Elliptic curves in Huff's model*

Hongfeng Wu[1], Rongquan Feng[2]

1 College of Sciences, North China University of Technology, Beijing 100144, China
whfmath@gmail.com

2 LMAM, School of Mathematical Sciences, Peking University, Beijing 100871, China
fengrq@math.pku.edu.cn

Abstract

The general Huff curves which contains Huff's model as a special case is introduced in this paper. It is shown that every elliptic curve with three points of order 2 is isomorphic to a general Huff curve. Some fast explicit formulae for general Huff curves in projective coordinates are presented. These explicit formulae for addition and doubling are almost as fast as they are for the Huff curves in [9]. Finally, the number of isomorphism classes of general Huff curves defined over a finite field is enumerated.

Keywords: elliptic curve, Huff curve, isomorphism classes, scalar multiplication, cryptography

1 Introduction

The elliptic curve cryptosystem was independently proposed by Koblitz [10] and Miller [12] which relies on the difficulty of discrete logarithmic problem in the group of rational points on an elliptic curve. One of the main operations and challenges in elliptic curve cryptosystems is the scalar multiplication.

*Supported by NSF of China (No. 10990011)

The speed of scalar multiplication plays an important role in the efficiency of the whole system. Elliptic curves can be represented in different forms. To obtain faster scalar multiplications, various forms of elliptic curves have been extensively studied in the last two decades. Some important elliptic curve families include Jacobi intersections, Edward curves, Jacobi quartics, Hessian curves etc.. Details of previous works can be found in [1, 3, 9]. Recently, Joye, Tibouchi, and Vergnaud [9] revisit a model for elliptic curves over $\mathbb{Q}$ introduced by Huff [8] in 1948. They presented fast explicit formulae for point addition and doubling on Huff curves. They also addresses in [9] the problem of the efficient evaluation of pairings over Huff curves such as completeness and independence of the curve parameters.

In order to study the elliptic curve cryptosystem, one need first to answer how many curves there are up to isomorphism, because two isomorphic elliptic curves are the same in the point of cryptographic view. So it is natural to count the isomorphism classes of some kinds of elliptic curves. Some formulae about counting the number of the isomorphism classes of general elliptic curves over a finite field can be found in literatures, such as [6, 11, 13, 14].

In this paper, the general Huff curves $x(ay^2 - 1) = y(bx^2 - 1)$ which contains Huff curves $ax(y^2 - 1) = by(x^2 - 1)$ as a special case is introduced. We show that every elliptic curve with three points of order 2 is isomorphic to a general Huff curve. Some fast explicit formulae for general Huff curves in projective coordinates are presented. These explicit formulae for addition and doubling are almost as fast in the general case as they are for the Huff curves. Finally, the number of isomorphism classes of general Huff curves and Huff curves defined over a finite field is enumerated.

Throughout this paper, K will be a filed and $\mathbb{F}_q$ a finite field with q elements. The algebraic closure of K is denoted by $\overline{K}$.

2 General Huff curves

In [9], Joye, Tibouchi, and Vergnaud developed an elliptic curve model introduced by Huff [8] in 1948 to study a diophantine problem. The Huff's model for elliptic curves is given by the equation $ax(y^2 - 1) = by(x^2 - 1)$. They also presented addition formula on Huff curves. Using $(0, 0, 1)$ as the neutral element, the addition formula was given by

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{(x_1 + x_2)(1 + x_1x_2)}{(1 + x_1x_2)(1 - y_1y_2)}, \frac{(y_1 + y_2)(1 + x_1x_2)}{(1 - x_1x_2)(1 + y_1y_2)} \right)$$

in affine coordinates. Moreover, this addition law is unified, that is, it can be used to double a point. Actually, curve families $ax(y^2-1)=by(x^2-1)$ are included in curve families $x(ay^2-1)=y(bx^2-1)$. We call the curve with the equation $x(ay^2-1)=y(bx^2-1)$ the general Huff curve. For the general Huff curve $H_{a,b}: x(ay^2-1)=y(bx^2-1)$, if $a=\mu^2$ and $b=\nu^2$ are square elements of the field K, and let $x'=\nu x$ and $y'=\mu y$, then $\mu x'(y'^2-1)=\nu y'(x'^2-1)$. That is, curve families $ax(y^2-1)=by(x^2-1)$ are part of curve families $x(ay^2-1)=y(bx^2-1)$ with a,b are square elements of the field K. Note that $H_{a,b}: x(ay^2-1)=y(bx^2-1)$ is a smooth elliptic curve if $ab(a-b)\neq 0$. Let $F(X,Y,Z) := aXY^2-bX^2Y-XZ^2+YZ^2$, then the Hessian of the curve $F(X,Y,Z)=0$ is

$$H(F)=\begin{vmatrix} F_{XX} & F_{XY} & F_{XZ} \\ F_{YX} & F_{YY} & F_{YZ} \\ F_{ZX} & F_{ZY} & F_{ZZ} \end{vmatrix} = 8\begin{vmatrix} -bY & (aY-bX) & Z \\ (aY-bX) & aX & -Z \\ Z & -Z & (X-Y) \end{vmatrix},$$

where F_{XY} is the second partial derivative of the polynomial F with respect to X and Y. Since the general Huff curve is smooth, the inflection points of F are the intersection points of F and $H(F)$. Hence, it is clear that $(0,0,1)$ is an inflection point and there is no inflection points with $Z=0$.

Theorem 2.1. *Let K be a field of characteristic $\neq 2$, and let $a,b\in K$ with $a\neq b$. Then the curve*

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

is isomorphic to the elliptic curve

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

via the change of variables $\varphi(X,Y,Z)=(U,V,W)$, where

$$U=bX-aY,\ V=(b-a)Z,\ \textit{and}\ W=Y-X.$$

The inverse change is $\psi(U,V,W)=(X,Y,Z)$, where

$$X=U+aW,\ Y=U+bW,\ \textit{and}\ Z=V.$$

Proof. From $U=bX-aY$, $V=(b-a)Z$, and $W=Y-X$, we have $V^2W=(b-a)^2(Y-X)Z^2$ and $U(U+aW)(U+bW)=(b-a)^2XY(bX-aY)$. Therefore, $V^2W=U(U+aW)(U+bW)$ since $X(aY^2-Z^2)=Y(bX^2-Z^2)$.

