Faster Scalar Multiplication on Ordinary Weierstrass Elliptic Curves over Fields of Characteristic Three

Hongfeng Wu[1], Chang-An Zhao[2]

[1] College of Sciences, North China University of Technology,
Beijing 100144, P.R.China
[2] School of Computer Science and Educational Software, Guangzhou University,
Guangzhou 510006, P.R.China
whfmath@gmail.com
changanzhao@gzhu.edu.cn

Abstract. This paper proposes new explicit formulae for the point doubling, tripling and addition on ordinary Weierstrass elliptic curves with a point of order 3 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 $3M + 2C$, $8M + 1C + 1D$ and $4M + 4C + 1D$ respectively, where M, C and D is the cost of a field multiplication, a cubing and a multiplication by a constant. We also provide the unified and complete group laws. Finally, we present several examples of ordinary elliptic curves in characteristic three for high security levels.

Keywords: Elliptic curve, scalar multiplication, unified addition, cryptography, explicit formulae

1 Introduction

Elliptic curve cryptosystems which was discovered by Neal Koblitz [9] and Victor Miller [12] 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 [2, 6, 4] for the two cases. However, elliptic curves in characteristic three could be preferred in certain cryptographic schemes. For example, the η_T pairing on supersingular curves in characteristic three may offer the best possible performance for software and hardware implementations [1]. Moreover, Koblitz implemented the Elliptic Curve Digital Signature Algorithm (ECDSA) on a special family of supersingular elliptic curves in characteristic three with great efficiency [10]. Compared to elliptic curves on large prime fields or binary fields, Smart *et al.* pointed out that ordinary elliptic curve in characteristic three can be an alternative for implementing elliptic curve cryptosystems [15]. Further improved formulae are given in [13, 7].

The goal of the present work is to speed up scalar multiplication on ordinary elliptic curves with a point of order 3 in characteristic three. We explore the elliptic curve of the form $E_a/\mathbb{F}_{3^m} : y^2 = x^3 + x^2 - 1/a^3$ which is $\mathbb{F}_{3^m}$-isomorphic to the curve investigated by Smart *et al.* in [15]. The main contribution of this paper is given as follows:

- A modified projective coordinate system is presented. It is named as $\mathcal{A}$-projective coordinate system since it is related with the key parameter a. This offers better performance than the other projective coordinate system.
- The basic point operations of addition, doubling, and tripling are investigated in the new coordinate system. The proposed formulae are faster than the previous known results.
- The unified addition formulae are devised for resisting the side channel analysis. Furthermore, the complete group law of point operations is shown.
- Examples of ordinary elliptic curves over characteristic three are provided for high security levels.

The rest of this paper is organized as follows. Section 2 introduces the basic point operations on ordinary elliptic curves in characteristic three. Section 3 presents the new formulae for scalar multiplication. In section 4, the unified and complete formulae are proposed on ordinary elliptic curves in characteristic three. Section 5 gives the efficiency consideration and timing results. We draw our conclusion in Section 6.

2 Preliminaries

The focus of this paper will be with elliptic curves defined over fields $\mathbb{F}_{3^m}$. For the finite field $\mathbb{F}_{3^m}$, the elliptic curves can be divided into two kinds: ordinary elliptic curves and supersingular elliptic curves. Every ordinary elliptic curves can be written in the Weierstrass form

$$E : y^2 = x^3 + ax^2 + b$$

where $a, b \in \mathbb{F}_{3^m}$ and $ab \neq 0$.

The addition formulas for affine coordinates on E are given as follows. Let $P = (x_1, y_1)$, $Q = (x_2, y_2)$ and $P+Q = (x_3, y_3)$ be points on $E(\mathbb{F}_{3^m})$. If $P \neq \pm Q$ then

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1},\ x_3 = \lambda^2 - x_1 - x_2 - a,\ y_3 = \lambda(x_1 - x_3) - y_1, \tag{1}$$

If $P = Q$ then

$$\lambda = \frac{ax_1}{y_1},\ x_3 = \lambda^2 + x_1 - a,\ y_3 = \lambda(x_1 - x_3) - y_1, \tag{2}$$

Let $P = (x_1, y_1)$ and $3P = (x_3, y_3)$, then

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

For efficiency, field inversions in group operations should be avoided, and point operations can be preferred in projective coordinate systems. There are some different types of projective coordinates which have the respective advantages in efficiency. The relationship between (x, y) and (X, Y, Z) in different coordinate systems are listed as follows.

