Efficient Arithmetic on Hessian Curves over Fields of Characteristic Three

Reza R. Farashahi[1,2], Hongfeng Wu[3], Chang-An Zhao[4]

[1] Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
[2] Department of Mathematical Sciences, Isfahan University of Technology, P.O. Box 85145, Isfahan, Iran
r.rezaeian@gmail.com
[3] College of Sciences, North China University of Technology, Beijing 100144, China
whfmath@gmail.com
[4] School of Computer Science and Educational Software, Guangzhou University, Guangzhou 510006, China
changanzhao@gzhu.edu.cn

Abstract. This paper presents new explicit formulas for the point doubling, tripling and addition for Hessian curves and their equivalent Weierstrass curves over finite fields of characteristic three. The cost of basic point operations is lower than that of all previously proposed ones. The new doubling, mixed addition and tripling formulas in projective coordinates require $3\mathbf{M} + 2\mathbf{C}$, $8\mathbf{M} + 1\mathbf{C} + 1\mathbf{D}$ and $4\mathbf{M} + 4\mathbf{C} + 1\mathbf{D}$ respectively, where $\mathbf{M}$, $\mathbf{C}$ and $\mathbf{D}$ is the cost of a field multiplication, a cubing and a multiplication by a constant. Finally, we present several examples of ordinary elliptic curves in characteristic three for high security levels.

Keywords: Elliptic curve, Hessian curve, scalar multiplication, cryptography

1 Introduction

Elliptic curve cryptosystems which was discovered by Neal Koblitz [14] and Victor Miller [17] independently requires smaller key sizes than the other public cryptosystems such as RSA at the same level of security. For example, a 160-bit elliptic curve key is competitive with a 1024-bit RSA key at the AES 80-bit security level. Thus it may be advantageous to use elliptic curve cryptosystems in resource-constrained environments, such as smart cards and embedded devices.

Scalar multiplication is a central operation in elliptic curve cryptographic schemes. There are numerous investigations of fast point multiplication on elliptic curves over large prime fields or binary fields. We refer to [3, 9, 7] for the two cases. Note that ordinary elliptic curves in characteristic three could be applied in cryptographic schemes. For example, Koblitz implemented the digital signature algorithm on a special family of supersingular elliptic curves in characteristic three with great efficiency [15]. Compared to elliptic curves on large prime fields or binary fields, Smart *et al.* first pointed out that ordinary elliptic curve in characteristic three can be an alternative for implementing elliptic curve cryptosystems [21]. Recently, the improved formulas on this case are given in [18, 13]. In [11], Hisil *et al.* given a new tripling formulas for Hessian curve in characteristic three. The generalized form of Hessian curves have been presented by Farashahi, Joye, Bernstein, Lange and Kohel [6, 4].

The goal of the present work is to speed up scalar multiplication on ordinary elliptic curves in characteristic three. We study the Hessian curves and their birationally equivalent Weierstraß elliptic curves over finite fields of characteristic 3. The main contribution of this paper is given as follows:

- The new addition, doubling and tripling formulas are presented for Hessian curves over finite fields of characteristic 3. These formulas are the fastest known in the literature and have the feature of being unified.
- The doubling and tripling formulas are complete for all input points in the rational group of the Hessian curves. Furthermore, the unified addition formulas are valid for all input points in the rational subgroup which is employed in practical cryptographic applications.
- A modified projective coordinate system is presented for the Weierstraß elliptic curves with a rational point of order 3 over finite fields of characteristic 3. It is named as the scaled projective coordinate system which offers better performance than other projective coordinate systems.
- The basic point operations of addition, doubling, and tripling are investigated in the new scaled coordinate system for Weierstraß curves. The proposed formulas have the same cost as the proposed formulas for Hessian curves which are faster than the previous known results.
- Examples of ordinary elliptic curves over characteristic three are provided for different security levels.

The paper is organized as follows. §2 recalls the necessary background for Hessian curves. §3 presents the new addition and doubling formulas for Hessian curves. §4 describes the birational equivalence between Hessian and Weierstraß forms. §5 present new tripling formulas and provide the addition and doubling formulas using the simple map between the Hessian and the equivalent Weierstraß form. §6 gives the efficiency consideration and timing results and §7 concludes the paper.