On the other hand, since $V^2W = U(U+aW)(U+bW)$, $X = U+aW$, $Y = U + bW$, and $Z = V$, we have $W = \frac{X-Y}{a-b}$ and $U = \frac{aY-bX}{a-b}$. Therefore, $Z^2(X-Y) = XY(aY-bX)$, that is, $X(aY^2-Z^2) = Y(bX^2-Z^2)$. Obviously, the maps φ and ψ are mutually inverse to each other. $\square$

For the affine edition, the general Huff curve $x(ay^2-1) = y(bx^2-1)$ is isomorphic to $y^2 = x(x+a)(x+b)$ over K. Tt was proposed in [7] that an elliptic curve E over an algebraic number field $\mathbb{K}$ contains a copy of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ if and only if E admits one of the normal forms $y^2 = x(x-a)(x-b)$, where $a, b \in \mathbb{K}$ and $ab(a-b) \neq 0$, and E over $\mathbb{K}$ contains a copy of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ if and only if E admits one of the normal forms $y^2 = x(x^2 + 2(a^2+1)x + (a^2-1)^2))$, where $a \in \mathbb{K}$ and $a \neq 0, \pm 1$. Noting that $y^2 = x(x^2 + 2(a^2+1)x + (a^2-1)^2)) = x(x + (a+1)^2)(x + (a-1)^2)$, E contains a copy of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ if and only if E admits one of the normal forms $y^2 = x(x+t^2)(x+(t+2)^2)$, where $t \in \mathbb{K}$ and $t \neq 0, -1, -2$. For any $a, b \in \mathbb{K}$ with $a \neq b$, let $u = \dfrac{2}{b-a}$ and $t = \dfrac{2a}{b-a}$, then $\dfrac{t}{u} = a$ and $\dfrac{t+2}{u} = b$. Since $y^2 = x(x+t^2)(x+(t+2)^2)$ is isomorphic to $(\dfrac{y}{u^3})^2 = \dfrac{x}{u^2}(\dfrac{x}{u^2} + (\dfrac{t}{u})^2)(\dfrac{x}{u^2} + (\dfrac{t+2}{u})^2)$, and then is isomorphic to $y^2 = x(x+a^2)(x+b^2)$, E contains a copy of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ if and only if E is isomorphic over $\mathbb{K}$ to a Huff curve $ax(y^2-1) = by(x^2-1)$. Therefore we give another proof of Theorem 2 in [9]. Note that the j-invariant of the curve $x(ay^2-1) = y(bx^2-1)$ is $2^8 \dfrac{(a^2-ab+b^2)^3}{a^2b^2(a-b)^2}$, and the j-invariant of the curve $ax(y^2-1) = by(x^2-1)$ is $j = 2^8 \dfrac{(a^4-a^2b^2+b^4)^3}{a^4b^4(a^2-b^2)^2}$.

2.1 Huff curves and twisted Jacobi intersections curves

Twisted Jacobi intersections elliptic curves were introduced in [5]. A twisted Jacobi intersections elliptic curve over the field K is defined by the affine equations $au^2 + v^2 = 1, bu^2 + w^2 = 1$ or by the projective equations $aU^2 + V^2 = Z^2$, $bU^2 + W^2 = Z^2$, where $a, b \in K$ with $ab(a-b) \neq 0$. In [5], it was shown that a twisted Jacobi intersections curve $E_{a,b}$: $au^2 + v^2 = 1$, $bu^2 + w^2 = 1$ with $ab(a-b) \neq 0$ is a smooth curve and is isomorphic to an elliptic curve $y^2 = x(x-a)(x-b)$ over K. However, every elliptic curve over K having three K-rational points of order 2 is isomorphic to a twisted Jacobi intersections curve. Since the general Huff curve $H_{a,b}$: $x(ay^2-1)=y(bx^2-1)$ is isomorphic to $y^2=x(x+a)(x+b)$ over K, the general Huff curve $H_{a,b}: x(ay^2-1)=y(bx^2-1)$ is isomorphic to a twisted Jacobi intersections curve $-au^2+v^2=1,\ -bu^2+w^2=1$. Especially, a Huff curve $ax(y^2-1)=by(x^2-1)$ is isomorphic to a twisted Jacobi intersections curve $-a^2u^2+v^2=1,\ -b^2u^2+w^2=1$. Actually, as proposed in [9], Huff [8] considered rational distance sets S with some forms. Such a point must then satisfy the equations $x^2+a^2=u^2$ and $x^2+b^2=v^2$ with $u,v\in\mathbb{Q}$. The system of associated homogeneous equations $x^2+a^2z^2=u^2$ and $x^2+b^2z^2=v^2$ defines a curve of genus 1 in $\mathbb{P}^3$. This homogeneous equations is just a twisted Jacobi intersections curve

$$-a^2z^2+u^2=x^2, -b^2z^2+v^2=x^2.$$

It is smooth if and only if $a^2\neq b^2$ and $ab\neq 0$ according to Theorem 1 in [5].

2.2 Huff curves and twisted Edwards curves

In [2] it is proved that every Edwards curve $E_d: x^2+y^2=1+dx^2y^2$ is birationally equivalent to a Montogomery curve $M_{A,B}: By^2=x^3+Ax^2+x$ via

$$\varphi: M_{\frac{2(1+d)}{1-d},\frac{d}{1-d}} \to E_d \ \text{ with } \ (x,y)\mapsto\left(\frac{x}{y},\frac{x-1}{x+1}\right).$$

The map is not defined everywhere. However, this maps can be extended to give an everywhere-defined isomorphism between the respective desingularized projective models. The extended map takes the neutral element to the neutral element, hence, φ and φ^{-1} commute with the group structures. Moreover, the twisted Edwards curve $E_{a,d}: ax^2+y^2=1+dx^2y^2$ is isomorphic to $M_{\frac{2(a+d)}{(a-d)},\frac{4}{(a-d)}}$. Since the Huff curve $ax(y^2-1)=by(x^2-1)$ is isomorphic to $M_{\frac{a^2+b^2}{ab},\frac{1}{ab}}: \frac{1}{ab}y^2=x^3+\frac{a^2+b^2}{ab}x^2+x$, the Huff curve $ax(y^2-1)=by(x^2-1)$ is isomorphic to the Edwards curve $E_{(\frac{a-b}{a+b})^2}: x^2+y^2=1+(\frac{a-b}{a+b})^2x^2y^2$.

3 Enumeration of isomorphism classes

Let E be an elliptic curve over a field K given by a Weierstrass equation

$$E:\ Y^2=X^3+a_2X^2+a_4X+a_6$$

with $a_2, a_4, a_6 \in K$. An admissible change of variables defined over an extension field L/K in a Weierstrass equation is one of the form

$$X' = u^2X + r \text{ and } Y' = u^3Y$$

with $u, r \in L$ and $u \neq 0$. The elliptic curves E_1/K and E_2/K are said to be isomorphic over L, denote by $E_1 \cong_L E_2$, if there is an admissible change of variables defined over L transforming E_1 to E_2.

Let $E_1/K : Y^2 = X^3 + a_2X^2 + a_4X + a_6$ and $E_2/K : Y^2 = X^3 + a_2^{'}X^2 + a_4^{'}X + a_6^{'}$ be two elliptic curves defined over K. It is well known from the definition that $E_1 \cong_L E_2$ if and only if there exists $u, r \in L$ and $u \neq 0$ satisfy the following equations

$$\begin{cases} u^2a_2^{'} &= a_2 + 3r, \\ u^4a_4^{'} &= a_4 + 2ra_2 + 3r^2, \\ u^6a_6^{'} &= a_6 + ra_4 + r^2a_2 + r^3. \end{cases} \tag{1}$$

Note that E_1 and E_2 are isomorphic over $\overline{K}$ if and only if $j(E_1) = j(E_2)$. If $K = \mathbb{F}_q$ is a finite field, then the statement is not true. We have only $j(E_1) = j(E_2)$ if E_1 and E_2 are isomorphic over $\mathbb{F}_q$. The reader is referred to [15] for more results on the isomorphism of elliptic curves.