- Ordinary projective coordinates: $(x, y) = (X/Z, Y/Z)$,
- Jacobian projective coordinates: $(x, y) = (X/Z^2, Y/Z^3)$,
- López Dahab projective coordinates [11]: $(x, y) = (X/Z, Y/Z^2)$,
- ML-projective coordinates (X, Y, Z, T) [7]: $(x, y) = (X/T, Y/Z^3),\ T = Z^2$.

In the next section, we will explore a new modified projective coordinate systems which offers competitive performance in basic point operations.

3 Fast Arithmetic on Ordinary Weierstrass Elliptic Curves in Characteristic Three

In this section, we show how to use a variant of Weierstrass elliptic curves over finite fields of characteristic three to speed up basic point operations.

3.1 A New Variant of Ordinary Weierstrass Elliptic Curves in Characteristic Three

Without loss of too much generality, we will mainly consider the ordinary elliptic curve in characteristic three which has a point of order three. The following lemma can be found in [15].

Lemma 1 *([15]) An ordinary elliptic curve over a field of characteristic 3 has a point of order three if and only if it can be written in the form* $y^2 = x^3 + x^2 + c$.

The following lemma shows that the number of $\mathbb{F}_{3^m}$-isomorphism classes of the Weierstrass curves like the form $y^2 = x^3 + x^2 + c$ equals $3^m - 1$.

Lemma 2 *Let* $E_1 : y^2 = x^3 + x^2 + a$ *defined over* $\mathbb{F}_{3^m}$*. Then* E_1 *is* $\mathbb{F}_{3^m}$*-isomorphic to* $E_2 : y^2 = x^3 + x^2 + b$ *if and only if* $a = b$.

Proof. Assume that E_1 is $\mathbb{F}_q$-isomorphic to E_2. Then there exists an admissible change of variables $(x, y) \to (u^2x, u^3y)$ with $u \in \mathbb{F}_{3^m}$ and $u \neq 0$ which transforms E_1 into E_2. Hence $u^2 = 1$ and $a = u^6b = b$. □

Note that for any curve $y^2 = x^3 + x^2 + c$ over $\mathbb{F}_{3^m}$ with $c \neq 0$, take $a = (\frac{-1}{c})^{3^{(m-1)}}$, then $-\frac{1}{a^3} = c^{3^m} = c$. With loss of generality, from now on we will only consider Weierstrass equations of the form

$$E_a : y^2 = x^3 + x^2 - 1/a^3$$

with $a \in \mathbb{F}_{3^m}$ and $a \neq 0$. Note that $(1/a, \pm 1/a)$ are points of order three on E_a.

3.2 Point Doubling

Here we define a new projective coordinate system, which we call $\mathcal{A}$-projective coordinate systems. The relationship between the projective coordinates and the affine coordinates is given as follows

$$(X/aZ, Y/aZ) \leftrightarrow (X, Y, aZ).$$

Note that the projective equation of E_a is $Y^2Z = X^3 + X^2Z - Z^3/a^3$. If $P = (X_1, Y_1, aZ_1)$ is a point on E_a in $\mathcal{A}$-projective coordinates, then $aY_1^2Z_1 = X_1^3 + aX_1^2Z_1 - Z_1^3$.

Now we first consider the operation of point doubling in the modified coordinate system. The following theorem will provide a new formulae for point doubling.

Theorem 3 *Let $P = (X_1, Y_1, aZ_1)$ be a point on $E_a : Y^2Z = X^3 + X^2Z - Z^3/a^3$. The doubling formulae on E_a are given by $[2](X_1, Y_1, aZ_1) = (X_3, Y_3, aZ_3)$ where*

$$\begin{aligned} X_3 &= X_1Y_1^3 + Y_1Z_1^3 - X_1^3Y_1, \\ Y_3 &= X_1^4 - Y_1^4 - X_1Z_1^3, \\ Z_3 &= Z_1Y_1^3. \end{aligned} \tag{4}$$

Proof. Note that $aY_1^2Z_1 = X_1^3 + aX_1^2Z_1 - Z_1^3$, from the affine doubling formula (2) in Section 2, we can get that

$$\begin{aligned} X_3 &= a(X_1^2Y_1 - Y_1^3)Z_1 + X_1Y_1^3, \\ Y_3 &= a(X_1Y_1^2 - X_1^3)Z_1 - Y_1^4, \\ Z_3 &= Z_1Y_1^3. \end{aligned} \tag{5}$$

