Efficient Arithmetic on Elliptic 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 formulae for the point doubling, tripling and addition for ordinary Weierstraß elliptic curves with a point of order 3 and their equivalent Hessian 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 formulae 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 formulae on this case are given in [18, 13]. In [11], Hisil *et al.* gave a new tripling formulae for Hessian curve in characteristic three. The generalized form of Hessian curves has 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 ordinary Weierstraß elliptic curves with a point of order 3 and their birationally equivalent Hessian curves over finite fields of characteristic 3.

The main contribution of this paper is given as follows:

- 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 formulae are faster than the previous known results.
- The new tripling formulae are presented for Hessian curves over finite fields of characteristic 3.
- The doubling and tripling formulae are complete for all input points in the rational group of these curves. Furthermore, the unified addition formulae are valid for all input points in the rational subgroup which is employed in practical cryptographic applications.
- 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 Weierstraßcurves and Hessian curves over the finite fields $\mathbb{F}_{3^m}$. §3 presents new doubling, addition and tripling formulae for Weierstraß elliptic curves over $\mathbb{F}_{3^m}$ with a point of order three. §4 presents the new addition and tripling formulae for Hessian curves. §5 gives the efficiency consideration and timing results and §6 concludes the paper.

2 Preliminaries

2.1 Weierstraß elliptic curves over $\mathbb{F}_{3^m}$

Elliptic curves over any field can be divided into two classes of ordinary and supersingular elliptic curves. Every ordinary elliptic curve over the finite filed $\mathbb{F}_{3^m}$ can be written in the Weierstraß form $y^2 = x^3 + ax^2 + b$, where $a, b \in \mathbb{F}_{3^m}$ and $ab \neq 0$. It is known, [21], that every ordinary elliptic curve over $\mathbb{F}_{3^m}$ with a point of order three can be written in the form

$$\mathbf{E}_b : y^2 = x^3 + x^2 + b$$

where $b \in \mathbb{F}_{3^m}$.

The sum of two (different) points (x_1, y_1), (x_2, y_2) on $\mathbf{E}_b$ is the point (x_3, y_3) given by

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

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

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

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

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

Projective coordinate systems are preferred for point operations to avoid field inversions. There are some different types of projective coordinates which have the respective advantages in efficiency. The relationship between affine coordinates (x, y) and projective coordinates (X, Y, Z) is $(x, y) = (X/Z, Y/Z)$, for Jacobian projective coordinates, $(x, y) = (X/Z^2, Y/Z^3)$, and for López Dahab projective coordinates [16], $(x, y) = (X/Z, Y/Z^2)$.

2.2 Hessian curves over $\mathbb{F}_{3^m}$

A *Hessian curve* over a finite field $\mathbb{F}_{3^m}$ is given by the cubic equation

$$\mathrm{H}_d : \; u^3 + v^3 + 1 = duv\,, \tag{4}$$

for some $d \in \mathbb{F}_{3^m}$ with $d \neq 0$ [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 $\mathbb{F}_{3^m}$ is defined by the equation

$$\mathrm{H}_{c,d} \; : \; u^3 + v^3 + c = duv \;\; ,$$

where $c, d \in \mathbb{F}_{3^m}$ with $c, d \neq 0$. 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 $\mathbb{F}_{3^m}$, via the map $(u, v) \mapsto (\widetilde{u}, \widetilde{v})$ given by $\widetilde{u} = u/\zeta$, $\widetilde{v} = v/\zeta$, with $\zeta = \sqrt[3]{c}$, is isomorphic to the Hessian curve $\mathrm{H}_{\frac{d}{\zeta}} \; : \; \widetilde{u}^3 + \widetilde{v}^3 + 1 = \frac{d}{\zeta}\widetilde{u}\widetilde{v}$. So, the families of Hessian curves and generalized Hessian over $\mathbb{F}_{3^m}$ are the same. For simplicity, from now on we consider the family of Hessian curves over $\mathbb{F}_{3^m}$. 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 $q - 1$.

The sum of two (different) points (u_1, v_1), (u_2, v_2) on H_d is the point (u_3, v_3) given by

$$u_3 = \frac{{v_1}^2 u_2 - {v_2}^2 u_1}{u_2 v_2 - u_1 v_1} \quad \text{and} \quad v_3 = \frac{{u_1}^2 v_2 - {u_2}^2 v_1}{u_2 v_2 - u_1 v_1} \;\; .$$

The doubling of the point (u_1, v_1) on H_d is the point (u_3, v_3) given by

$$u_3 = \frac{v_1(1-{u_1}^3)}{{u_1}^3 - {v_1}^3} \quad \text{and} \quad v_3 = \frac{u_1({v_1}^3 - 1)}{{u_1}^3 - {v_1}^3} \ .$$

Also, the inverse of the point (u_1, v_1) on H_d is the point (v_1, u_1).