The Legendre elliptic curve over K is defined as

$$E_\lambda : y^2 = x(x-1)(x-\lambda),$$

where $\lambda \in K$. It is clear that the Legendre curve E_λ is nonsingular for $\lambda \neq 0, 1$. The points $\mathcal{O}$, $(0,0)$, $(1,0)$, and $(\lambda, 0)$ are all the 2-division points, that is, the points of order 2. The j-invariant of E_λ is $j(E_\lambda) = 2^8\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$.

In this section, let $K = \mathbb{F}_q$. It is clear that any general Huff elliptic curve is isomorphic to a Legendre curve over the algebraic closure $\overline{\mathbb{F}}_q$. From the enumeration result of the isomorphism classes of Legendre curves over $\overline{\mathbb{F}}_q$ ([6]), we have the following theorem.

Theorem 3.1. *Suppose $\mathbb{F}_q$ is a finite field with q elements and char$(\mathbb{F}_q) \neq 2, 3$. Let $\overline{N}_q$ denote the number of $\overline{\mathbb{F}}_q$-isomorphism classes of general Huff curves $H_{a,b} : x(ay^2 - 1) = y(bx^2 - 1)$(which is the same as the Huff curves $ax(y^2 - 1) = by(x^2 - 1)$) defined over $\mathbb{F}_q$ with $ab(a - b) \neq 0$. Then*

$$\overline{N}_q = \begin{cases} \dfrac{q+5}{6}, & \text{if } q \equiv 1, 7 \ (mod\ 12), \\ \dfrac{q+1}{6}, & \text{if } q \equiv 5, 11 \ (mod\ 12). \end{cases}$$

3.1 $\mathbb{F}_q$-isomorphism classes of Huff curves

Since $ax(y^2-1) = by(x^2-1)$ is $\mathbb{F}_q$-isomorphic to $y^2 = x(x+a^2)(x+b^2)$, it is also $\mathbb{F}_q$-isomorphic to $y^2 = x(x-1)(x-(1-t^2))$ by $(x,y) \to (x/a^2+1, y/a^3)$, where $t = b/a$.

Lemma 3.2. *The Huff curves $ax(y^2-1) = by(x^2-1)$ with $a, b \in \mathbb{F}_q$ and $ab(a-b) \neq 0$ (or curves $y^2 = x(x-1)(x-(1-t^2))$ with $t \in \mathbb{F}_q$ and $t \neq 0, 1$) are isomorphic to Legendre curves $y^2 = x(x-1)(x-\lambda)$ with at least one of $\lambda, 1-\lambda$ is a square element over $\mathbb{F}_q$.*

The following lemma can be gotten easily.

Lemma 3.3. *Suppose that $\mathbb{F}_q$ is a finite field with $char(\mathbb{F}_q) > 3$. Let $N(s,t)$ be the number of $a \in \mathbb{F}_q$ with $\left(\frac{a}{q}\right) = s$ and $\left(\frac{1-a}{q}\right) = t$. Then*

$$N(-1,-1) = \begin{cases} \dfrac{q-1}{4}, & \text{if } q \equiv 1 (mod\ 4), \\ \dfrac{q+1}{4}, & \text{if } q \equiv 3 (mod\ 4). \end{cases}$$

Firstly, assume that $q \equiv 1 (\mathrm{mod}\ 4)$. According to [6], we can divide the Legendre elliptic curves $E_b : y^2 = x(x-1)(x-b)$ with $b \neq 0, 1$, into the following 4 disjoint sets H_1, H_2, H_3 and H_4, where

$$\begin{aligned} H_1 &= \left\{ y^2 = x(x-1)(x-b) | \left(\tfrac{b}{q}\right) = \left(\tfrac{1-b}{q}\right) = 1 \right\}, \\ H_2 &= \left\{ y^2 = x(x-1)(x-b) | \left(\tfrac{b}{q}\right) = 1, \left(\tfrac{1-b}{q}\right) = -1 \right\}, \\ H_3 &= \left\{ y^2 = x(x-1)(x-b) | \left(\tfrac{b}{q}\right) = -1, \left(\tfrac{1-b}{q}\right) = 1 \right\}, \\ H_4 &= \left\{ y^2 = x(x-1)(x-b) | \left(\tfrac{b}{q}\right) = -1, \left(\tfrac{1-b}{q}\right) = -1 \right\}. \end{aligned}$$

From Lemma 3.3, we get that $|H_1| = \frac{q-5}{4}$ and $|H_2| = |H_3| = |H_4| = \frac{q-1}{4}$.

Therefore, We know from [6] the Legendre curves from the 3 distinct sets H_1, $H_2 \cup H_3$ and H_4 can not be $\mathbb{F}_q$-isomorphic to each other. let N_{q,H_4} be the number of $\mathbb{F}_q$-isomorphism classes of Legendre elliptic curves H_4. Then we have ([6])

$$N_{q,H_4} = \begin{cases} \dfrac{q-1}{8}, & \text{if } q \equiv 1, 17 \text{ (mod 24)}, \\ \dfrac{q+3}{8}, & \text{if } q \equiv 5, 13 \text{ (mod 24)}. \end{cases}$$

Secondly, assume that $q \equiv 3 (\text{mod } 4)$. The number of Legendre curves $E_\lambda : y^2 = x(x-1)(x-b)$ with b and $1-b$ are non-square elements equals to $\frac{q+1}{4}$. From [6], the number of curves isomorphic to a given curve with both b and $1-b$ are non-square elements equals to 3 if the j-invariant $j \neq 0$, and equals to 2 otherwise. But $j = 0$ occurs only when $q \equiv 7 (\text{mod } 12)$. Therefore, the number of $\mathbb{F}_q$-isomorphism classes of Huff curves equals to

$$\begin{cases} (\frac{q+1}{4} - 2)/3 + 1 = \frac{q+5}{12}, & \text{if } q \equiv 7 \ (\text{mod } 12), \\ (\frac{q+1}{4})/3 = \frac{q+1}{12}, & \text{if } q \equiv 11 \ (\text{mod } 12). \end{cases}$$

By subtracting above numbers from the number of $\mathbb{F}_q$-isomorphism classes of Legendre curves ([6]), we have the following enumeration result.

