Advanced Studies in Contemporary Mathematics
27 (2017), No. 2, pp. 223 – 228

www.jangjeon.or.kr
http://dx.doi.org/10.23001/ascm2017.27.2.223

SCALAR MULTIPLICATION ON HUFF CURVES USING THE FROBENIUS MAP

GYOYONG SOHN

Abstract. This paper introduces the scalar multiplication on Huff elliptic curves over a finite field using the Frobenius expansion. Applying the Frobenius endomorphism on Huff curve, we construct a Frobenius map defined on the quadratic twist of a Huff curve. To speed up the scalar multiplication on Huff curves, we use the GLV method combined with the Frobenius endomorphism over the curve.

2010 Mathematics Subject Classification. 94A55, 11T71.

Keywords and phrases. Huff Curve, Scalar Multiplication, Frobenius Map.

1. Introduction

Elliptic curve cryptography was independently proposed by Koblitz [9] and Miller [10] 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[11, 5].

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(a good reference is [1]). If an elliptic curve admits an efficient endomorphism, its use can speed up scalar multiplication. In [7], 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 [4].

There are several models of elliptic curves to provide the efficient computation and implement for cryptography in recent year [2, 6]. In [8], Joye, Tibouchi and Vergnaud revisits a model for elliptic curves over $\mathbb{Q}$ introduced in [6] in 1948 to study a diophantine problem. The Huff's model for elliptic curves is given by equation $ax(y^2 - 1) = by(x^2 - 1)$.

In this paper, we present the Frobenius endomorphism on Huff curves over a finite field and the scalar multiplication on Huff curves using Frobenius

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

expansion. Applying the Frobenius endomorphism on Huff curve, we construct a Frobenius map defined on the quadratic twist of a Huff curve. To speed up the scalar multiplication on Huff curves, we use the GLV method combined with the Frobenius endomorphism over the curve.

This paper is organized as follows. Section 1 illustrate some basic notions on Huff curves and Forbnius endomorphism. We also give expression of the group law and the birational equivalence between Huff curve and Weierstrass equation of elliptic curve. Second section describe Frobenius endomorphism for Huff's Model and some basic properties.

2. Premiminaries

This section recall some basic notions for Huff curves and Frobenius maps on elliptic curves.

2.1. **Huff Curves.** Huff curves was introduced by Joye, Tibouchi and Vergnaud in 2010 [8]. They revisits a model for elliptic curves over $\mathbb{Q}$ introduced in [6] in 1948 to study a diophantine problem. The Huff's model for elliptic curves is given by the following defnition.

Definition 2.1. Let K be a finite field with odd characteristic. The Huff's model of an elliptic curve is the affine curve

$$H_{a,b} \ : \ ax(y^2-1) = by(x^2-1),$$

where $a, b \in K^*$ and $a^2 \neq b^2$.

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

$$x_3 = \frac{(x_1+x_2)(1+y_1y_2)}{(1+x_1x_2)(1-y_1y_2)} \text{ and } y_3 = \frac{(y_1+y_2)(1+x_1x_2)}{(1-x_1x_2)(1+y_1y_2)}.$$

The additive identity is the point $(0, 0)$, and the additive inverse of a point P is the point $-P = (-x, -y)$. The Huff model of elliptic curves in projective coordinates are defined by

$$aX(Y^2 - Z^2) = bY(X^2 - Y^2),$$

where $a, b \neq 0$ and $a^2 \neq b^2$. Huff curves has an additive group structure together with the identity element $O = (0 : 0 : 1)$. We note that a point at infinity is its own inverse. Hence, there are three points at infinity, namly, $(1 : 0 : 0)$, $(0 : 1 : 0)$ and $(a : b : 0)$. These points at infinity are exactly the three primitive 2-torsion points of $H_{a,b}$. 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 $char(\mathbb{F}_q) \neq 2$ 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 $\widehat{\pi}$ 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 Huff curves

Let $\mathbb{F}_q$ be a finite field of characteristic different from 2 and let $H_{a,b}$ be a Huff elliptic curve over $\mathbb{F}_q$. We define the q-power Frobenius endomorphism 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 folloiwng lemmas to use the main result of this section.

