$, and that σ^{-1} is an isogeny form E to $H_{a,b}$ defined over $\mathbb{F}_q$. Hence ψ is an isogeny of $H_{a,b}$ to itself, and is defined over $\mathbb{F}_q$. Therefore ψ is a group homomorphism.

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

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

Therefore

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

□

Now we have the main result of this section.

Theorem 3.3. *Let $H_{a,b}$ be a generalized Huff curve defined over a finite field $\mathbb{F}_q$ and $\sharp H_{a,b}(\mathbb{F}_q) = q + 1 - t$. Then the Frobenius map of $H_{a,b}$ satisfies*

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

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

Proof. Let E be the elliptic curve over $\mathbb{F}_q$ that is isomorphic to $H_{a,b}$, and ψ be the endomorphism of $H_{a,b}$ in Lemma 3.2. By definition of ψ, for all $P = (x, y) \in H_{a,b}(\overline{\mathbb{F}}_q)$,

$$\begin{aligned}\psi(x,y) = (\sigma^{-1}\pi\sigma)(x,y) &= (\sigma^{-1}\pi)\Big(\frac{bx-ay}{y-x}, \frac{b-a}{y-x}\Big)\\ &= \sigma^{-1}\Big(\frac{(bx-ay)^q}{(y-x)^q}, \frac{(b-a)^q}{(y-x)^q}\Big) = (x^q, y^q),\end{aligned}$$

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

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

4. Skew-Frobenius map on quadratic twists of a generalized Huff curves

In this section, we will construct a skew-Frobenius map on the quadratic twist of a generalized Huff curve according to the Frobenius map on a generalized Huff curve.

Let $H_{a,b}$ be a generalized Huff curve over $\mathbb{F}_q$ defined by (1). The quadratic twist of a generalized Huff curve is

$$H_{a,b}^t \ : \ x(ay^2 - d) = y(bx^2 - d)$$

where $a, b, d \in \mathbb{F}_q^*$ and $ab(a-b) \neq 0$. If $d \in \mathbb{F}_q^*$ is a non-square, then the map ϕ is an isomorphism from $H_{a,b}$ to $H_{a,b}^t$ over $\mathbb{F}_q(\sqrt{d})$. The map ϕ is given by $(x, y) = (\frac{x}{\sqrt{d}}, \frac{y}{\sqrt{d}})$. Then we can construct the skew-Frobenius map $\widehat{\psi}$ on $H_{a,b}^t$ by computing the map $\phi\widehat{\pi}\phi^{-1}$. The skew-Frobenius map on $H_{a,b}^t$ is defined by

$$\widehat{\psi} \ : \ H_{a,b}^t \to H_{a,b}^t, \ (x, y) \mapsto (\sqrt{d}^{q-1} x^q, \sqrt{d}^{q-1} y^q).$$

Theorem 4.1. *Let $H_{a,b}$ be a generalized Huff curve defined over $\mathbb{F}_q$ and $H_{a,b}^t$ be a quadratic twist of $H_{a,b}$. Let $\sharp H_{a,b}(\mathbb{F}_q) = q+1-t$ and let ϕ is an isomorphism from $H_{a,b}$ to $H_{a,b}^t$ over $\mathbb{F}_q(\sqrt{d})$. Let $\widehat{\pi}$ be the q-th power Frobenius map on $H_{a,b}$. Define $\widehat{\psi} = \phi\widehat{\pi}\phi^{-1}$. Then for all $P \in H_{a,b}^t(\overline{\mathbb{F}}_q)$, we have*

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

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

The GLV method provided an efficiently computable homomorphism for elliptic curves where E is defined over $\mathbb{F}_q$ with a large characteristic. The following map can be used for the GLV method to perform point multiplication on generalized Huff curves by extending the method in Galbraith et. al. [4].

Theorem 4.2. *Let $H_{a,b}$ be a generalized Huff curve over $\mathbb{F}_q$ with $q+1-t$ points. Let π be the q-th power Frobenius map on $H_{a,b}$. Write $H_{a,b}^t$ for the quadratic twist of $H_{a,b}$ over $\mathbb{F}_{q^2}$ and let $\phi : H_{a,b} \to H_{a,b}^t$ be the twisting isomorphism defined over $\mathbb{F}_{q^4}$. Let $\psi = \phi\widehat{\pi}\phi^{-1}$. Let $r|\sharp H_{a,b}^t(\mathbb{F}_{q^2})$ be a prime such that $r > 2q$. Let $P \in H_{a,b}^t(\mathbb{F}_{q^2})[r]$. Then $\psi(P) = [\lambda]P$ where $\lambda \in \mathbb{Z}/r\mathbb{Z}$ satisfies $\lambda^2 + 1 \equiv 0$ (mod r). Also, we have $\psi(P)^2 + P = O_{H_{a,b}^t}$.*

Proof. Since ϕ and $\widehat{\pi}$ are group homomorphisms it follows that ψ is too. We have $H_{a,b}(\mathbb{F}_{q^4}) \cong H_{a,b}^t(\mathbb{F}_{q^4})$ as groups.

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

By definition, $\psi(x,y) = (\phi\widehat{\pi})(\frac{x}{\sqrt{d}}, \frac{y}{\sqrt{d}}) = \phi(\frac{x^q}{\sqrt{d}^q}, \frac{y^q}{\sqrt{d}^q}) = (\sqrt{d}^{1-q}x^q, \sqrt{d}^{1-q}y^q)$ for $P = (x,y) \in H^t_{a,b}(\overline{\mathbb{F}}_q)$. Also, since $x^{q^2} = x$, $y^{q^2} = y$ for $x, y \in \mathbb{F}_{q^2}$, we have

$$\psi^2(x,y) = \Big(\frac{\sqrt{d}x^{q^2}}{\sqrt{d}^{q^2}}, \frac{\sqrt{d}y^{q^2}}{\sqrt{d}^{q^2}}\Big) = (-x,-y) = -(x,y).$$

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

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

□

Hence, the above map can be used for the GLV method on generalized Huff curve.

5. Conclusion

In this paper, we discussed the endomorphism on the generalized Huff curves defined over finite field. Based on this, we constructed a skew-Frobenius map defined on the quadratic twist of a generalized Huff curve and demonstrated how it can accelerate 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] 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.

[3] 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.

[4] 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.

[5] 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.

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

[7] M. Joye, M. Tibbouchi, and D. Vergnaud, *Huff's Model for Elliptic Curves*, Algorithmic Number Theory - ANTS-IX, Lecture Notes in Computer Science Vol. 6197, Springer, pp. 234-250, 2010.

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

[9] 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.

[10] H. Wu, R. Feng. Elliptic curves in Huff's model, 2010, Available at HTTP://EPRINT.IACR.ORG/2010/390.

[11] H. Wu and R. Feng, *Elliptic curves in Huff's model* eprint.iacr.org/2010/390.pdf

[12] 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
Email address: gysohn@dnue.ac.kr