Theorem 3.4. *Suppose $\mathbb{F}_q$ is a finite field with q elements and $char(\mathbb{F}_q) > 3$. Let N_q be the number of $\mathbb{F}_q$-isomorphism classes of Huff curves $ax(y^2-1) = by(x^2-1)$ defined over $\mathbb{F}_q$ with $ab(a-b) \neq 0$. Then*

$$N_q = \begin{cases} \frac{q+5}{6}, & \text{if } q \equiv 1 \ (mod\ 12), \\ \frac{q+1}{6}, & \text{if } q \equiv 5 \ (mod\ 12), \\ \frac{q+1}{4}, & \text{if } q \equiv 7 \ (mod\ 12), \\ \frac{q-3}{4}, & \text{if } q \equiv 11 \ (mod\ 12). \end{cases}$$

3.2 $\mathbb{F}_q$-isomorphism classes of general Huff curves

In order to enumerate the $\mathbb{F}_q$-isomorphism classes of general Huff curves, it is sufficient to count the $\mathbb{F}_q$-isomorphism classes of elliptic curves of the form $B_{a,b} : y^2 = x(x-a)(x-b)$. For any elliptic curve $y^2 = x^3 + ax + b$ defined over $\mathbb{F}_q$, the number of elliptic curves which are $\mathbb{F}_q$-isomorphic to $y^2 = x^3 + ax + b$ equals to ([11])

$$\begin{cases} \frac{q-1}{6}, & \text{if } a = 0 \text{ and } q \equiv 1 \ (\text{ mod } 3), \\ \frac{q-1}{4}, & \text{if } b = 0 \text{ and } q \equiv 1 \ (\text{ mod } 4), \\ \frac{q-1}{2}, & \text{otherwise.} \end{cases}$$

Let E be an elliptic curve with at least one order 2 point then by moving this point to $(0,0)$ it can be changed to the form $E_{a,b} : y^2 = x^3 + ax^2 + bx$. The j-invariant of $E_{a,b}$ is $\frac{256(a^2-3b)^3}{b^2(a^2-4b)}$. Note that $j(E_{a,b}) = 0$ if and only if $a^2 = 3b$, and $j(E_{a,b}) = 1728$ if and only if $a(9b - 2a^2) = 0$ since $E_{a,b}$ is isomorphic to the elliptic curve $y^2 = x^2 - (a^2 - 3b)x + (1/2)a(9b - 2a^2)$. Every order 2 point admits this change, hence, the number of elliptic curves which is $\mathbb{F}_q$ isomorphic to $E_{a,b}$ equals to

$$\begin{cases} \dfrac{q-1}{2}, & \text{if } j = 0 \text{ and } q \equiv 1 \pmod 3, \\ \dfrac{3(q-1)}{4}, & \text{if } j = 1728 \text{ and } q \equiv 1 \pmod 4, \\ \dfrac{3(q-1)}{2}, & \text{otherwise.} \end{cases}$$

if the curve has three order 2 points.

The number of elliptic curves with three order 2 points equals to $\frac{(q-1)(q-2)}{2}$ since they admit the normal forms $y^2 = x(x-a)(x-b)$. Hence, the number of elliptic curves with only one order 2 points equals to $q(q-1) - \frac{(q-1)(q-2)}{2} - (q-1) = \frac{q(q-1)}{2}$. The number of elliptic curves $E_{a,b} : y^2 = x^3 + ax^2 + bx$ with $j(E_{a,b}) = 0$ equals to $q - 1$ since $j(E_{a,b}) = 0$ if and only if $a^2 = 3b$. Thus, if it possess three order 2 points then

$$1 = \left(\frac{a^2 - 4b}{q}\right) = \left(\frac{-b}{q}\right) = \left(\frac{-3}{q}\right).$$

Hence, the number of elliptic curves $E_{a,b} : y^2 = x^3 + ax^2 + bx$ possess three order 2 points with $j(E_{a,b}) = 0$ equals to $(q-1)$ if $q \equiv 1 \pmod 3$, and equals to 0 if $q \equiv 2 \pmod 3$. Similarly, $j(E_{a,b}) = 1728$ if and only if $a(9b - 2a^2) = 0$ and then if and only if $b = 2(a/3)^2$. Therefore, the number of elliptic curves $E_{a,b} : y^2 = x^3 + ax^2 + bx$ with $j(E_{a,b}) = 1728$ equals to $(q-1) + (q-1) = 2(q-1)$. Thus, if it possess three order 2 points then $a^2 - 4b$ is a square element in $\mathbb{F}_q$. From $9b = 2a^2$ we have $a^2 - 4b = b/2 = (a/3)^2$. Hence, the number of elliptic curves $E_{a,b} : y^2 = x^3 + ax^2 + bx$ possess three order 2 points with $j(E_{a,b}) = 1728$ equals to $\frac{3(q-1)}{2}$. Thus, the number of elliptic curves $E_{a,b} : y^2 = x^3 + ax^2 + bx$ which possess three order 2 points with $j(E_{a,b}) \neq 0, 1728$ equals to

$$\begin{cases} \dfrac{(q-1)(q-7)}{2}, & \text{if } q \equiv 1 \pmod 3, \\ \dfrac{(q-1)(q-5)}{2}, & \text{if } q \equiv 2 \pmod 3. \end{cases}$$

By the above argument, the number of $\mathbb{F}_q$-isomorphism classes of elliptic curves $B_{a,b} : y^2 = x(x-a)(x-b)$ defined over $\mathbb{F}_q$ equals to

$$\frac{q-1}{\frac{q-1}{2}} + \frac{\frac{3(q-1)}{2}}{\frac{3(q-1)}{4}} + \frac{\frac{(q-1)(q-7)}{2}}{\frac{3(q-1)}{2}} = \frac{q+5}{3}$$

if $q \equiv 1 \pmod{12}$. Other cases can be computed similarly. Therefore we have the following theorem.

Theorem 3.5. *Let $\mathbb{F}_q$ be a finite field with q elements and $char(\mathbb{F}_q) > 3$. Let N'_q denote the number of $\mathbb{F}_q$-isomorphism classes of $x(ay^2-1) = y(bx^2-1)$ defined over $\mathbb{F}_q$ with $ab(a-b) \neq 0$. Then*

$$N'_q = \begin{cases} \frac{q+5}{3}, & \text{if } q \equiv 1 \ (mod\ 12), \\ \frac{q+1}{3}, & \text{if } q \equiv 5 \ (mod\ 12), \\ \frac{q+2}{3}, & \text{if } q \equiv 7 \ (mod\ 12), \\ \frac{q-2}{3}, & \text{if } q \equiv 11 \ (mod\ 12). \end{cases}$$

4 Arithmetic on general Huff curves

Let C be a nonsingular cubic curve defined over a field K, and let O be a point on $C(K)$. For any two points P and Q, the line through P and Q meets the cubic curve C at one more point, denoted by PQ. With a point O as zero element and the chord-tangent composition PQ we can define the group law $P+Q$ by $P+Q = O(PQ)$ on $C(K)$ making $C(K)$ into an abelian group with O as zero element and $-P = P(OO)$. If O is an inflection point then $-P = PO$ and $OO = O$.