It will be sufficient to show that projective point representation (4) and (5) give the same affine point. From (4), obviously

$$\begin{aligned} X_3 &= X_1Y_1^3 - X_1^3Y_1 + Y_1(X_1^3 + aX_1^2Z_1 - aY_1^2Z_1) = aX_1^2Y_1Z_1 - aY_1^3Z_1 + X_1Y_1^3, \\ Y_3 &= X_1(X_1^3 - Z_1^3) - Y_1^4 = X_1(aY_1^2Z_1 - aX_1^2Z_1) - Y_1^4 = a(X_1Y_1^2 - X_1^3)Z_1 - Y_1^4, \\ Z_3 &= Z_1Y_1^3. \end{aligned}$$

This means that (4) and (5) gives the same affine point. □

On the basis of Theorem 3, we obtain the following explicit formulae for point doubling.

Doubling in $\mathcal{A}$-projective coordinates $2(X_1, Y_1, aZ_1) = (X_3, Y_3, aZ_3)$

$$\begin{aligned} &A = X_1 + Y_1,\ B = X_1 - Y_1,\ D = (Z_1 - A)^3, \\ &E = (B - Z_1)^3,\ F = B \cdot D,\ G = A \cdot E,\ H = Z_1 \cdot (D + E), \\ &X_3 = F + G,\ Y_3 = F - G,\ Z_3 = H. \end{aligned}$$

Let M, S, C, and D denote the cost of a multiplication, a squaring, a cubing and a multiplication by a constant in the finite field of characteristic three, respectively. Then it is not hard to see that the above algorithm costs $3M+2C$. We note that in the case of ternary finite field, a field addition and subtraction can be negligible compared with a field multiplication, squaring or a cubing. Furthermore, a cubing operation in the finite field with characteristic three is faster than a multiplication and a squaring.

3.3 Point Tripling

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

Theorem 4 *Let $P=(X_1,Y_1,aZ_1)$ be a point on $E_a: Y^2Z=X^3+X^2Z-Z^3/a^3$. The tripling formulae on E_a are given by $[3](X_1,Y_1,aZ_1)=(X_3,Y_3,aZ_3)$ where*

$$\begin{aligned} X_3 &= (X_1-Z_1)^3(X_1^2-Y_1^2-X_1Z_1)^3, \\ Y_3 &= Y_1^3(X_1^2+X_1Z_1+Z_1^2-Y_1^2)^3, \\ Z_3 &= (Z_1^9-X_1^9)/a. \end{aligned} \tag{6}$$

Proof. Note that $aY_1^2Z_1=X_1^3+aX_1^2Z_1-Z_1^3$, from the affine tripling formula (3) in Section 2, we can get that

$$\begin{aligned} X_3 &= (X_1^3-Z_1^3)(X_1^9-Z_1^9+a^3X_1^3Z_1^6), \\ Y_3 &= a^3Y_1^3Z_1^3(Y_1^2-X_1^2-Z_1^2-X_1Z_1)^3, \\ Z_3 &= a^2(X_1^9Z_1^3-Z_1^{12}). \end{aligned} \tag{7}$$

It will be sufficient to show that projective point representation (6) and (7) give the same affine point. From (7), obviously

$$\begin{aligned} X_3 &= (X_1^3-Z_1^3)(X_1^9-Z_1^9+a^3X_1^3Z_1^6) \\ &= (X_1-Z_1)^3(a^3Y_1^6Z_1^3-a^3X_1^6Z_1^3+a^3X_1^3Z_1^6) \\ &= -a^3Z_1^3\cdot(X_1-Z_1)^3(X_1^6-Y_1^6-X_1^3Z_1^3) \\ &= -a^3Z_1^3\cdot(X_1-Z_1)^3(X_1^2-Y_1^2-X_1Z_1)^3, \\ Y_3 &= -a^3Z_1^3\cdot Y_1^3(X_1^2+X_1Z_1+Z_1^2-Y_1^2)^3, \\ Z_3 &= -a^3Z_1^3\cdot(Z_1^9-X_1^9)/a. \end{aligned}$$

It means that in (6) and (7) are different only by a common factor, giving the same affine point. □

Note that

$$X_1^2+X_1Z_1+Z_1^2-Y_1^2=X_1^2-2X_1Z_1+Z_1^2-Y_1^2=(X_1-Z_1+Y_1)(X_1-Z_1-Y_1)$$

and

$$X_1^2-Y_1^2-X_1Z_1=(X_1^2+X_1Z_1+Z_1^2-Y_1^2)+X_1Z_1-Z_1^2.$$

Based on Theorem 4, we have the following point tripling formulae.