The projective closure of the curve H_d is

$$\mathbf{H}_d : \ U^3 + V^3 + W^3 = dUVW \ .$$

The neutral element of the group of $\mathbb{F}$-rational points of $\mathbf{H}_d$ is the point at infinity $(1, -1, 0)$ and the inverse of the point $P = (U_1, V_1, W_1)$ on $\mathbf{H}_d$, is the point $-P = (V_1, U_1, W_1)$.

The sum of the points (U_1, V_1, W_1), (U_2, V_2, W_2) on $\mathbf{H}_d$ is the point (U_3, V_3, W_3) with

$$U_3 = U_2W_2{V_1}^2 - U_1W_1{V_2}^2, \quad V_3 = V_2W_2{U_1}^2 - V_1W_1{U_2}^2, \\ W_3 = U_2V_2{W_1}^2 - U_1V_1{W_2}^2 \ . \quad (5)$$

The doubling of the point (U_1, V_1, W_1) on $\mathbf{H}_d$ is the point (U_3, V_3, W_3) given by

$$U_3 = V_1({W_1}^3 - {U_1}^3), \quad V_3 = U_1({V_1}^3 - {W_1}^3), \quad W_3 = W_1({U_1}^3 - {V_1}^3) \ . \quad (6)$$

We note that the addition formulae (5) is not *unified*, i.e., the formulae do not work to double a point. The following set of formulae are unified which make Hessian curves interesting against side-channel attacks [1, 2].

The sum of the points (U_1, V_1, W_1) and (U_2, V_2, W_2) on $\mathbf{H}_d$ is the point (U_3, V_3, W_3) given by

$$U_3 = V_2W_2{W_1}^2 - U_1V_1{U_2}^2, \quad V_3 = U_2V_2{V_1}^2 - U_1W_1{W_2}^2, \\ W_3 = U_2W_2{U_1}^2 - V_1W_1{V_2}^2 \ . \quad (7)$$

Furthermore, by swapping the order of the points in the addition formulae (7), we obtain the following unified formulae.

$$U_3 = V_1W_1{W_2}^2 - U_2V_2{U_1}^2, \quad V_3 = U_1V_1{V_2}^2 - U_2W_2{W_1}^2, \\ W_3 = U_1W_1{U_2}^2 - V_2W_2{V_1}^2 \ . \quad (8)$$

We recall [6, Propositions 1], which describes the exceptional cases of the addition formulae (5).

Proposition 1. *The addition formulae* (5) *work for all pairs of points* P_1, P_2 *on* $\mathbf{H}_d$ *if and only if* $P_1 - P_2$ *is not the point at infinity.*

Since the curve $\mathbf{H}_d$ over $\mathbb{F}_{3^m}$ has only one $\mathbb{F}_{3^m}$-rational point at infinity, the addition formulae (5) work for all *distinct* pairs of $\mathbb{F}_{3^m}$-rational inputs.

We recall [6, Propositions 2], that explains the exceptional cases of the addition formulae (7).

Proposition 2. *The addition formulae* (7) *work for all pairs of points* P_1, P_2 *on* $\mathbf{H}_d$ *if and only if* $P_1 - P_2 \neq (-1, 0, 1)$.

Similarly, the addition formulae (8) work for all pairs of points P_1, P_2 on $\mathbf{H}_d$ if and only if $P_1 - P_2$ is not a 3-torsion point of $\mathbf{H}_d$ with X-coordinate equals 0. So, the set of formulae (7) and (8) are complement of each other, i.e., if formulae (7) do not work for the pair of inputs P_1, P_2, then the other do work.

As a consequence, the doubling formulae (6) work for all points of the curve $\mathbf{H}_d$. Moreover, for the subgroup $\mathcal{H}$ of $\mathbf{H}_d(\mathbb{F}_{3^m})$ not including the point $(-1, 0, 1)$, the addition formulae (7) (and (8)) work for all pairs of points in $\mathcal{H}$.