2 Background on Hessian Curves

A *Hessian curve* over a field $\mathbb{F}$ is given by the cubic equation

$$\mathrm{H}_d : \ x^3 + y^3 + 1 = dxy \,, \tag{1}$$

for some $d \in \mathbb{F}$ with $d^3 \neq 27$ [10]. Furthermore, the generalized form of Hessian curves, called twisted Hessian as well, have been studied in [6, 4]. A generalized Hessian curve $\mathrm{H}_{c,d}$ over $\mathbb{F}$ is defined by the equation

$$\mathrm{H}_{c,d} \ : \ x^3 + y^3 + c = dxy \ \ ,$$

where $c, d \in \mathbb{F}$ with $c \neq 0$ and $d^3 \neq 27c$. Clearly, a Hessian curve H_d is a generalized Hessian curve $\mathrm{H}_{c,d}$ with $c = 1$. Furthermore, the generalized Hessian curve $\mathrm{H}_{c,d}$ over $\mathbb{F}$, via the map $(x, y) \mapsto (\widetilde{x}, \widetilde{y})$ given by $\widetilde{x} = x/\zeta$, $\widetilde{y} = y/\zeta$, with $\zeta^3 = c$, is isomorphic to the Hessian curve $\mathrm{H}_{\frac{d}{\zeta}}$: $\widetilde{x}^3 + \widetilde{y}^3 + 1 = \frac{d}{\zeta}\widetilde{x}\widetilde{y}$. So, a generalized Hessian curve $\mathrm{H}_{c,d}$ is birationally equivalent to a Hessian curve if c is a cube in $\mathbb{F}$. In particular, a generalized Hessian curve over the finite field $\mathbb{F}_q$ of characteristic 3 is a Hessian curve.

The sum of two (different) points (x_1, y_1), (x_2, y_2) on $\mathrm{H}_{c,d}$ is the point (x_3, y_3) given by

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

The doubling of the point (x_1, y_1) on $\mathrm{H}_{c,d}$ is the point (x_3, y_3) given by

$$x_3 = \frac{y_1(c - {x_1}^3)}{{x_1}^3 - {y_1}^3} \quad \text{and} \quad y_3 = \frac{x_1({y_1}^3) - c}{{x_1}^3 - {y_1}^3} \ .$$

Also, the inverse of the point (x_1, y_1) on $\mathrm{H}_{c,d}$ is the point (y_1, x_1).

The projective closure of the curve $\mathrm{H}_{c,d}$ is

$$\mathbf{H}_{c,d} : \ X^3 + Y^3 + cZ^3 = dXYZ \ .$$

The neutral element of the group of $\mathbb{F}$-rational points of $\mathbf{H}_{c,d}$ is the point at infinity $(1 : -1 : 0)$ and the inverse of the point $P = (X_1 : Y_1 : Z_1)$ on $\mathbf{H}_{c,d}$, is the point $-P = (Y_1 : X_1 : Z_1)$.

The sum of the points $(X_1 : Y_1 : Z_1)$, $(X_2 : Y_2 : Z_2)$ on $\mathbf{H}_{c,d}$ is the point $(X_3 : Y_3 : Z_3)$ with

$$X_3 = X_2 Z_2 {Y_1}^2 - X_1 Z_1 {Y_2}^2, \quad Y_3 = Y_2 Z_2 {X_1}^2 - Y_1 Z_1 {X_2}^2, \quad Z_3 = X_2 Y_2 {Z_1}^2 - X_1 Y_1 {Z_2}^2 \ . \tag{2}$$

The doubling of the point $(X_1 : Y_1 : Z_1)$ on $\mathbf{H}_{c,d}$ is the point $(X_3 : Y_3 : Z_3)$ given by

$$X_3 = Y_1(c{Z_1}^3 - {X_1}^3), \quad Y_3 = X_1({Y_1}^3 - c{Z_1}^3), \quad Z_3 = Z_1({X_1}^3 - {Y_1}^3) \ . \tag{3}$$

We note that the addition formulas (2) is not *unified*, i.e., the formulas do not work to double a point. The following set of formulas are unified which make the generalized Hessian curves interesting against side-channel attacks [1, 2].

The sum of the points $(X_1 : Y_1 : Z_1)$ and $(X_2 : Y_2 : Z_2)$ on $\mathbf{H}_{c,d}$ is the point $(X_3 : Y_3 : Z_3)$ given by

$$X_3 = cY_2 Z_2 {Z_1}^2 - X_1 Y_1 {X_2}^2, \quad Y_3 = X_2 Y_2 {Y_1}^2 - cX_1 Z_1 {Z_2}^2, \quad Z_3 = X_2 Z_2 {X_1}^2 - Y_1 Z_1 {Y_2}^2 \ . \tag{4}$$

Furthermore, by the swapping the order of the points in the addition formulas (4), we obtain the following unified formulas.

$$X_3 = cY_1 Z_1 {Z_2}^2 - X_2 Y_2 {X_1}^2, \quad Y_3 = X_1 Y_1 {Y_2}^2 - cX_2 Z_2 {Z_1}^2, \quad Z_3 = X_1 Z_1 {X_2}^2 - Y_2 Z_2 {Y_1}^2 \ . \tag{5}$$

We recall [6, Propositions 1], which describes the exceptional cases of the addition formulas (2).