Tripling in $\mathcal{A}$-projective coordinates $3(X_1,Y_1,aZ_1)=(X_3,Y_3,aZ_3)$.

$$\begin{aligned} A=X_1-Z_1;\ B=(A+Y_1)\cdot(A-Y_1),\\ D=A\cdot(B+Z_1\cdot A),\ E=(1/a)A^9,\\ X_3=D^3,\ Y_3=(Y_1\cdot B)^3,\ Z_3=-E. \end{aligned}$$

We can see that the cost for point tripling is $4M+4C+1D$.

3.4 Point Addition

In this subsection, we consider how to add two points in the $\mathcal{A}$-projective coordinate systems. By the affine point addition formula (1), we can devise the point addition formula in $\mathcal{A}$-projective coordinates.

Let $P=(X_1,Y_1,aZ_1)$ and $Q=(X_2,Y_2,aZ_2)$ be two points on $Y^2Z=X^3+X^2Z-Z^3/a^3$. The addition formulae are given by $P+Q=(X_3,Y_3,aZ_3)$ where

$$\begin{aligned} X_3&=aZ_1Z_2(X_2Z_1-X_1Z_2)((Y_2Z_1-Y_1Z_2)^2-(X_2Z_1-X_1Z_2)^2)\\ &\quad-(X_2Z_1-X_1Z_2)^3(X_2Z_1+X_1Z_2),\\ Y_3&=-aZ_1Z_2(Y_2Z_1-Y_1Z_2)((Y_2Z_1-Y_1Z_2)^2-(X_2Z_1-X_1Z_2)^2)\\ &\quad+(X_2Z_1-X_1Z_2)^3(Y_2Z_1+Y_1Z_2),\\ Z_3&=Z_1Z_2(X_2Z_1-X_1Z_2)^3. \end{aligned} \tag{8}$$

The above addition formulae costs $12M+1C+1D$. Using a long and directly calculation, we can get the following point addition formulae in $\mathcal{A}$-projective coordinates which do not depend on the curve constant a.

$$\begin{aligned} X_3&=Z_2(X_1^2X_2+X_1Y_1Y_2+X_2Y_1^2)-Z_1(X_1X_2^2+Y_1X_2Y_2+X_1Y_2^2),\\ Y_3&=Z_2(X_1^2Y_2+X_1Y_1X_2+Y_2Y_1^2)-Z_1(Y_1X_2^2+X_1X_2Y_2+Y_1Y_2^2),\\ Z_3&=Z_1^2(X_2+Y_2)(X_2-Y_2)-Z_2^2(X_1+Y_1)(X_1-Y_1). \end{aligned} \tag{9}$$

Note that

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

Therefore, we have the following algorithm.

$$\begin{aligned}&A_1=X_1+Y_1,\ B_1=X_1-Y_1,\ A_2=X_2+Y_2,\ B_2=X_2-Y_2,\\&D=Z_1\cdot A_2,\ E=Z_1\cdot B_2,\ F=Z_2\cdot A,\ G=Z_2\cdot B,\\&H=A_1\cdot B_2,\ I=A_2\cdot B_1,\ X_3=G\cdot I-E\cdot H,\\&Y_3=F\cdot H-D\cdot I,\ Z_3=D\cdot E-F\cdot G.\end{aligned}$$

The algorithm cost $12M$. Since

$$(Z_1-X_1)^3=aZ_1(X_1+Y_1)(X_1-Y_1),$$

Thus

$$\begin{aligned}&Z_1Z_2\cdot(Z_1^2(X_2+Y_2)(X_2-Y_2)-Z_2^2(X_1+Y_1)(X_1-Y_1))\\&=(1/a)(Z_1^3(Z_2-X_2)^3-Z_2^3(Z_1-X_1)^3)=(1/a)(X_1Z_2-X_2Z_1)^3.\end{aligned}$$

Therefore, we can modify the point addition formula $(X_1,Y_1,aZ_1)+(X_2,Y_2,aZ_2)=(X_3,Y_3,aZ_3)$ to the following formula.