2.3 Birational equivalence

We note that every Hessian curve H_d over $\mathbb{F}_{3^m}$ has a point of order 3. Moreover, every elliptic curve over $\mathbb{F}_{3^m}$ with a point of order 3 can be given in generalized Hessian form (see [6]) and so in Hessian form. From §2.1, we recall that an ordinary elliptic curve over $\mathbb{F}_{3^m}$ 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 ordinary elliptic curve $\mathbf{E}_b$ in Weierstraß form $\mathbf{E}_b : y^2 = x^3 + x^2 + b$, with $b \neq 0$ via the map $(x, y) \mapsto (u, v)$ defined by

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

is birationally equivalent to Hessian curve $\mathrm{H}_d : u^3 + v^3 + 1 = duv$, where $d^3 = -1/b$. The inverse map $(u, v) \mapsto (x, y)$ is given by

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

In the projective model, the point (U, V, W) on the projective curve

$$\mathbf{H}_d : U^3 + V^3 + W^3 = dUVW,$$

is mapped to the point $(-(U + V), -(U - V), dW)$ on the projective Weierstraß curve

$$\mathbf{E}_b : ZY^2 = X^3 + X^2Z + bZ^3,$$

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

3 Explicit formulae for ordinary Weierstraß form

In this section, we show how to use a new projective coordinate system to speed up basic point operations on ordinary Weierstraß elliptic curves with a point of order 3 over finite fields of characteristic three.

Here, we consider elliptic curves in Weierstraß form

$$\mathbf{E}_b : Y^2Z = X^3 + X^2Z + bZ^3,$$

where $b \in \mathbb{F}_{3^m}, b \neq 0$. We let $b = -1/a^3$ for some $a \in \mathbb{F}_q$, i.e., $a = (\frac{-1}{b})^{3^{(m-1)}}$. We use the *scaled* projective system, where the point (X, Y, T) is a *scaled* point, if $T = Z/a$ and (X, Y, Z) is a point on $\mathbf{E}_{-1/a^3}$. We note that points $(1/a, \pm 1/a, 1)$ are the points of order three on $\mathbf{E}_{-1/a^3}$. The correspondence between the scaled projective coordinates and the affine coordinates is given as follows

$$(\frac{X}{aT}, \frac{Y}{aT}) \leftrightarrow (X, Y, T).$$

3.1 Point Doubling

Here, using the scaled projective coordinates system, we provide a new formulae for point doubling for the elliptic curve $\mathbf{E}_{-1/a^3}$: $Y^2Z = X^3 + X^2Z - Z^3/a^3$, where $a \in \mathbb{F}_{3^m}$.

Let (X_1, Y_1, T_1) be a scaled point on $\mathbf{E}_{-1/a^3}$, i.e., $T_1 = Z_1/a$ and (X_1, Y_1, Z_1) is a point on $\mathbf{E}_{-1/a^3}$. So, $aY_1^2T_1 = X_1^3 + aX_1^2T_1 - T_1^3$. Let $(X_3, Y_3, T_3) = [2](X_1, Y_1, T_1)$, which is the doubling in the scaled projective coordinates system. From the affine doubling formula (2), we have

$$X_3 = a(X_1^2Y_1 - Y_1^3)T_1 + X_1Y_1^3,\ Y_3 = a(X_1Y_1^2 - X_1^3)T_1 - Y_1^4,\ T_3 = T_1Y_1^3.$$

Then

$$\begin{aligned} X_3 &= X_1Y_1^3 - X_1^3Y_1 + Y_1(X_1^3 + aX_1^2T_1 - aY_1^2T_1), \\ Y_3 &= X_1(aY_1^2T_1 - aX_1^2T_1) - Y_1^4 = X_1(X_1^3 - T_1^3) - Y_1^4. \end{aligned}$$

Therefore, we obtain

$$X_3 = X_1Y_1^3 + Y_1T_1^3 - X_1^3Y_1,\ Y_3 = X_1^4 - Y_1^4 - X_1T_1^3,\ T_3 = T_1Y_1^3. \qquad (9)$$

The following algorithm computes (X_3, Y_3, T_3), i.e., the doubling of the point (X_1, Y_1, T_1).

$$\begin{aligned} &A = X_1 + Y_1,\ B = X_1 - Y_1,\ D = (T_1 - A)^3, \\ &E = (B - T_1)^3,\ F = B \cdot D,\ G = A \cdot E,\ H = T_1 \cdot (D + E), \\ &X_3 = F + G,\ Y_3 = F - G,\ T_3 = H. \end{aligned}$$

The cost of above algorithm is $3\mathbf{M} + 2\mathbf{C}$, where $\mathbf{M}$ is the cost of a field multiplication and $\mathbf{C}$ is the cost of cubing.

The following proposition shows that the doubling formulae is complete.

Proposition 3. *The doubling formulae (9) work for all input points on* $\mathbf{E}_{-1/a^3}$.