Proposition 1. *The addition formulas* (2) *work for all pairs of points* P_1, P_2 *on* $\mathbf{H}_{c,d}$ *if and only if* $P_1 - P_2$ *is not a point at infinity.*

If the curve $\mathbf{H}_{c,d}$ over $\mathbb{F}$ has only one $\mathbb{F}$-rational point at infinity, i.e., if $\mathbb{F}$ has only one third root of unity, then the addition formulas (2) work for all *distinct* pairs of $\mathbb{F}$-rational inputs. This happens in particular for generalized Hessian curves $\mathbf{H}_{c,d}$ over $\mathbb{F}_{3^n}$.

Let $\mathcal{T}_1$, be the set of 3-torsion points of $\mathbf{H}_{c,d}$ with Y-coordinate equals 0. That is,

$$\mathcal{T}_1 = \left\{(-\zeta : 0 : 1) \mid \zeta \in \overline{\mathbb{F}},\ \zeta^3 = c\right\}.$$

We also recall [6, Propositions 2], that explains the exceptional cases of the addition formulas (4).

Proposition 2. *The addition formulas* (4) *work for all pairs of points* P_1, P_2 *on* $\mathbf{H}_{c,d}$ *if and only if* $P_1 - P_2 \notin \mathcal{T}_1$.

Similarly, the addition formulas (5) work for all pairs of points P_1, P_2 on $\mathbf{H}_{c,d}$ if and only if $P_1 - P_2$ is not a 3-torsion point of $\mathbf{H}_{c,d}$ with X-coordinate equals 0. So, the set of formulas (4) and (5) are complement of each other, i.e., if formulas (4) do not work for the pair of inputs P_1, P_2, then the other do work.

As a consequence, the doubling formulas (3) work for all points of the curve $\mathbf{H}_{c,d}$. Moreover, for the subgroup $\mathcal{H}$ of $\mathbf{H}_{c,d}(\overline{\mathbb{F}})$ disjoint from $\mathcal{T}_1$, the addition formulas (4) (and (5)) work for all pairs of points in $\mathcal{H}$.

We note that for Hessian curves over $\mathbb{F}_q$ of characteristic 3, the set $\mathcal{T}_1$ equals $\{(-1 : 0 : 1)\}$.

3 Explicit Formulas for Hessian curves in Characteristic 3

From now on, we let $\mathbb{F}_q$ be a finite field of characteristic 3, i.e., $q = 3^k$ for some positive integer k. We consider the family of Hessian curves H_d over $\mathbb{F}_q$ given by (1).

We recall (see § 2) that the family of Hessian curves and generalized Hessian are the same up to isomorphism over $\mathbb{F}_q$. Therefore, any result on efficiency of the arithmetic of Hessian curves can be applied for the generalized Hessian curves. Furthermore, we recall from [6, Theorem 5] that the number of $\mathbb{F}_q$-isomorphism classes of the family of Hessian (or generalized Hessian) curves over $\mathbb{F}_q$ is $q - 1$.

In this section, we present fast and efficient addition, doubling, tripling formulas for Hessian curves over a field $\mathbb{F}$ of characteristic 3.

3.1 Addition

The point addition algorithms for formulas (2) are described in [5, 12, 20] with the cost of 12**M**. Also, these addition formulas can be performed in a parallel way, see [20]. In particular, the addition formulas (2) in a parallel environment using $3, 4$ or 6 processors require $4\mathbf{M}$, $3\mathbf{M}$ or $2\mathbf{M}$, respectively.

Furthermore, from the addition formulas (2), the sum of the points $(X_1 : Y_1 : Z_1)$, $(X_2 : Y_2 : Z_2)$ on H_d is the point $(X_3 : Y_3 : Z_3)$ given by

$$X_3 = Z_1 Z_2 (X_2 Z_2 {Y_1}^2 - X_1 Z_1 {Y_2}^2), \quad Y_3 = Z_1 Z_2 (Y_2 Z_2 {X_1}^2 - Y_1 Z_1 {X_2}^2),$$

$$\begin{aligned} Z_3 &= Z_1 Z_2 (X_2 Y_2 {Z_1}^2 - X_1 Y_1 {Z_2}^2) = Z_1^3 (X_2 Y_2 Z_2) - Z_2^3 (X_1 Y_1 Z_1) \\ &= Z_1^3 (X_2^3 + Y_2^3 + Z_2^3)/d - Z_2^3 (X_1^3 + Y_1^3 + Z_1^3)/d \\ &= (X_2 Z_1 + Y_2 Z_1 - X_1 Z_2 - Y_1 Z_2)^3 / d. \end{aligned}$$