Theorem 5 *Let $P=(X_1,Y_1,aZ_1)$ and $Q=(X_2,Y_2,aZ_2)$ be two points on $Y^2Z=X^3+X^2Z-Z^3/a^3$. The addition formulae are given by $P+Q=(X_3,Y_3,aZ_3)$, then*

$$\begin{aligned}X_3&=Z_2Z_1^2(X_1X_2^2+Y_1X_2Y_2+X_1Y_2^2)-Z_1Z_2^2(X_1^2X_2+X_1Y_1Y_2+X_2Y_1^2),\\Y_3&=Z_2Z_1^2(Y_1X_2^2+X_1X_2Y_2+Y_1Y_2^2)-Z_1Z_2^2(X_1^2Y_2+X_1Y_1X_2+Y_2Y_1^2),\\Z_3&=(1/a)(X_2Z_1-X_1Z_2)^3.\end{aligned}\tag{10}$$

Note that

$$\begin{aligned}X_3=&Z_1(X_2+Y_2)Z_2^2(X_1-Y_1)^2+Z_1(X_2-Y_2)Z_2^2(X_1+Y_1)^2\\&-Z_2(X_1+Y_1)Z_1^2(X_2-Y_2)^2-Z_2(X_1-Y_1)Z_1^2(X_2+Y_2)^2,\end{aligned}$$

and

$$\begin{aligned}Y_3=&Z_1(X_2+Y_2)Z_2^2(X_1-Y_1)^2-Z_1(X_2-Y_2)Z_2^2(X_1+Y_1)^2\\&-Z_2(X_1+Y_1)Z_1^2(X_2-Y_2)^2+Z_2(X_1-Y_1)Z_1^2(X_2+Y_2)^2.\end{aligned}$$

Therefore, we have the following algorithm.
Addition in $\mathcal{A}$-projective coordinates $(X_1, Y_1, aZ_1)+(X_2, Y_2, aZ_2) = (X_3, Y_3, aZ_3)$.

$$\begin{aligned} A_1 &= X_1 + Y_1,\ B_1 = X_1 - Y_1,\ A_2 = X_2 + Y_2,\ B_2 = X_2 - Y_2,\\ D &= B_1 \cdot Z_2,\ E = A_2 \cdot Z_1,\ F = A_1 \cdot Z_2,\ G = B_2 \cdot Z_1,\ H = D \cdot E\\ I &= F \cdot G,\ J = F \cdot I,\ K = E \cdot H,\ X_3 = D \cdot H + J - G \cdot I - K,\\ Y_3 &= X_3 + FI + EH,\ Z_3 = (1/a)(D + F - E - G)^3. \end{aligned}$$

The costs for addition in $\mathcal{A}$-projective coordinates will be $10M + 1C + 1D$.

In the case of mixed addition, let $P = (X_1, Y_1, a)$ and $Q = (X_2, Y_2, aZ_2)$ be two points on E_a. Thus, the mixed addition takes $8M + 1C + 1D$ by setting $Z_1 = 1$ in the above algorithm.

4 Unified and Complete Addition Formulae

In this section, we study the *unified* and *complete* addition formulae. In generally, the *unified* addition formulae work for all but finitely many pairs of points. The *complete* addition formulae emphasize work for all inputs. We recall that the affine addition formula (1) and projective formula (10) do not work to double a point. Hereafter, we give an *unified* addition formulae for E_a. The unified addition formula make the curve E_a interesting against side-channel attacks. We present the *unified* addition formula for $E_a : y^2 = x^3 + x^2 - 1/a^3$ in $\mathcal{A}$-projective coordinates.

Theorem 6 *Let $P = (X_1, Y_1, aZ_1)$ and $Q = (X_2, Y_2, aZ_2)$ be two points on $Y^2Z = X^3 + X^2Z - Z^3/a^3$. The unified addition formulae on E_a are given $P + Q = (X_3, Y_3, aZ_3)$ where*

$$\begin{aligned} X_3 &= Z_1Z_2(Z_2(X_1 - Y_1) - Z_1(X_2 + Y_2)) + (X_1 + Y_1)(X_2 - Y_2)(X_1Y_2 + X_2Y_1),\\ Y_3 &= Z_1Z_2(Z_2(X_1 - Y_1) + Z_1(X_2 + Y_2)) + (X_1 + Y_1)(X_2 - Y_2)(X_1X_2 + Y_1Y_2),\\ Z_3 &= Z_2(X_1 - Y_1)^2(X_2 - Y_2) - Z_1(X_1 + Y_1)(X_2 + Y_2)^2. \end{aligned} \tag{11}$$

These formulae also work for point doubling, i.e., they are unified addition formulae.