4.1 The addition law on general Huff curves

Let the line joining $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be $y = y_1 + \lambda(x - x_1) = \lambda x + \mu$, where λ is the slope of the line. Substituting this expression for y

into the Huff equation $x(ay^2-1)=y(bx^2-1)$, we get $x(a(\lambda x+\mu)^2-1)=(\lambda x+\mu)(bx^2-1)$, that is,

$$(a\lambda^2-b\lambda)x^3+(2a\lambda\mu-b\mu)x^2+(a\mu^2+\lambda-1)x+\mu=0.$$

Let $PQ=(x_3,y_3)$, then

$$x_1+x_2+x_3=-\frac{2a\lambda\mu-b\mu}{a\lambda^2-b\lambda}.$$

Hence,

$$-x_3=x_1+x_2+\frac{[2a(y_2-y_1)-b(x_2-x_1)](x_2y_1-x_1y_2)}{(y_2-y_1)(a(y_2-y_1)-b(x_2-x_1))}.$$

Noting that

$$\begin{aligned}
& (a(y_2-y_1)-b(x_2-x_1))(x_2+x_1)y_1y_2 \\
= & \left(a(x_1y_2+x_1y_2-x_2y_1-x_1y_1)-bx_2^2+bx_1^2\right)y_1y_2 \\
= & (ax_2y_2^2-bx_2y_2)y_1-(ax_1y_1^2-bx_1^2y_1)y_2+a(x_1y_2-x_2y_1)y_1y_2 \\
= & (x_2-y_2)y_1-(x_1-y_1)y_2+a(x_1y_2-x_2y_1)y_1y_2 \\
= & (x_1y_2-x_2y_1)(ay_1y_2-1),
\end{aligned}$$

we have

$$\begin{aligned}
-x_3 &= x_1+x_2-\frac{a(x_1+x_2)y_1y_2}{ay_1y_2-1}+\frac{(a(y_2-y_1)-b(x_2-x_1))(x_2+x_1)y_1y_2}{(y_1-y_2)(ay_1y_2-1)} \\
&= x_1+x_2+\frac{x_1y_2-x_2y_1}{y_1-y_2}-\frac{a(x_1+x_2)y_1y_2}{ay_1y_2-1} \\
&= \frac{x_1y_1-x_2y_2}{y_1-y_2}-\frac{a(x_1+x_2)y_1y_2}{ay_1y_2-1}.
\end{aligned} \tag{2}$$

From

$$\begin{aligned}
& (y_1-y_2)\left(ax_1x_2(y_1+y_2)+(x_1+x_2)\right) \\
= & (ax_1y_1^2+y_1)x_2-(ax_2y_2^2+y_2)x_1+(x_1y_1-x_2y_2) \\
= & (bx_1^2y_1+x_1)x_2-(bx_2y_2^2+x_2)x_1+(x_1y_1-x_2y_2) \\
= & bx_1x_2((x_1y_1-x_2y_2))+(x_1y_1-x_2y_2) \\
= & (x_1y_1-x_2y_2)(bx_1x_2+1),
\end{aligned}$$

we get

$$\frac{x_1y_1-x_2y_2}{y_1-y_2}=\frac{ax_1x_2(y_1+y_2)+(x_1+x_2)}{bx_1x_2+1}.$$

Furthermore, from formula (2) we get

$$\begin{aligned} -x_3 &= \frac{ax_1x_2(y_1+y_2)+(x_1+x_2)}{bx_1x_2+1} - \frac{a(x_1+x_2)y_1y_2}{ay_1y_2-1} \\ &= \frac{(ax_1x_2(y_1+y_2)+(x_1+x_2))(ay_1y_2-1)-a(x_1+x_2)y_1y_2(bx_1x_2+1)}{(bx_1x_2+1)(ay_1y_2-1)}. \end{aligned} \tag{3}$$

Again from

$$\begin{aligned} & (ax_1x_2(y_1+y_2)+(x_1+x_2))(ay_1y_2-1)-a(x_1+x_2)y_1y_2(bx_1x_2+1) \\ = \ & a^2x_1x_2(y_1+y_2)y_1y_2 - ax_1x_2(y_1+y_2)-(x_1+x_2)-ab(x_1+x_2)x_1x_2y_1y_2 \\ = \ & a(ax_1y_1^2x_2y_2+ax_2y_2^2x_1y_1-bx_1^2y_1x_2y_2-bx_2^2y_2x_1y_1)-ax_1x_2(y_1+y_2)-(x_1+x_2) \\ = \ & a((x_1-y_1)x_2y_2+(x_2-y_2)x_1y_1)-ax_1x_2(y_1+y_2)-(x_1+x_2) \\ = \ & -ax_2y_1y_2-ax_1y_1y_2-(x_1+x_2) \\ = \ & -(x_1+x_2)(1+ay_1y_2), \end{aligned} \tag{4}$$

we have

$$x_3 = \frac{(x_1+x_2)(ay_1y_2+1)}{(bx_1x_2+1)(ay_1y_2-1)}.$$

Similarly, by symmetry we have

$$y_3 = \frac{(y_1+y_2)(bx_1x_2+1)}{(bx_1x_2-1)(ay_1y_2+1)}.$$

we claim that the third intersection point (x_3, y_3) of the tangent line at P has coordinates

$$x_3 = \frac{2x_1(ay_1^2+1)}{(bx_1^2+1)(ay_1^2-1)}, \quad \text{and} \quad y_3 = \frac{2y_1(bx_1^2+1)}{(bx_1^2-1)(ay_1^2+1)}.$$

Note that the slope of the tangent line at P is

$$\lambda_P = \frac{ay_1^2-2bx_1y_1-1}{bx_1^2-2ax_1y_1-1}.$$

In order to prove the claim we need only to check

$$\frac{ay_1^2-2bx_1y_1-1}{bx_1^2-2ax_1y_1-1} = \frac{\dfrac{2y_1(bx_1^2+1)}{(bx_1^2-1)(ay_1^2+1)} - y_1}{\dfrac{2x_1(ay_1^2+1)}{(bx_1^2+1)(ay_1^2-1)} - x_1}.$$

This is true since the right side of the above equation is

$$
\begin{aligned}
& \frac{2y_1(bx_1^2+1)-y_1(bx_1^2-1)(ay_1^2+1)}{2x_1(ay_1^2+1)-x_1(bx_1^2+1)(ay_1^2-1)}\frac{(bx_1^2+1)(ay_1^2-1)}{(bx_1^2-1)(ay_1^2+1)} \\
= & \frac{y_1(bx_1^2+ay_1^2-abx_1^2y_1^2+3)}{x_1(bx_1^2+ay_1^2-abx_1^2y_1^2+3)}\frac{(bx_1^2+1)(ay_1^2-1)}{(bx_1^2-1)(ay_1^2+1)} \\
= & \frac{y_1(bx_1^2+1)(ay_1^2-1)}{x_1(bx_1^2-1)(ay_1^2+1)} = \frac{(ay_1^2-1)(-y_1(bx_1^2+1))}{(bx_1^2-1)(-x_1(ay_1^2+1))} \\
= & \frac{(ay_1^2-1)(y_1(bx_1^2-1)-2bx_1^2y_1)}{(bx_1^2-1)(x_1(ay_1^2-1)-2ax_1y_1^2)} = \frac{(ay_1^2-1)(x_1(ay_1^2-1)-2bx_1^2y_1)}{(bx_1^2-1)(y_1(bx_1^2-1)-2ax_1y_1^2)} \\
= & \frac{(ay_1^2-1)(x_1(ay_1^2-2bx_1y_1-1))}{(bx_1^2-1)(y_1(bx_1^2-2ax_1y_1-1))} = \frac{x_1(ay_1^2-1)(ay_1^2-2bx_1y_1-1)}{y_1(bx_1^2-1)(bx_1^2-2ax_1y_1-1)} \\
= & \frac{ay_1^2-2bx_1y_1-1}{bx_1^2-2ax_1y_1-1} = \lambda_P.
\end{aligned}
$$