Proof. Let $P = (X_1, Y_1, T_1)$ be a scaled point on $\mathbf{E}_{-1/a^3}$ such that the doubling formulae (9) do not work for the input P. Thus, we have

$$X_3 = X_1Y_1^3 + Y_1T_1^3 - X_1^3Y_1 = 0,\ Y_3 = X_1^4 - Y_1^4 - X_1T_1^3 = 0,\ T_3 = T_1Y_1^3 = 0.$$

From $T_3 = 0$, we have $T_1 = 0$ or $Y_1 = 0$. By the curve equation we have $aY_1^2T_1 = X_1^3 + aX_1^2T_1 + T_1^3$. If $T_1 = 0$ then $X_1 = 0$. From $Y_3 = 0$, we obtain $Y_1 = 0$. So $(X_1, Y_1, T_1) = (0, 0, 0)$ which is a contradiction. If $Y_1 = 0$, by $Y_3 = 0$ we have $X_1(X_1 - T_1)^3 = 0$. Then, by the curve equation we obtain $T_1 = 0$, which is a contradiction. □

3.2 Point Addition

Now, we provide the addition formulae for the scaled points on $\mathbf{E}_{-1/a^3} : Y^2Z = X^3 + X^2Z - Z^3/a^3$

Let $P_1 = (X_1, Y_1, T_1)$ and $P_2 = (X_2, Y_2, T_2)$ be two scaled points on $\mathbf{E}_{-1/a^3}$, i.e., $T_1 = Z_1/a$, $T_2 = Z_2/a$ and (X_1, Y_1, Z_1), (X_2, Y_2, Z_2) are points on $\mathbf{E}_{-1/a^3}$. Let (X_3, Y_3, T_3) be the sum of P_1 and P_2, where $T_3 = Z_3/a$ and (X_3, Y_3, Z_3) is a point on $\mathbf{E}_{-1/a^3}$. From the affine addition formulae (1), we have

$$\begin{aligned}
X_3 &= aT_1T_2(X_2T_1 - X_1T_2)((Y_2T_1 - Y_1T_2)^2 - (X_2T_1 - X_1T_2)^2) \\
&\quad -(X_2T_1 - X_1T_2)^3(X_2T_1 + X_1T_2), \\
Y_3 &= -aT_1T_2(Y_2T_1 - Y_1T_2)((Y_2T_1 - Y_1T_2)^2 - (X_2T_1 - X_1T_2)^2) \\
&\quad +(X_2T_1 - X_1T_2)^3(Y_2T_1 + Y_1T_2), \\
T_3 &= T_1T_2(X_2T_1 - X_1T_2)^3.
\end{aligned}$$

Then, we obtain

$$\begin{aligned}
X_3 &= T_2(X_1^2X_2 + X_1Y_1Y_2 + X_2Y_1^2) - T_1(X_1X_2^2 + Y_1X_2Y_2 + X_1Y_2^2), \\
Y_3 &= T_2(X_1^2Y_2 + X_1Y_1X_2 + Y_2Y_1^2) - T_1(Y_1X_2^2 + X_1X_2Y_2 + Y_1Y_2^2), \\
T_3 &= T_1^2(X_2 + Y_2)(X_2 - Y_2) - T_2^2(X_1 + Y_1)(X_1 - Y_1).
\end{aligned} \tag{10}$$

The following addition algorithm performs the addition formulae (10), which requires 12**M**.

$$\begin{aligned}
&A_1 = X_1 + Y_1,\ B_1 = X_1 - Y_1,\ A_2 = X_2 + Y_2,\ B_2 = X_2 - Y_2, \\
&D = T_1 \cdot A_2,\ E = T_1 \cdot B_2,\ F = T_2 \cdot A,\ G = T_2 \cdot B, \\
&H = A_1 \cdot B_2,\ I = A_2 \cdot B_1,\ X_3 = G \cdot I - E \cdot H, \\
&Y_3 = F \cdot H - D \cdot I,\ T_3 = D \cdot E - F \cdot G.
\end{aligned}$$

Notice that $(T_1 - X_1)^3 = aT_1(X_1 + Y_1)(X_1 - Y_1)$. Then, we have

$$\begin{aligned}
&T_1T_2 \cdot (T_1^2(X_2 + Y_2)(X_2 - Y_2) - T_2^2(X_1 + Y_1)(X_1 - Y_1)) \\
&= (1/a)(T_1^3(T_2 - X_2)^3 - T_2^3(T_1 - X_1)^3) = (1/a)(X_1T_2 - X_2T_1)^3.
\end{aligned}$$