Using the next algorithm, the cost of above formulas is $10\mathbf{M} + 1\mathbf{C} + 1\mathbf{D}$, where $1\mathbf{D}$ is the cost of the multiplication by the constant $1/d$.

$$\begin{gathered} A = X_2 Z_1,\ B = Y_2 Z_1,\ C = X_1 Z_2,\ D = Y_1 Z_2,\ E = AD,\ F = BC, \\ X_3 = DE - BF, \quad Y_3 = CF - AE, \quad Z_3 = (1/d)(A + B - C - D)^3 \ . \end{gathered} \tag{6}$$

Also, the mixed addition formulas requires $8\mathbf{M} + 1\mathbf{C} + 1\mathbf{D}$. We note that the addition algorithm (6) is not unified.

The next algorithm evaluates the unified addition formulas (4) for the Hessian curve H_d with $12\mathbf{M}$.

$$\begin{gathered} A = X_1 X_2,\ B = Y_1 Y_2,\ C = Z_1 Z_2,\ D = X_1 Z_2,\ E = Y_1 X_2,\ F = Z_1 Y_2, \\ X_3 = CF - AE, \quad Y_3 = BE - CD, \quad Z_3 = AD - BF \ . \end{gathered}$$

The mixed addition formulas requires $10\mathbf{M}$ by setting $Z_2 = 1$. Furthermore, the addition formulas (4) can be performed in a parallel way. The following addition algorithm is similar to the addition algorithm (6) which requires $10\mathbf{M}+1\mathbf{C}+1\mathbf{D}$.

$$\begin{gathered} A = Z_2 X_1,\ B = X_2 X_1,\ C = Y_1 Y_2,\ D = Z_1 Y_2,\ E = AD,\ F = BC, \\ X_3 = DE - BF, \quad Y_3 = CF - AE, \quad Z_3 = (1/d)(A + B - C - D)^3 \ . \end{gathered}$$

Moreover, this addition algorithm is unified. Also, the cost of the mixed addition formulas is $8\mathbf{M} + 1\mathbf{C} + 1\mathbf{D}$ by setting $X_1 = 1$.

3.2 Doubling

From the doubling formulas (3), the doubling of the point $(X_1 : Y_1 : Z_1)$ on H_d is the point $(X_3 : Y_3 : Z_3)$ given by

$$X_3 = Y_1 (Z_1 - X_1)^3, \quad Y_3 = X_1 (Y_1 - Z_1)^3, \quad Z_3 = Z_1 (X_1 - Y_1)^3 \ .$$

The following algorithm performs above doubling formulas which requires $3\mathbf{M}+2\mathbf{C}$:

$$\begin{gathered} A = (X_1 - Y_1)^3,\ B = (Y_1 - Z_1)^3, \\ X_3 = -Y_1 (A + B), \quad Y_3 = X_1 B, \quad Z_3 = Z_1 A \ . \end{gathered}$$

4 The equivalent Weierstraß form in Characteristic 3

As before, $\mathbb{F}_q$ is a finite field of characteristic 3. We note that every Hessian curve H_d over $\mathbb{F}_q$ has a point of order 3. Moreover, every elliptic curve over $\mathbb{F}_q$ with a point of order 3 can be given in generalized Hessian form (see [6]) and so in Hessian form. From [21], we recall that an ordinary elliptic curve over $\mathbb{F}_q$ has a point of order 3 if and only if it can be written in the form $y^2 = x^3 + x^2 + b$, for some $b \in \mathbb{F}_q$. Therefore, we have the birational equivalence between these two forms.

The Hessian curve H_d, given by (1) with $d \neq 0$, via the map $(x, y) \mapsto (u, v)$ defined by

$$u = -(x + y)/d \quad \text{and} \quad v = -(x - y)/d$$

is birationally equivalent to the ordinary elliptic curve E_b in Weierstraß form

$$E_b : v^2 = u^3 + u^2 + b,$$

where $b = -1/d^3$. The inverse map $(u, v) \mapsto (x, y)$ is given by

$$u = d(x + y) \quad \text{and} \quad v = d(x - y).$$

The sum of two (different) points (x_1, y_1), (x_2, y_2) on E_b is the point (x_3, y_3) given by

$$x_3 = \lambda^2 - x_1 - x_2 - 1, \quad \text{and} \quad y_3 = \lambda(x_1 - x_3) - y_1,$$

where $\lambda = (y_2 - y_1)/(x_2 - x_1)$.