Let $H_{a,b}$ be a general Huff curve $X(aY^2-Z^2)=Y(bX^2-Z^2)$. We know that $(0,0,1)$ is an inflection point and $(1,0,0)$, $(0,1,0)$ and $(a,b,0)$ are exactly the three infinite points from Section 2. For any two points $P=(X_1,Y_1,Z_1)$ and $Q=(X_2,Y_2,Z_2)$, the third intersection point (U_3,V_3,W_3) of the line joining P and Q has coordinates

$$
\begin{cases}
U_3 &= (X_1Z_2+X_2Z_1)(bX_1X_2-Z_1Z_2)(aY_1Y_2+Z_1Z_2)^2, \\
V_3 &= (Y_1Z_2+Y_2Z_1)(aY_1Y_2-Z_1Z_2)(bX_1X_2+Z_1Z_2)^2, \\
W_3 &= (b^2X_1^2X_2^2-Z_1^2Z_2^2)(a^2Y_1^2Y_2^2-Z_1^2Z_2^2).
\end{cases}
$$

Firstly, choose $O=(1,0,0)$ as then neutral element. Then for any point $P=(X_1,Y_1,Z_1)$ with $X_1Y_1Z_1\neq 0$ on the curve, the point $OP=(-Z_1^2,bX_1Y_1,bX_1Z_1)$. Furthermore $OO=(0,0,1)$, $O(a,b,0)=(0,1,0)$, $O(0,1,0)=(a,b,0)$, $O(0,0,1)=(1,0,0)$, and $-(X_1,Y_1,Z_1)=(X_1,Y_1,-Z_1)$. Hence, let $P+Q=(X_3,Y_3,Z_3)$, then

$$
\begin{cases}
X_3 &= (bX_1X_2-Z_1Z_2)(bX_1X_2+Z_1Z_2)(Z_1Z_2-aY_1Y_2), \\
Y_3 &= b(X_1Z_2+X_2Z_1)(bX_1X_2+Z_1Z_2)(Y_1Z_2+Y_2Z_1), \\
Z_3 &= b(X_1Z_2+X_2Z_1)(bX_1X_2-Z_1Z_2)(aY_1Y_2+Z_1Z_2).
\end{cases} \tag{5}
$$

The affine addition formula is

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{(bx_1x_2 + 1)(1 - ay_1y_2)}{b(x_1 + x_2)(1 + ay_1y_2)}, \frac{(y_1 + y_2)(bx_1x_2 + 1)}{(1 + ay_1y_2)(bx_1x_2 - 1)} \right).$$

Secondly, choose $O = (0, 1, 0)$ as the neutral element. Then for any point $P = (X_1, Y_1, Z_1)$ with $X_1Y_1Z_1 \neq 0$ on the curve, the point $OP = (aX_1Y_1, -Z_1^2, aY_1Z_1)$. We also have $OO = (0, 0, 1)$, $O(a, b, 0) = (1, 0, 0)$, $O(1, 0, 0) = (a, b, 0)$, $O(0, 0, 1) = (0, 1, 0)$, and $-(X_1, Y_1, Z_1) = (X_1, Y_1, -Z_1)$. Hence, let$P + Q = (X_3, Y_3, Z_3)$, then

$$\begin{cases} X_3 &= a(X_1Z_2 + X_2Z_1)(Y_1Z_2 + Y_2Z_1)(aY_1Y_2 + Z_1Z_2), \\ Y_3 &= (Z_1Z_2 - bX_1X_2)(aY_1Y_2 - Z_1Z_2)(aY_1Y_2 + Z_1Z_2), \\ Z_3 &= a(bX_1X_2 + Z_1Z_2)(aY_1Y_2 - Z_1Z_2)(Y_1Z_2 + Y_2Z_1). \end{cases} \quad (6)$$

The affine addition formula is

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{(x_1 + x_2)(1 + ay_1y_2)}{(1 + bx_1x_2)(ay_1y_2 - 1)}, \frac{(1 - bx_1x_2)(1 + ay_1y_2)}{a(y_1 + y_2)(bx_1x_2 + 1)} \right).$$

Thirdly, choose $O = (0, 0, 1)$ as the neutral element. Then for any point $P = (X_1, Y_1, Z_1)$ with $X_1Y_1Z_1 \neq 0$ on the curve, the point $OP = (aX_1Y_1, -Z_1^2, aY_1Z_1)$. Now $OO = (0, 0, 1)$ and $-(X_1, Y_1, Z_1) = (X_1, Y_1, -Z_1)$. Hence, let $P + Q = (X_3, Y_3, Z_3)$, then

$$\begin{cases} X_3 &= (X_1Z_2 + X_2Z_1)(aY_1Y_2 + Z_1Z_2)^2(Z_1Z_2 - bX_1X_2), \\ Y_3 &= (Y_1Z_2 + Y_2Z_1)(bX_1X_2 + Z_1Z_2)^2(Z_1Z_2 - aY_1Y_2), \\ Z_3 &= (b^2X_1^2X_2^2 - Z_1^2Z_2^2)(a^2Y_1^2Y_2^2 - Z_1^2Z_2^2). \end{cases} \quad (7)$$

The affine addition formula is

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{(x_1 + x_2)(ay_1y_2 + 1)}{(1 + bx_1x_2)(1 - ay_1y_2)}, \frac{(y_1 + y_2)(1 + bx_1x_2)}{(1 + ay_1y_2)(1 - bx_1x_2)} \right).$$

The Addition Law on the Huff curve $ax(y^2 - 1) = by(x^2 - 1)$. Let us consider the curve $aX(Y^2 - Z^2) = bY(X^2 - Z^2)$. For any two points $P = (X_1, Y_1, Z_1)$ and $Q = (X_2, Y_2, Z_2)$ on the curve, the third intersection point (U_3, V_3, W_3) of the line joining P and Q has coordinates ([9])

$$\begin{cases} U_3 &= (X_1Z_2 + X_2Z_1)(X_1X_2 - Z_1Z_2)(Y_1Y_2 + Z_1Z_2)^2, \\ V_3 &= (Y_1Z_2 + Y_2Z_1)(Y_1Y_2 - Z_1Z_2)(X_1X_2 + Z_1Z_2)^2, \\ W_3 &= (X_1^2X_2^2 - Z_1^2Z_2^2)(Y_1^2Y_2^2 - Z_1^2Z_2^2). \end{cases}$$