The proof of Theorem 6 is omitted here since it is a long straight calculation. But we provide a magma code for checking the correctness of Theorem 6 in the Appendix A.1.

Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points of $y^2 = x^3 + x^2 - 1/a^3$ in affine coordinates, assume that $P + Q = (x_3, y_3)$, then the affine version of the above unified formula given by

$$\begin{aligned} x_3 &= \frac{(1/a^3)(x_1 - y_1 - x_2 - y_2) + (x_1 + y_1)(x_2 - y_2)(x_1 y_2 + x_2 y_1)}{(x_1 - y_1)^2(x_2 - y_2) - (x_1 + y_1)(x_2 + y_2)}, \\ y_3 &= \frac{(1/a^3)(x_1 - y_1 + x_2 + y_2) + (x_1 + y_1)(x_2 - y_2)(x_1 x_2 + y_1 y_2)}{(x_1 - y_1)^2(x_2 - y_2) - (x_1 + y_1)(x_2 + y_2)}. \end{aligned} \tag{12}$$

Unified Addition in $\mathcal{A}$-projective coordinates $(X_1, Y_1, aZ_1) + (X_2, Y_2, aZ_2) = (X_3, Y_3, aZ_3)$.

$$\begin{aligned} &A_1 = X_1 + Y_1,\ B_1 = X_1 - Y_1,\ A_2 = X_2 + Y_2,\ B_2 = X_2 - Y_2, \\ &D = A_1 \cdot A_2,\ E = B_1 \cdot B_2,\ F = Z_1 \cdot Z_2,\ G = Z_1 \cdot A_2,\ H = A_1 \cdot B_2, \\ &I = Z_2 \cdot B_1,\ X_3 = F \cdot (I - G) + H \cdot (E - D), \\ &Y_3 = F \cdot (I + G) - H \cdot (E + D),\ Z_3 = E \cdot I - D \cdot G. \end{aligned}$$

The algorithm costs $12M$.

Now we study the exceptional cases of formulae (4), (6), (10) and (11).

Theorem 7 *The doubling formulae (4) work for all input points on $E_a : Y^2 Z = X^3 + X^2 Z - Z^3/a^3$.*

Proof. Let $P = (X_1, Y_1, aZ_1)$ be a point on $E_a : Y^2 Z = X^3 + X^2 Z - Z^3/a^3$ such that the doubling formulae (4) do not work for the input P, that is the formulae (4) output

$$\begin{aligned} X_3 &= X_1 Y_1^3 + Y_1 Z_1^3 - X_1^3 Y_1 = 0, \\ Y_3 &= X_1^4 - Y_1^4 - X_1 Z_1^3 = 0, \\ Z_3 &= Z_1 Y_1^3 = 0. \end{aligned}$$

Hence $Z_1 = 0$ or $Y_1 = 0$ by $Z_3 = 0$. If $Z_1 = 0$ then $X_1 = 0$ and $Y_1 \neq 0$ implies $Y_3 \neq 0$. If $Y_1 = 0$ then $Z_1 \neq 0$ and $X_1 \neq 0$, one can get $X_1(X_1 - Z_1)^3 = 0$ by $Y_3 = 0$, thus $X_1 = Z_1$ implies $X_1 = Z_1 = 0$ which is a contradiction. □

The following theorem shows that tripling formulae work for all inputs.