Lemma 3.1. *Let K be a finite field with odd characteristic. Then, every Huff curves $H_{a,b}$ is birationally equivalent over K to an elliptic curve E given by the Weierstrass equation*

$$E \ : \ v^2 = u(u + a^2)(u + b^2).$$

Proof. See [8] □

From Lemma 3.1, one can see that there exists an elliptic curve E over $\mathbb{F}_q$ such that $H_{a,b}(\overline{\mathbb{F}}_q) \cong E(\overline{\mathbb{F}}_q)$. Let σ be the isomorphism

$$\begin{aligned} \sigma \ &: \ H_{a,b} \longrightarrow E \\ &(x, y) \longmapsto (u, v) \end{aligned}$$

where

$$(u, v) = \Big(\frac{ab(bx - ay)}{-ax + by}, \frac{ab(b^2 - a)}{-ax + by}\Big), \text{ if } ax \neq by. \tag{1}$$

The only point on H with $ax = by$ is $(0, 0)$ which is mapped to O. The inverse transformation is given by

$$\begin{aligned} \sigma^{-1} \ &: \ E \longrightarrow H_{a,b} \\ &(u, v) \longmapsto (x, y), \end{aligned}$$

where

$$(x, y) = \Big(\frac{b(u + a^2)}{v}, \frac{a(u + b^2)}{v}\Big), \text{ if } v \neq 0.$$

The points (u, v) with $v = 0$ are the points of order 2 which get sent to the points at infinity on $H_{a,b}$.

Lemma 3.2. *Let $H_{a,b}$ be a Huff curve defined over $\mathbb{F}_q$ and E be the birational equivalent elliptic curve of $H_{a,b}$ 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 $\psi = \sigma^{-1}\pi\sigma$. 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 isomorphism defined over $\mathbb{F}_q$, that π is an isogeny from E to itself defined over $\mathbb{F}_q$. Hence ψ is an isogeny of $H_{a,b}$ to itself 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 Huff curve defined over a finite field $\mathbb{F}_q$ and $\sharp H_{a,b}(\mathbb{F}_q) = q + 1 - t$. Then the Frobenius endomorsphim of $H_{a,b}$ satisfies*

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

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

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

$$\begin{aligned}\psi(x,y) = (\sigma^{-1}\pi\sigma)(x,y) &= (\sigma^{-1}\pi)\Big(\frac{ab(bx-ay)}{by-ax}, \frac{ab(b^2-a^2)}{by-ax}\Big)\\ &= \sigma^{-1}\Big(\frac{(ab)^q(bx-ay)^q}{(by-ax)^q}, \frac{(ab)^q(b^2-a^2)^q}{(by-ax)^q}\Big) = (x^q, y^q),\end{aligned}$$

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

Hence we have for all $P \in H_{a,b}(\overline{\mathbb{F}}_q)$, $\psi(P) = \pi(P)$ 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. Frobenius map on quadratic twists of an Huff curves

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

The quadratic twist of a Huff curve is

$$H^t_{a,b} \ : \ ax(y^2 - d) = by(x^2 - d)$$

where $a, b, d \in \mathbb{F}_q^*$ and $a^2 \neq b^2$. ($d \in \mathbb{F}_q^*$ is a non-square.) The sum of two finite points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ such that $x_1 x_2 \neq \pm d$ and $y_1 y_2 \neq \pm d$ is given by (x_3, y_3) where

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

The corresponding isomorphism $\phi : H_{a,b} \to H^t_{a,b}$ defined over $\mathbb{F}_{q^2}$ is given by $(x, y) = (\frac{x}{\sqrt{d}}, \frac{y}{\sqrt{d}})$.

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

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

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 Huff curves by extending the method in Galbraith et. al. [3].

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

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

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

By definition, $\psi(x, y) = (\phi\widehat{\pi})(\frac{x}{\sqrt{d}}, \frac{y}{\sqrt{d}}) = \phi(\frac{x^q}{\sqrt{u}^q}, \frac{y^q}{\sqrt{u}^q}) = (\sqrt{d}^{1-q}x^q, \sqrt{d}^{1-q}y^q)$ 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,

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

□

Acknoledgements
This paper is dedicated to Professor Dae San Kim who will get an honorable retirement form Sogang University in Seoul, August of 2016.

5. Conclusion

In this paper, we presented the Frobenius endomorphism of Huff curve over a finite field. Based on it, we constructed a Frobenius map defined on the quadratic twist of a Huff 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] H. M. Edwards, A normal form for elliptic curves, Bulletin of the American Mathematical Society 44(3) (2007), 393–422.
[3] 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.
[4] 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.
[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] 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.
[8] 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.
[9] N. Koblitz, *Elliptic curve cryptosystems*, Math. Comp. 48 (1987), 203–209.
[10] 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.
[11] 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