Choose $O = (1,0,0)$ as the neutral element. Then for any point $P = (X_1, Y_1, Z_1)$ with $X_1Y_1Z_1 \neq 0$ on the curve, the point $OP = (-Z_1^2, X_1Y_1, X_1Z_1)$. Furthermore $OO = (0,0,1)$, $O(a,b,0) = (0,1,0)$, $O(0,1,0) = (a,b,0)$, $O(0,0,1) = (1,0,0)$ and $-(X_1, Y_1, Z_1) = (X_1, Y_1, -Z_1)$. Hence, let $P + Q = (X_3, Y_3, Z_3)$ then

$$\left\{ \begin{array}{lcl} X_3 & = & (X_1X_2 - Z_1Z_2)(X_1X_2 + Z_1Z_2)(Z_1Z_2 - Y_1Y_2), \\ Y_3 & = & (X_1Z_2 + X_2Z_1)(X_1X_2 + Z_1Z_2)(Y_1Z_2 + Y_2Z_1), \\ Z_3 & = & (X_1Z_2 + X_2Z_1)(X_1X_2 - Z_1Z_2)(Z_1Z_2 + Y_1Y_2). \end{array} \right. \tag{8}$$

Similarly, choose $O = (0,1,0)$ as the neutral element Then for any point $P = (X_1, Y_1, Z_1)$ with $X_1Y_1Z_1 \neq 0$ on the curve, the point $OP = (X_1Y_1, -Z_1^2, Y_1Z_1)$. Now we have $OO = (0,0,1)$, $O(a,b,0) = (1,0,0)$, $O(1,0,0) = (a,b,0)$, $O(0,0,1) = (0,1,0)$, and $-(X_1, Y_1, Z_1) = (X_1, Y_1, -Z_1)$. Hence, let $P + Q = (X_3, Y_3, Z_3)$ then ([9])

$$\left\{ \begin{array}{lcl} X_3 & = & (X_1Z_2 + X_2Z_1)(Y_1Z_2 + Y_2Z_1)(Y_1Y_2 + Z_1Z_2), \\ Y_3 & = & (X_1X_2 - Z_1Z_2)(Z_1Z_2 - Y_1Y_2)(Y_1Y_2 + Z_1Z_2), \\ Z_3 & = & (X_1X_2 + Z_1Z_2)(Y_1Y_2 - Z_1Z_2)(Y_1Z_2 + Y_2Z_1). \end{array} \right. \tag{9}$$

Now we choose $O = (0,0,1)$ as the neutral element. Let $P + Q = (X_3, Y_3, Z_3)$ then ([9])

$$\left\{ \begin{array}{lcl} X_3 & = & (X_1Z_2 + X_2Z_1)(Y_1Y_2 + Z_1Z_2)^2(Z_1Z_2 - X_1X_2), \\ Y_3 & = & (Y_1Z_2 + Y_2Z_1)(X_1X_2 + Z_1Z_2)^2(Z_1Z_2 - Y_1Y_2), \\ Z_3 & = & (Z_1^2Z_2^2 - X_1^2X_2^2)(Z_1^2Z_2^2 - Y_1^2Y_2^2). \end{array} \right. \tag{10}$$

4.2 Algorithms

Noting that formula (5) and (6) are symmetric to each other, we need only to consider the formula (5) in algorithms.

Addition on $X(aY^2 - Z^2) = Y(bX^2 - Z^2)$. By formula (5), the following algorithm compute $(X_3 : Y_3 : Z_3) = (X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2)$ in $11M + 3D$ costs, i.e., 11 field multiplications and $3D$ constant multiplications by a, b and $1/b$ respectively.

$$\begin{array}{rcl} A & = & X_1X_2;\ B = Y_1Y_2;\ D = Z_1Z_2;\ E = bA;\ F = aB; \\ G & = & (X_1 + Z_1)(X_2 + Z_2) - A - D; \\ H & = & (Y_1 + Z_1)(Y_2 + Z_2) - B - D; \\ X_3 & = & (1/b) \cdot (E + D)(E - D)(D - F); \\ Y_3 & = & GH(E + D); \\ Z_3 & = & G(E - D)(F + D). \end{array}$$

By formula (7), the following algorithm compute $(X_3 : Y_3 : Z_3) = (X_1 : Y_1 : Z_1)+(X_2 : Y_2 : Z_2)$ in $12M+2D$ costs, where $2D$ are constant multiplications by a and b respectively.

$$\begin{aligned}
A &= X_1X_2;\; B = Y_1Y_2;\; D = Z_1Z_2;\; E = bA;\; F = aB;\\
G &= (X_1 + Z_1)(X_2 + Z_2) - A - D;\\
H &= (Y_1 + Z_1)(Y_2 + Z_2) - B - D;\\
L &= (D - E)(D + F);\; M = (D + E)(D - F);\\
X_3 &= GL(D + F);\; Y_3 = HM(D + E);\; Z_3 = LM.
\end{aligned}$$

Doubling on $X(aY^2 - Z^2) = Y(bX^2 - Z^2)$. By formula (5), the following algorithm compute $(X_3 : Y_3 : Z_3) = 2(X_1 : Y_1 : Z_1)$ costs $6M + 5S + 3D$, where $3D$ are constant multiplications by a, b and $1/b$ respectively.

$$\begin{aligned}
A &= X_1^2;\; B = Y_1^2;\; C = Z_1^2;\; D = bA;\; E = aB;\\
F &= (X_1 + Z_1)^2 - A - C;\\
G &= (Y_1 + Z_1)^2 - B - C;\\
X_3 &= (D - C)(D + C)(C - E);\\
Y_3 &= FG(C + D);\\
Z_3 &= F(D - C)(C + E).
\end{aligned}$$

By formula (7), the following algorithm compute $(X_3 : Y_3 : Z_3) = 2(X_1 : Y_1 : Z_1)$ in $7M + 5S + 2D$ costs, where $2D$ are constant multiplications by a and b respectively.

$$\begin{aligned}
A &= X_1^2;\; B = Y_1^2;\; C = Z_1^2;\; D = bA;\; E = aB;\\
F &= (X_1 + Z_1)^2 - A - C;\\
G &= (Y_1 + Z_1)^2 - B - C;\\
L &= (E + C)(C - D);\; M = (C + D)(C - E);\\
X_3 &= LF(C + E);\; Y_3 = GM(C + D);\; Z_3 = LM.
\end{aligned}$$

The costs of addition and doubling on the Huff curve $aX(Y^2 - Z^2) = bY(X^2 - Z^2)$ are $11M$ and $7M + 5S$, respectively in [9]. Therefore, the addition in general Huff curves $X(aY^2 - Z^2) = Y(bX^2 - Z^2)$ are almost as fast as that in the curves $aX(Y^2 - Z^2) = bY(X^2 - Z^2)$, but the general Huff curves possess more curves.