The doubling of the point (x_1, y_1) on E_b is the point (x_3, y_3) given by

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

where $\lambda = ax_1/y_1$. Also, the inverse of the point (x_1, y_1) on E_b is the point $(x_1, -y_1)$. Furthermore, the tripling of the point (x_1, y_1) on E_b is the point (x_3, y_3) given by

$$x_3 = \frac{(x_1^3 + b)^3 - bx_1^3}{(x_1 + b)^2}, \quad \text{and} \quad y_3 = \frac{y_1^9 - y_1^3(x_1^3 + b)^2}{(x_1 + b)^3}. \tag{7}$$

In projective model, the point (X, Y, Z) on the projective curve

$$\mathbf{H}_d : X^3 + Y^3 + Z^3 = dXYZ,$$

is mapped to the point $(-(X + Y), -(X - Y), dZ)$ on the projective Weierstraß curve

$$\mathbf{E}_b : WV^2 = U^3 + U^2W + bW^3,$$

where $b = -1/d^3$. Furthermore, via the inverse map, the point $(U : V : W)$ on $\mathbf{E}_b$ is corresponded to the point $(U + V, U - V, W/d)$ on $\mathbf{H}_d$. So, we suggest to use the scaled projective coordinate system (U, V, T), where $dT = W$ and (U, V, W) is a point on $\mathbf{E}_b$.

5 Explicit Formulas for Weierstraß form

Here, we consider elliptic curves in Weierstraß form

$$\mathbf{E}_b : V^2W = U^3 + U^2W + bW^3,$$

where b is in finite field $\mathbb{F}_q$ of characteristic 3. We let $b = -1/d^3$ for $d \in \mathbb{F}_q$. We use the scaled projective system (U, V, T) and call the point (U, V, T) a scaled point, where $T = W/d$ and (U, V, W) is a point on $\mathbf{E}_{-1/d^3}$. From §4, we recall that the scaled point (U, V, T) on $\mathbf{E}_b$ is corresponded to the point $(U+V, U-V, T)$ on the Hessian curve $\mathbf{H}_d$. Furthermore, the point (X, Y, Z) on $\mathbf{H}_d$ is corresponded to the scaled point $(-(X+Y), -(X-Y), Z)$ on $\mathbf{E}_b$. In other words, all addition and doubling formulas for the Hessian curve H_d can be applied for the elliptic curve E_b with the same cost. Clearly, the outcome formulas via these linear transformation save the property of being unified.

For example, the addition algorithm (5) for H_d can be used to obtain the following addition algorithm for the Weierstraß form E_b. The sum of the scaled points (U_1, V_1, T_1), (U_2, V_2, T_2) on $\mathbf{E}_b$ with $b = -1/d^3$ is the scaled point (U_3, V_3, T_3) given by the next algorithm.

$$\begin{gathered}
X_1 = U_1 + V_1,\ Y_1 = U_1 - V_1,\ X_2 = U_2 + V_2,\ Y_2 = U_2 - V_2,\\
A = T_2X_1,\ B = X_2X_1,\ C = Y_1Y_2,\ D = T_1Y_2,\ E = AD,\ F = BC,\\
G = DE,\ H = BF,\ I = CF,\ J = AE,\\
U_3 = -G + H - I + J,\ V_3 = -G + H + I - J,\ T_3 = (1/d)(A + B - C - D)^3\ .
\end{gathered}$$

The above addition algorithm is unified with the cost of $10\mathbf{M} + 1\mathbf{C} + 1\mathbf{D}$. Furthermore, the mixed addition algorithm is with the cost of $8\mathbf{M} + 1\mathbf{C} + 1\mathbf{D}$ by setting $X_1 = 1$, i.e., $V_1 = 1 - U_1$.

5.1 Point Tripling

When implementing scalar multiplication on elliptic curves over finite fields of characteristic three, it is convenient to choose a base three expansion for an exponent k since the cubing operation in the finite field is cheaper than other basic operations. Now point tripling is considered as follows.