Therefore, we obtain

$$\begin{aligned}
X_3 &= T_2T_1^2(X_1X_2^2 + Y_1X_2Y_2 + X_1Y_2^2) - T_1T_2^2(X_1^2X_2 + X_1Y_1Y_2 + X_2Y_1^2), \\
Y_3 &= T_2T_1^2(Y_1X_2^2 + X_1X_2Y_2 + Y_1Y_2^2) - T_1T_2^2(X_1^2Y_2 + X_1Y_1X_2 + Y_2Y_1^2), \\
T_3 &= (1/a)(X_2T_1 - X_1T_2)^3.
\end{aligned} \tag{11}$$

We write

$$\begin{aligned}
X_3 = T_1(X_2 + Y_2)T_2^2(X_1 - Y_1)^2 + T_1(X_2 - Y_2)T_2^2(X_1 + Y_1)^2 \\
-T_2(X_1 + Y_1)T_1^2(X_2 - Y_2)^2 - T_2(X_1 - Y_1)T_1^2(X_2 + Y_2)^2
\end{aligned}$$

and

$$\begin{aligned} Y_3 = {} & T_1(X_2+Y_2)T_2^2(X_1-Y_1)^2 - T_1(X_2-Y_2)T_2^2(X_1+Y_1)^2 \\ & -T_2(X_1+Y_1)T_1^2(X_2-Y_2)^2 + T_2(X_1-Y_1)T_1^2(X_2+Y_2)^2. \end{aligned}$$

Therefore, we have the following addition algorithm which requires $10\mathbf{M}+1\mathbf{C}+1\mathbf{D}$, where $\mathbf{D}$ is the cost of a field multiplication by the constant $1/a$.

$$\begin{aligned} & A_1 = X_1+Y_1,\ B_1 = X_1-Y_1,\ A_2 = X_2+Y_2,\ B_2 = X_2-Y_2, \\ & D = B_1\cdot T_2,\ E = A_2\cdot Z_1,\ F = A_1\cdot T_2,\ G = B_2\cdot T_1,\ H = D\cdot E \\ & I = F\cdot G,\ J = F\cdot I,\ K = E\cdot H,\ X_3 = D\cdot H + J - G\cdot I - K, \\ & Y_3 = X_3 + FI + EH,\ Z_3 = (1/a)(D+F-E-G)^3. \end{aligned}$$

The cost of mixed scaled addition formulae is $8\mathbf{M}+1\mathbf{C}+1\mathbf{D}$, by setting $T_1 = 1$.

3.3 Unified Addition Formulae

Here, we study the *unified* addition formulae. In general, the *unified* addition formulae work for all but finitely many pairs of points. The *complete* addition formulae emphasize to work for all inputs. We recall that the affine addition formulae (1) and projective formulae (11) do not work to double a point. More precisely, the addition formula (11) do not work for the points P_1 and P_2 if and only if $P_1 - P_2 = (0,1,0)$.

Hereafter, we give some *unified* addition formulae for $\mathbf{E}_{-1/a^3} :\ Y^2Z = X^3 + X^2Z - Z^3/a^3$. The unified addition formulae make the curve $\mathbf{E}_{-1/a^3}$ interesting against side-channel attacks.

Let $P_1 = (X_1, Y_1, T_1)$ and $P_2 = (X_2, Y_2, T_2)$ be two scaled points on $\mathbf{E}_{-1/a^3}$, where $T_1 = Z_1/a, T_2 = Z_2/a$ and (X_1, Y_1, Z_1), (X_2, Y_2, Z_2) are points on $\mathbf{E}_{-1/a^3}$. Then, $Q_1 = (X_1+Y_1, X_1-Y_1, T_1)$ and $Q_2 = (X_2+Y_2, X_2-Y_2, T_2)$ are points of H_d. From the unified formulae (7) we obtain the point (U_3, V_3, W_3) on H_d, where

$$\begin{aligned} U_3 &= T_1^2T_2(X_2-Y_2) - (X_1+Y_1)(X_1-Y_1)(X_2+Y_2)^2, \\ V_3 &= -T_1T_2^2(X_1+Y_1) + (X_2+Y_2)(X_2-Y_2)(X_1-Y_1)^2, \\ W_3 &= T_2(X_1+Y_1)^2(X_2+Y_2) - T_1(X_1-Y_1)(X_2-Y_2)^2. \end{aligned}$$