Theorem 8 *The tripling formulae (6) work for all input points on $E_a : Y^2Z = X^3 + X^2Z - Z^3/a^3$.*

Proof. Let $P = (X_1, Y_1, aZ_1)$ be a point on $E_a : Y^2Z = X^3 + X^2Z - Z^3/a^3$ such that the doubling formulae (6) do not work for the input P, that is the formulae (6) output

$$\begin{aligned} X_3 &= (X_1 - Z_1)^3(X_1^2 - Y_1^2 - X_1Z_1)^3 = 0, \\ Y_3 &= Y_1^3(X_1^2 + X_1Z_1 + Z_1^2 - Y_1^2)^3 = 0, \\ Z_3 &= (Z_1^9 - X_1^9)/a = 0. \end{aligned}$$

One can get $X_1 = Z_1$ by $Z_3 = 0$, hence $Y_1 \neq 0$ implies $X_1^2 + X_1Z_1 + Z_1^2 - Y_1^2 = 0$. Since $X_1 = Z_1$, hence $Y_1 = 0$ which is a contradiction. □

The following lemma describes the exceptional cases of addition formulae (10).

Lemma 9 *Let $P_1 = (X_1, Y_1, aZ_1)$ and $P_2 = (X_2, Y_2, aZ_2)$ be two points on $E_a : Y^2Z = X^3 + X^2Z - Z^3/a^3$. The addition formula (10) do not work for the input P_1 and P_2 if and only if $P_1 - P_2 = (0, 1, 0)$.*

Proof. First, assume that addition formula (10) do not work for the input P_1 and P_2, that is, we have $X_3 = Y_3 = Z_3 = 0$. If $Z_1 = 0$ then $X_1 = 0$ implies $Z_3 = Z_2^2Y_1^2 = 0$ by formula (9), which means $Z_2 = 0$. Similarly, If $Z_2 = 0$ then $Z_1 = 0$. Assume now that $Z_1Z_2 \neq 0$. We can let $Z_1 = Z_2 = 1$, then $P_1 = (X_1, Y_1, a)$ and $P_2 = (X_2, Y_2, a)$. Hence $Z_3 = (1/a)(X_2 - X_1)^3 = 0$ implies $X_1 = X_2$. Thus $X_3 = X_1(Y_1 + Y_2)(Y_1 - Y_2) = 0$ and $Y_3 = Y_1Y_2(Y_1 - Y_2) = 0$ by formula (9). If $Y_1 - Y_2 \neq 0$ then $Y_1Y_2 = 0$. Since $aY_1^2 = X_1^3 + aX_1^2 - 1$ and $X_1 = X_2$, thus $aY_1^2 = aY_2^2 = -1$ which is a contradiction, hence $Y_1 - Y_2 = 0$ then $P_1 = P_1$, thus $P_1 - P_2 = (0, 1, 0)$. The other direction is clear. □

The following lemma describes a special property of addition formulae (11).

Lemma 10 *Let $P_1 = (X_1, Y_1, aZ_1)$ and $P_2 = (X_2, Y_2, aZ_2)$ be two points on $E_a : Y^2Z = X^3 + X^2Z - Z^3/a^3$. Assume that the addition formulae (11) do not work for the input P_1 and P_2, then the addition formulae (11) work for the input P_2 and P_1.*

Proof. Since the addition formulae (11) do not work for the input P_1 and P_2, that is, we have $X_3 = Y_3 = Z_3 = 0$. If $Z_1 = 0$, then $X_1 = 0$ and we can let $Y_1 = 1$. Thus, $X_3 = X_2(X_2 - Y_2) = 0, Y_3 = Y_2(X_2 - Y_2) = 0, Z_3 = Z_2(X_2 - Y_2) = 0$.

If $Z_2 = 0$ then $X_2 = 0$ implies $Y_2 = 0$ from $Y_3 = 0$ which is a contradiction. Hence $Z_2 \neq 0$, thus $X_2 = Y_2$ by $Z_3 = 0$, hence $aX_2^2 Z_2 = X_2^3 + aX_2^2 - Z_2^3$ implies $X_2 = Z_2$. Therefore one get $P_2 = (1/a, 1/a, 1)$. The other direction, let $P_1 = (1/a, 1/a, 1) = (1, 1, a)$ and $P_2 = (0, 1, 0)$, then $X_3 = Y_3 = Z_3 = 2$.

Similarly, if $Z_2 = 0$ one can get $P_1 = (1/a, -1/a, 1) = (1, -1, a)$ and $P_2 = (0, 1, 0)$. The other direction, let $P_1 = (0, 1, 0)$ and $P_2 = (1, -1, a)$, then $X_3 = Y_3 = Z_3 = 2$.