From the affine tripling formulas (7) in Section 4, the tripling of the scaled point (U_1, V_1, T_1) on $\mathbf{E}_{-1/d^3}$ is the point (U_3, V_3, T_3) given by

$$\begin{aligned}
U_3 &= (U_1^3 - T_1^3)(U_1^9 - T_1^9 + d^3U_1^3T_1^6),\\
V_3 &= d^3V_1^3T_1^3(V_1^2 - U_1^2 - T_1^2 - U_1T_1)^3,\\
T_3 &= d^2(U_1^9T_1^3 - T_1^{12}).
\end{aligned} \tag{8}$$

Then, we have

$$\begin{aligned}
U_3 &= (U_1 - T_1)^3(d^3V_1^6T_1^3 - d^3U_1^6T_1^3 + d^3U_1^3T_1^6)\\
&= -d^3T_1^3 \cdot (U_1 - T_1)^3(U_1^6 - V_1^6 - U_1^3T_1^3)\\
&= -d^3T_1^3 \cdot (U_1 - T_1)^3(U_1^2 - V_1^2 - U_1T_1)^3,\\
V_3 &= -d^3T_1^3 \cdot V_1^3(U_1^2 + U_1T_1 + T_1^2 - V_1^2)^3,\\
T_3 &= -d^3T_1^3 \cdot (T_1^9 - U_1^9)/d.
\end{aligned}$$

So, we obtain

$$\begin{aligned}U_3 &= (U_1 - T_1)^3(U_1^2 - V_1^2 - U_1T_1)^3,\\ V_3 &= V_1^3(U_1^2 + U_1T_1 + T_1^2 - V_1^2)^3,\\ T_3 &= (T_1^9 - U_1^9)/d.\end{aligned} \tag{9}$$

We also write

$$\begin{aligned}U_1^2 + U_1T_1 + T_1^2 - V_1^2 &= (U_1 - T_1 + V_1)(U_1 - T_1 - V_1),\\ U_1^2 - V_1^2 - U_1T_1 &= (U_1^2 + U_1T_1 + T_1^2 - V_1^2) + U_1T_1 - T_1^2\ .\end{aligned}$$

Then, we propose the following very fast point tripling algorithm.

$$\begin{gathered}A = U_1 - T_1,\ B = (A + V_1)(A - V_1),\ D = A(B + T_1A),\\ U_3 = D^3,\ V_3 = (V_1B)^3,\ T_3 = -(1/d)A^9\ .\end{gathered}$$

We see that the cost for above point tripling algorithm is $4\mathbf{M} + 4\mathbf{C} + 1\mathbf{D}$. The tripling algorithm works for all inputs in $\mathbf{E}_{-1/d^3}$. We note that above tripling algorithm can be used to obtain a tripling algorithm with the same cost for Hessian curves over $\mathbb{F}_q$.

6 Curve Parameters and Operation Count Comparison

In [21], Smart *et al.* provided an elliptic curve suitable for the current security level. According to the methods in [19, 8], more ordinary curves over finite fields of characteristic three for high security level can be generated in the appendix.

The efficiency of implementing elliptic curve cryptosystems depends on the speed of basic point operations. In this section, we will compare the new formulas for point operations with the previously known results on the corresponding curve.

We first recall the previous results on ordinary curves in characteristic three. In [13], Kim *et al.* propose a type of projective coordinates(ML-coordinates) which consist of four variables and the relationship between it and affine coordinates is $(X, Y, Z, T) \leftrightarrow (X/T, Y/Z^3),$ where $T = Z^2$. In ML-coordinates, the doubling, mixed addition and tripling formulas in projective coordinates require $5\mathbf{M}+3\mathbf{S}+3\mathbf{C}$, $8\mathbf{M}+2\mathbf{C}$ and $6\mathbf{M}+6\mathbf{C}$ respectively. It was noticed that a tripling algorithm cost $5\mathbf{M} + 5\mathbf{C} + 1\mathbf{D}$ using Jacobian projective coordinates in [18].

For convenience, we summarize all results into the following Table 1. From the table, we can see that the new proposed formulas are always more efficient than all previous formulas published for basic point operations on curves.

7 Conclusion

In this paper, a new basic operation formulas are presented for Hessian curves over fields of characteristic 3. Also, new point representation scaled projective is introduced for Weierstrass elliptic curves in characteristic three. The efficient basic group operations are provided for the Weierstraß form.