Then, the point $(X_3, Y_3, T_3) = ((U_3+V_3), (U_3-V_3), -W_3)$ is a scaled point of $\mathbf{E}_{-1/a^3}$, which is the sum of P_1 and P_2. We obtain

$$\begin{aligned} X_3 &= T_1T_2(T_1(X_2-Y_2) - T_2(X_1+Y_1)) + (X_1-Y_1)(X_2+Y_2)(X_1Y_2+X_2Y_1), \\ Y_3 &= T_1T_2(T_1(X_2-Y_2) + T_2(X_1+Y_1)) + (X_1-Y_1)(X_2+Y_2)(X_1X_2+Y_1Y_2), \\ T_3 &= T_1(X_1-Y_1)(X_2-Y_2)^2 - T_2(X_1+Y_1)^2(X_2+Y_2). \end{aligned} \tag{12}$$

We note that by swapping the order of the points P_1 and P_2 we obtain another unified formulae as follows.

$$\begin{aligned} X_3 &= T_1T_2(T_2(X_1-Y_1) - T_1(X_2+Y_2)) + (X_1+Y_1)(X_2-Y_2)(X_1Y_2+X_2Y_1), \\ Y_3 &= T_1T_2(T_2(X_1-Y_1) + T_1(X_2+Y_2)) + (X_1+Y_1)(X_2-Y_2)(X_1X_2+Y_1Y_2), \\ T_3 &= T_2(X_1-Y_1)^2(X_2-Y_2) - T_1(X_1+Y_1)(X_2+Y_2)^2. \end{aligned} \tag{13}$$

Moreover, the algorithm which performs above addition formulae (12) (or (13)) requires $12\mathbf{M}$.

We recall that the set of formulae (7) and (8) are complement of each other, so the same property is true for the set of formulae (12) and (13). From Proposition 2, we see that the addition formulae (12) do not work for the inputs P_1, P_2 if and only if $P_1 - P_2 = (1, 1, 1)$.

Then, one can easily see that the doubling formulae (6) work for all points of the curve $\mathbf{H}_d$. Moreover, for the subgroup $\mathcal{G}$ of $\mathbf{E}_{-1/a^3}(\mathbb{F}_{3^m})$ not including the point $(1, 1, a)$, the addition formulae (12) (and (13)) work for all pairs of points in $\mathcal{G}$.

3.4 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 formulae (3), the tripling of the scaled point (X_1, Y_1, T_1) on $\mathbf{E}_{-1/a^3}$ is the point (X_3, Y_3, T_3) given by

$$\begin{aligned} X_3 &= (X_1^3 - T_1^3)(X_1^9 - T_1^9 + a^3 X_1^3 T_1^6), \\ Y_3 &= a^3 Y_1^3 T_1^3 (Y_1^2 - X_1^2 - T_1^2 - X_1 T_1)^3, \\ T_3 &= a^2 (X_1^9 T_1^3 - T_1^{12}). \end{aligned} \tag{14}$$

Then, we have

$$\begin{aligned} X_3 &= (X_1 - T_1)^3 (a^3 Y_1^6 T_1^3 - a^3 X_1^6 T_1^3 + a^3 X_1^3 T_1^6) \\ &= -a^3 T_1^3 \cdot (X_1 - T_1)^3 (X_1^6 - Y_1^6 - X_1^3 T_1^3) \\ &= -a^3 T_1^3 \cdot (X_1 - T_1)^3 (X_1^2 - Y_1^2 - X_1 T_1)^3, \\ Y_3 &= -a^3 T_1^3 \cdot Y_1^3 (X_1^2 + X_1 T_1 + T_1^2 - Y_1^2)^3, \\ T_3 &= -a^3 T_1^3 \cdot (T_1^9 - X_1^9)/a. \end{aligned}$$

So, we obtain

$$\begin{aligned} X_3 &= (X_1 - T_1)^3 (X_1^2 - Y_1^2 - X_1 T_1)^3, \\ Y_3 &= Y_1^3 (X_1^2 + X_1 T_1 + T_1^2 - Y_1^2)^3, \\ T_3 &= (T_1^9 - X_1^9)/a. \end{aligned} \tag{15}$$

We also write

$$\begin{aligned} X_1^2 + X_1 T_1 + T_1^2 - Y_1^2 &= (X_1 - T_1 + Y_1)(X_1 - T_1 - Y_1), \\ X_1^2 - Y_1^2 - X_1 T_1 &= (X_1^2 + X_1 T_1 + T_1^2 - Y_1^2) + X_1 T_1 - T_1^2 \ . \end{aligned}$$

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

$$\begin{gathered} A = X_1 - T_1,\ B = (A + Y_1)(A - Y_1),\ D = A(B + T_1 A), \\ X_3 = D^3,\ Y_3 = (Y_1 B)^3,\ T_3 = -(1/a) A^9 \ . \end{gathered}$$

We see that the cost for above point tripling algorithm is $4\mathbf{M} + 4\mathbf{C} + 1\mathbf{D}$. The following proposition shows that tripling formulae work for all inputs.