Tripling on $X(aY^2 - Z^2) = Y(bX^2 - Z^2)$.
We can get the tripling formula from addition formula when using $O =$

$(1,0,0)$ as the neutral element. Assuming that $(X_3 : Y_3 : Z_3) = 3(X_1 : Y_1 : Z_1)$, then

$$\begin{aligned} X_3 &= X_1(abX_1^2Y_1^2 - aY_1^2Z_1^2 - bX_1^2Z_1^2 - 3Z_1^4)(abX_1^2Y_1^2 + 3aY_1^2Z_1^2 + Z_1^4 - bX_1^2Z_1^2)^2; \\ Y_3 &= Y_1(abX_1^2Y_1^2 - aY_1^2Z_1^2 - bX_1^2Z_1^2 - 3Z_1^4)(abX_1^2Y_1^2 + 3bX_1^2Z_1^2 + Z_1^4 - aY_1^2Z_1^2)^2; \\ Z_3 &= Z_1(abX_1^2Y_1^2 + 3aY_1^2Z_1^2 + Z_1^4 - bX_1^2Z_1^2)(abX_1^2Y_1^2 + 3bX_1^2Z_1^2 + Z_1^4 - aY_1^2Z_1^2) \\ &\qquad \cdot (3abX_1^2Y_1^2 + aY_1^2Z_1^2 + bX_1^2Z_1^2 - Z_1^4). \end{aligned}$$

This algorithm compute $(X_3 : Y_3 : Z_3) = 3(X_1 : Y_1 : Z_1)$ costs $10M + 6S$ by using temporary variables $X_1^2, Y_1^2, Z_1^2, Z_1^4, X_1^2Y_1^2, Y_1Z_1^2, X_1Z_1^2$.

Similarly, we can also get the tripling formula from addition formula when using $O = (0,0,1)$ as the neutral element. Assuming that $(X_3 : Y_3 : Z_3) = 3(X_1 : Y_1 : Z_1)$, then

$$\begin{aligned} X_3 &= X_1(Z_1^4 - bX_1^2Z_1^2 + 3aY_1^2Z_1^2 + abX_1^2Y_1^2)^2(3Z_1^4 + bX_1^2Z_1^2 + aY_1^2Z_1^2 - abX_1^2Y_1^2); \\ Y_3 &= Y_1(Z_1^4 + 3bX_1^2Z_1^2 - aY_1^2Z_1^2 + abX_1^2Y_1^2)^2(3Z_1^4 + bX_1^2Z_1^2 + aY_1^2Z_1^2 - abX_1^2Y_1^2); \\ Z_3 &= Z_1(Z_1^4 + 3bX_1^2Z_1^2 - aY_1^2Z_1^2 + abX_1^2Y_1^2)(Z_1^4 - bX_1^2Z_1^2 - aY_1^2Z_1^2 - 3abX_1^2Y_1^2) \\ &\qquad \cdot (Z_1^4 - bX_1^2Z_1^2 + 3aY_1^2Z_1^2 + abX_1^2Y_1^2). \end{aligned}$$

The following formula can be used to triple the points on general Huff curves which is independent with the curve parameter a and b.

$$\begin{aligned} X_3 &= X_1(Z_1^4 - X_1^2Z_1^2 + 3Y_1^2Z_1^2 + X_1^2Y_1^2)^2(3Z_1^4 + X_1^2Z_1^2 + Y_1^2Z_1^2 - X_1^2Y_1^2); \\ Y_3 &= Y_1(Z_1^4 + 3X_1Z_1 - Y_1^2Z_1^2 + X_1^2Y_1^2)^2(3Z_1^4 + X_1^2Z_1^2 + Y_1^2Z_1^2 - X_1^2Y_1^2); \\ Z_3 &= Z_1(Z_1^4 + 3X_1Z_1 - Y_1^2Z_1^2 + X_1^2Y_1^2)(Z_1^4 - X_1^2Z_1^2 - Y_1^2Z_1^2 - 3X_1^2Y_1^2) \\ &\qquad \cdot (Z_1^4 - X_1^2Z_1^2 + 3Y_1^2Z_1^2 + X_1^2Y_1^2). \end{aligned}$$

This algorithm compute $(X_3 : Y_3 : Z_3) = 3(X_1 : Y_1 : Z_1)$ in $10M + 6S + 3D$ costs by using temporary variables $X_1^2, Y_1^2, Z_1^2, Z_1^4, X_1^2Y_1^2, Y_1Z_1^2, X_1Z_1^2$.

References

[1] D. J. Bernstein, and T. Lange, Explicit-formulae database. URL: http://www.hyperelliptic.org/EFD.

[2] D. J. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters, Twisted Edwards curves, In AFRICACRYPT 2008, LNCS 5023, 389-405, Springer, 2008.

[3] D. J. Bernstein and T. Lange, Analysis and optimization of elliptic-curve single-scalar multiplication, Cryptology ePrint Archive, Report 2007/455.

[4] W. Castryck, S.D. Galbraith and R. Rezaeian Farashahi, Efficient arithmetic on elliptic curves using a mixed Edwards-Montgomery representation, eprint 2008/218.

[5] R. Feng, M. Nie and F. Wu, Twisted Jacobi intersections curvesTAMC 2010, LNCS, 6108, pp 199-210, Springer, 2010. Cryptology ePrint Archive, Report 2009/597.

[6] R. Feng and H. Wu, On the isomorphism classes of Legendre elliptic curves over finite fields, arXiv:1001.2871, 2010.

[7] G. Fung, H. Ströher, H. Williams and H. Zimmer, Torsion groups of elliptic curves with integral j-invariant over pure cubic fields, Journal of Number Theory, Volume 36, Issue 1, September 1990, Pages 12-45.

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

[9] Marc Joye, Mehdi Tibouchi, and Damien Vergnaud, Huff's model for elliptic curves, In G.Hanrot, F.Morain and E. Thomé, Eds, Algorithmic Number Theory (ANTS-IX), LNCS 6197, pp. 234-250, Springer, 2010.

[10] N. Koblitz, Elliptic curve cryptosystems, Math. Comp., 48(177), (1987), 203-209.

[11] A.J. Menezes, Elliptic Curve Public Key Cryptosystems, Kluwer Academic Publishers, 1993.

[12] V.S. Miller, Use of elliptic curves in cryptography, Advances in Cryptology-Crypto 1985, Lecture Notes in Comp. Sci., vol. 218, Springer-Verlag, 1986, 417-426.

[13] R. Rezaeian Farashahi and I. E. Shparlinski. On the number of distinct elliptic curves in some families, Designs, Codes and Cryptography, 83-99, Vol.54, No.1, 2010.

[14] R. Schoof, Nonsigular plane cubic curves over finite field, J. Combine, Theory Ser. A 46(1987), 183-211.

[15] J.H. Silverman, The Arithmetic of Elliptic Curves, volume 106 of Graduate Texts in Mathematics, Springer-Verlag, 1986.