Coordinate System	Mixed addition	Doubling	Tripling
Projective[21]	$9\mathbf{M} + 2\mathbf{S} + 1\mathbf{C}$	$6\mathbf{M} + 0\mathbf{S} + 3\mathbf{C}$	$7\mathbf{M} + 2\mathbf{S} + 5\mathbf{C}$
Jacobian[21]	$7\mathbf{M} + 3\mathbf{S} + 2\mathbf{C}$	$6\mathbf{M} + 2\mathbf{S} + 3\mathbf{C}$	$5\mathbf{M} + 1\mathbf{S} + 4\mathbf{C} + 1\mathbf{D}$
López Dahab[21]	$10\mathbf{M} + 3\mathbf{S}$	$7\mathbf{M} + 4\mathbf{S} + 2\mathbf{C}$	$10\mathbf{M} + 3\mathbf{S} + 5\mathbf{C}$
Projective in Hessian form[21]	$10\mathbf{M}$	$3\mathbf{M} + 3\mathbf{C}$	$-$
Projective in Hessian form[11]	-	-	$6\mathbf{M} + 4\mathbf{C} + 2\mathbf{D}$
Jacobian[18]	$7\mathbf{M} + 3\mathbf{S} + 2\mathbf{C} + 1\mathbf{D}$	$5\mathbf{M} + 2\mathbf{S} + 3\mathbf{C}$	$3\mathbf{M} + 2\mathbf{S} + 5\mathbf{C} + 1\mathbf{D}$
ML-coordinates [13]	$8\mathbf{M} + 2\mathbf{C}$	$5\mathbf{M} + 3\mathbf{S} + 3\mathbf{C}$	$6\mathbf{M} + 6\mathbf{C}$
Hessian form	$8\mathbf{M} + 1\mathbf{C} + 1\mathbf{D}$	$3\mathbf{M} + 2\mathbf{C}$	$4\mathbf{M} + 4\mathbf{C} + 1\mathbf{D}$
scaled projective	$8\mathbf{M} + 1\mathbf{C} + 1\mathbf{D}$	$3\mathbf{M} + 2\mathbf{C}$	$4\mathbf{M} + 4\mathbf{C} + 1\mathbf{D}$

Table 1. Costs of point operations for different coordinate systems of elliptic curves over $\mathbb{F}_{3^m}$

We compared the performance of the proposed formulas to the previously best results for different coordinates systems. It is shown that the new formulas are superior to the previously known ones. It should be pointed out that, in double-base chain representation for a scalar number, the proposed point doubling and tripling may offer better performance.

References

1. R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, and F. Vercauteren. *Handbook of Elliptic and Hyperelliptic Curve Cryptography.* CRC Press, 2005.
2. I. F. Blake, G. Seroussi, and N. P. Smart. *Advances in Elliptic Curve Cryptography.* Cambridge University Press, 2005.
3. Blake, I.F., Seroussi, G., Smart, N.P.: Elliptic Curves in Cryptography, vol. 265. Cambridge University Press, New York, NY, USA (1999)
4. D. J. Bersntein, D. Kohel, and T. Lange. Twisted Hessian curves. http://www.hyperelliptic.org/EFD/g1p/auto-twistedhessian.html.
5. D. V. Chudnovsky and G. V. Chudnovsky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. *Advances in Applied Mathematics*, 7(4):385–434, 1986.
6. Farashahi, R.R., Joye, M.: Efficient Arithmetic on Hessian Curves. In Nguyen, P.Q., Pointcheval, D. (Eds.): PKC 2010, Lecture Notes in Computer Science, vol. 6056, pp. 243–260, Springer-Verlag Berlin/Heidelberg(2010)
7. Cohen, H., Frey, G. (eds.): Handbook of elliptic and hyperelliptic curve cryptography. CRC Press (2005)
8. Fouquet, M., Gaudry, P., R., H.: An extension of satoh's algorithm and its implementation. J. Ramanujan Math. Soc. 15, 281–318 (2000)
9. Hankerson, D., Menezes, A.J., Vanstone, S.: Guide to Elliptic Curve Cryptography. Springer-Verlag, pub-SV:adr (2004)
10. O. Hesse. Über die Elimination der Variabeln aus drei algebraischen Gleichungen vom zweiten Grade mit zwei Variabeln. *Journal für die reine und angewandte Mathematik*, 10:68–96, 1844.
11. Hisil, G., Carter, G., Dawson, E.: New Formulae for Efficient Elliptic Curve Arithmetic. In Pandu Rangan, K.C., Yung, M. (Eds.): INDOCRYPT: International

Conference in Cryptology in India, LNCS 4859, pp. 138–151, Springer-Verlag Berlin/Heidelberg(2007)