Proposition 4. *The tripling formulae* (15) *work for all points on* $\mathbf{E}_{-1/a^3}$.

Proof. Let $P = (X_1, Y_1, T_1)$ be a scaled point on $\mathbf{E}_{-1/a^3}$: $Y^2Z = X^3 + X^2Z - Z^3/a^3$ such that the tripling formulae (15) do not work for the point P. Thus, the formulae (15) output

$$X_3 = 0,\ Y_3 = 0,\ T_3 = (T_1^9 - X_1^9)/a = 0.$$

From $T_3 = 0$, we have $X_1 = T_1$. Then, $Y_3 = Y_1^3(X_1^2 + X_1T_1 + T_1^2 - Y_1^2)^3 = -Y_1^5$. Since $Y_3 = 0$, we have $Y_1 = 0$ and then $(X_1, Y_1, T_1) = (0, 0, 0)$ which is a contradiction. □

4 Explicit Formulae for Hessian curves in Characteristic 3

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

4.1 Addition and doubling formulae

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

Furthermore, from the addition formulae (5), 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

$$X_3 = Z_1Z_2(X_2Z_2{Y_1}^2 - X_1Z_1{Y_2}^2), \quad Y_3 = Z_1Z_2(Y_2Z_2{X_1}^2 - Y_1Z_1{X_2}^2),$$

$$\begin{aligned} Z_3 &= Z_1Z_2(X_2Y_2{Z_1}^2 - X_1Y_1{Z_2}^2) = Z_1^3(X_2Y_2Z_2) - Z_2^3(X_1Y_1Z_1) \\ &= Z_1^3(X_2^3 + Y_2^3 + Z_2^3)/d - Z_2^3(X_1^3 + Y_1^3 + Z_1^3)/d \\ &= (X_2Z_1 + Y_2Z_1 - X_1Z_2 - Y_1Z_2)^3/d. \end{aligned}$$

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

$$\begin{gathered} A = X_2Z_1,\ B = Y_2Z_1,\ C = X_1Z_2,\ D = Y_1Z_2,\ E = AD,\ F = BC, \\ X_3 = DE - BF, \quad Y_3 = CF - AE, \quad Z_3 = (1/d)(A + B - C - D)^3 \ . \end{gathered} \tag{16}$$

Also, the mixed addition formulae requires $8\mathbf{M} + 1\mathbf{C} + 1\mathbf{D}$. We note that the addition algorithm (16) is not unified. In [13], Kim *et al.* first propose a mixed addition algorithm requires $8\mathbf{M} + 1\mathbf{C} + 1\mathbf{D}$.

The next algorithm evaluates the unified addition formulae (7) for the Hessian curve H_d with 12**M**.

$$\begin{gathered} A = X_1X_2,\ B = Y_1Y_2,\ C = Z_1Z_2,\ D = X_1Z_2,\ E = Y_1X_2,\ F = Z_1Y_2, \\ X_3 = CF - AE, \quad Y_3 = BE - CD, \quad Z_3 = AD - BF \ . \end{gathered}$$

The mixed addition formulae requires $10\mathbf{M}$ by setting $Z_2 = 1$. Furthermore, the addition formulae (7) can be performed in a parallel way. The following addition algorithm is similar to the addition algorithm (16) which requires $10\mathbf{M}+1\mathbf{C}+1\mathbf{D}$.

$$A = Z_2X_1,\ B = X_2X_1,\ C = Y_1Y_2,\ D = Z_1Y_2,\ E = AD,\ F = BC,$$
$$X_3 = DE - BF, \quad Y_3 = CF - AE, \quad Z_3 = (1/d)(A + B - C - D)^3\ .$$

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

From the doubling formulae (6), 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

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

which requires $3\mathbf{M} + 2\mathbf{C}$([13]).

4.2 Point Tripling

From §2.3, we recall that the scaled point (X, Y, T) on $\mathbf{E}_b$ is corresponded to the point $(X + Y, X - Y, T)$ on the Hessian curve $\mathbf{H}_d$. Furthermore, the point (U, V, W) on $\mathbf{H}_d$ is corresponded to the scaled point $((U + V), (U - V), -T)$ on $\mathbf{E}_b$. The point tripling (15) for Weierstraß form $\mathbf{E}_b$ can be used to obtain the following point tripling algorithm for the Hessian curve $\mathbf{H}_d$. The tripling of the points (U_1, V_1, W_1) on $\mathbf{H}_d$ with $d^3 = -1/b$ is the scaled point (U_3, V_3, W_3) given by the next formulae.

$$\begin{aligned} U_3 &= (U_1W_1^2 + V_1U_1^2 + W_1V_1^2)^3, \\ V_3 &= (U_1V_1^2 + V_1W_1^2 + W_1U_1^2)^3, \\ W_3 &= -(1/a)(U_1 + V_1 + W_1)^9. \end{aligned} \tag{17}$$

Then, we propose the following point tripling algorithm.

$$A = U_1 + V_1 + W_1,\ B = (U_1 - W_1)(V_1 - W_1),\ D = A(B - AZ_1),\ E = V_1B$$
$$U_3 = (D + E)^3,\ V_3 = (D - E)^3,\ W_3 = -(1/a)A^9\ .$$

The cost for above point tripling algorithm is $4\mathbf{M} + 4\mathbf{C} + 1\mathbf{D}$. Moreover, from Proposition 4 we see that the tripling formulae work for all inputs.

5 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 formulae 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 formulae 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, where $\mathbf{S}$ denote the cost of a squaring in the finite field of characteristic three. 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 formulae are always more efficient than all previous formulae published for basic point operations on curves.

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

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 [13]	$9\mathbf{M}+1\mathbf{C}$	$3\mathbf{M}+2\mathbf{C}$	−
Hessian form(this work)	$8\mathbf{M}+1\mathbf{C}+1\mathbf{D}$	$3\mathbf{M}+2\mathbf{C}$	$4\mathbf{M}+4\mathbf{C}+1\mathbf{D}$
scaled projective(this work)	$8\mathbf{M}+1\mathbf{C}+1\mathbf{D}$	$3\mathbf{M}+2\mathbf{C}$	$4\mathbf{M}+4\mathbf{C}+1\mathbf{D}$

6 Conclusion

In this paper, a new basic operation formulae 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.

We compared the performance of the proposed formulae to the previously best results for different coordinates systems. It is shown that the new formulae 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. I. F. Blake, G. Seroussi, N.P. Smart. *Elliptic Curves in Cryptography, vol. 265.* Cambridge University Press, New York, 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. H. Cohen, G. Frey, (eds.). *Handbook of elliptic and hyperelliptic curve cryptography.* CRC Press, 2005.
8. M. Fouquet, P. Gaudry, R. Harley. An Extension of Satoh's Algorithm and its Implementation. J. Ramanujan Math. Soc. 15, pp. 281–318, 2000.
9. D. Hankerson, A.J. Menezes, S. Vanstone. *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. G. Hisil, G. Carter, E. Dawson. 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*, pp. 402–410. Springer, 2001.
13. K.H. Kim, S.I. Kim, J.S. Choe. New Fast Algorithms for Arithmetic on Elliptic Curves over Fields of Characteristic Three. Cryptology ePrint Archive, Report 2007/179, 2007.
14. N. Koblitz. Elliptic curve cryptosystems. Mathematics of Computation 48, pp. 203–209, 1987.
15. N. Koblitz. An elliptic curve implementation of the finite field digital signature algorithm. In: Krawczyk, H. (ed.) Advances in Cryptology- CRYPTO '98, volume 1462 of *LNCS*, pp. 327–337. Springer Berlin/Heidelberg, 1998.
16. J. Ĺopez, R. Dahab. Improved Algorithms for Elliptic Curve Arithmetic in Gf(2^n). In: Tavares, S., Meijer, H. (eds.) Selected Areas in Cryptography. volume 1556 of *LNCS*, pp. 632–632. Springer Berlin/Heidelberg, 1999.
17. V.S. Miller. Use of Elliptic Curves in Cryptography. In: In Advances in Cryptology - Crypto'85. volume 218 of *LNCS*, pp. 417–426, Springer-Verlag, 1986.
18. C. Nègre. Scalar multiplication on elliptic curves defined over fields of small odd characteristic. In: INDOCRYPT: International Conference in Cryptology in India. volume 3797 of *LNCS*, pp. 389–402, Springer-Verlag, 2005.
19. T. Satoh. 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*, pp. 118–125. Springer, 2001.
21. N.P. Smart, E.J. Westwood. Point Multiplication on Ordinary Elliptic Curves over Fields of Characteristic Three. Appl. Algebra Eng. Commun. Comput 13(6), pp. 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 ternary 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.