12. M. Joye and J.-J. Quisquater. Hessian elliptic curves and side-channel attacks. In Ç. K. Koç, D. Naccache, and C. Paar, editors, *CHES 2001*, volume 2162 of *LNCS*, pages 402–410. Springer, 2001.
13. Kim, K.H., Kim, S.I., Choe, J.S.: New fast algorithms for arithmetic on elliptic curves over fields of characteristic three. Cryptology ePrint Archive, Report 2007/179 (2007)
14. Koblitz, N.: Elliptic curve cryptosystems. Mathematics of Computation 48, 203–209. (1987)
15. Koblitz, N.: An elliptic curve implementation of the finite field digital signature algorithm. In: Krawczyk, H. (ed.) Advances in Cryptology- CRYPTO '98, Lecture Notes in Computer Science, vol. 1462, pp. 327–337. Springer Berlin/Heidelberg (1998)
16. Lǿpez, J., Dahab, R.: Improved algorithms for elliptic curve arithmetic in Gf(2^n). In: Tavares, S., Meijer, H. (eds.) Selected Areas in Cryptography, Lecture Notes in Computer Science, vol. 1556, pp. 632–632. Springer Berlin/Heidelberg (1999)
17. Miller, V.S.: Use of elliptic curves in cryptography. In: In Advances in Cryptology - Crypto'85. pp. 417–426. LNCS 218, Springer-Verlag (1986)
18. Negre: Scalar multiplication on elliptic curves defined over fields of small odd characteristic. In: INDOCRYPT: International Conference in Cryptology in India. LNCS, Springer-Verlag (2005)
19. Satoh, T.: The canonical lift of an ordinary elliptic curve over a finite field and its point counting. J. Ramanujan Math. Soc. 15, 247–270 (2000)
20. N. P. Smart. The Hessian form of an elliptic curve. In Ç. K. Koç, D. Naccache, and C. Paar, editors, *CHES 2001*, volume 2162 of *LNCS*, pages 118–125. Springer, 2001.
21. Smart, N.P., Westwood, E.J.: Point multiplication on ordinary elliptic curves over fields of characteristic three. Appl. Algebra Eng. Commun. Comput 13(6), 485–497 (2003)

A.1 Ordinary Elliptic Curves over Finite Fields of characteristic Three

The following table lists domain parameters for the ordinary elliptic curves over the finite field of characteristic three for high security level. The following parameters are given for each curve:

m	The extension degree of the binary field $\mathbb{F}_{3^m}$.
$f(z)$	The reduction polynomial of degree m.
b	The coefficients of the elliptic curve $E:\ y^2 = x^3 + x^2 + b$.
r	The prime order of the base point P.
h	The cofactor, that is $\#E(\mathbb{F}_{3^m}) = hr$.

Table 2. Parameters for Ordinary Elliptic Curves in Characteristic Three

E-151: $m = 151$, $f(z) = z^{151} + 2z^2 + 1$, $h = 3$ $b =$ 0x1FC4865AFE00A9216B0B5FD32C6300C4BED0707AE4072A03E55299F157B; $r =$ 0x359BA2B98CA11D6864A331B45AE711875640BA8E1297230F9EB217FB8393.
E-181: $m = 181$, $f(z) = z^{181} + 2z^{37} + 1$, $h = 3$ $b =$ 0x173CB756670960FD06D9438C9A55BE469574A995718B1786C9DAD40C45A7AC68C208FC3; $r =$ 0x27367561CDDFD3AAFB8EA1FD4470B1171C349B993B5282BC17E661A1B1DF65BCE845A035.
E-263: $m = 263$, $f(z) = z^{263} + 2z^{69} + 1$, $h = 3$ $b =$ 0x1E47D9F0855EB0ADDCE5948A2A1E5AF24EBFCC3051D647877CFFB91F564568C5103A09F22B234CE422567E0629358A740B8944C; $r =$ 0x994BBF51A32F5E702E4A3FFB7539AC6AAEAAF9B49E4CCA1DE8CE23F979DDA476F721963D0BF18B1216F037A8877236007190FD2F.
E-331: $m = 331$, $f(z) = z^{331} + 2z^2 + 1$, $h = 3$ $b =$ 0x52056E6E1C557FC37DD4D21EFFE1D5CA8E1528695E4B13536CF990AE79C9242B8602535C92522A4EBB87E522ABF5C1CEA952EE52B9F6EA738930402CA3713AA0; $r =$ 0x8361D3334042B3F713BEB5D2C7BFAE83C436C40B479A21A4D1BE815079F3C07FF992C36206C4E5B5DC9C2206CFB7F1AC1BD0F98A64CAB13DB53403AC4007E4875E5.
E-337: $m = 337$, $f(z) = z^{337} + 2z^3 + 1$, $h = 3$ $b =$ 0x359059FA58F98216D63B1FA12F4C194A09FDCFAF27CEEC308FB55B26938D4A1D2E73ED6E9A17CDF7A84D1FAEDB14E38FC212CD76E460C3C5BFF688234724B3EC0921; $r =$ 0x17621926CF1FDF27A973A13C53AD0D7F539BFF4441EE5E9CE59477E3E2B471F2C6735F0933BB1C1B7ECA1A64D72D8F8F9336B4EE7CCA98AE54623C8C15D6EF02AC7395.