Assume now $Z_1 \neq 0$ and $Z_2 \neq 0$. We write $P_1 = (X_1, Y_1, a)$ and $P_2 = (X_2, Y_2, a)$. From $X_3 = Y_3 = Z_3 = 0$, we have

$$(X_1 - Y_1) - (X_2 + Y_2) + (X_1 + Y_1)(X_2 - Y_2)(X_1Y_2 + X_2Y_1) = 0 \tag{13}$$

$$(X_1 - Y_1) + (X_2 + Y_2) + (X_1 + Y_1)(X_2 - Y_2)(X_1X_2 + Y_1Y_2) = 0 \tag{14}$$

$$(X_1 - Y_1)^2(X_2 - Y_2) - (X_1 + Y_1)(X_2 + Y_2)^2 = 0 \tag{15}$$

$$\text{Adding (13) } + \text{(14) yields } (X_1 - Y_1) = (X_1 + Y_1)^3(X_2 - Y_2)(X_2 + Y_2).$$

Putting this relation into the equation (15), we obtain the relation

$$(X_1 + Y_1)^3(X_2 - Y_2)^3 = 1 \Rightarrow (X_1 + Y_1)(X_2 - Y_2) = 1.$$

If the addition formulae (11) do not work for the input P_2 and P_1. Then, one have

$$(X_2 + Y_2)(X_1 - Y_1) = 1$$

by the swapping the order of the points in the addition formulae (11). Therefore, $(X_1+Y_1)(X_2-Y_2)-(X_2+Y_2)(X_1-Y_1) = 0$ implies $X_1Y_2 = X_2Y_1$. If $X_1 = 0$ then $X_2 = 0$, then $Y_1+Y_2 = 0$ by (13) and $Y_2-Y_1 = 0$ by (14), thus $Y_1 = Y_2 = 0$ which is a contradiction. Therefore, $X_1X_2Y_1Y_2 \neq 0$ implies $\frac{X_1}{X_2} = \frac{Y_1}{Y_2}$, implies $P_1 = P_2$. But putting this relation into the equation (15), one have $X_1 - Y_1 = X_1 + Y_1$ which is a contradiction. Therefore, the addition formulae (11) work for the input P_2 and P_1. □

Assume that the output of formulae (11) is (X_3, Y_3, Z_3) when input points P_1 and P_2, and assume that the output is (U_3, V_3, W_3) when input points P_2 and P_1. One can get, by the lemma 10, if $(X_3, Y_3, Z_3) = (0, 0, 0)$ then $(U_3, V_3, W_3) \neq (0, 0,)$, if $(U_3, V_3, W_3) = (0, 0,)$ then $(X_3, Y_3, Z_3) \neq (0, 0, 0)$. Moreover, if both items are not equal to $(0, 0, 0)$, then $(X_3, Y_3, Z_3) = (U_3, V_3, W_3)$ as the point on E_a. We write it as the following theorem.

Theorem 11 *Let $E_a : Y^2Z = X^3 + X^2 - Z^3/a^3$ over $\mathbb{F}_{3^m}$ with $a \neq 0$. Fix $P_1,\ P_2 \in E_a(\mathbb{F}_{3^m})$. Write $P_1 = (X_1, Y_1, aZ_1)$ and $P_2 = (X_2, Y_2, aZ_2)$. Define*

$$\begin{aligned} X_3 &= Z_1Z_2(Z_2(X_1 - Y_1) - Z_1(X_2 + Y_2)) + (X_1 + Y_1)(X_2 - Y_2)(X_1Y_2 + X_2Y_1), \\ Y_3 &= Z_1Z_2(Z_2(X_1 - Y_1) + Z_1(X_2 + Y_2)) + (X_1 + Y_1)(X_2 - Y_2)(X_1X_2 + Y_1Y_2), \\ Z_3 &= Z_2(X_2 - Y_2)(X_1 - Y_1)^2 - Z_1(X_1 + Y_1)(X_2 + Y_2)^2. \end{aligned}$$

and

$$\begin{aligned} U_3 &= Z_1Z_2(Z_1(X_2 - Y_2) - Z_2(X_1 + Y_1)) + (X_1 - Y_1)(X_2 + Y_2)(X_1Y_2 + X_2Y_1), \\ V_3 &= Z_1Z_2(Z_1(X_2 - Y_2) + Z_2(X_1 + Y_1)) + (X_1 - Y_1(X_2 + Y_2))(X_1X_2 + Y_1Y_2), \\ W_3 &= Z_1(X_1 - Y_1)(X_2 - Y_2)^2 - Z_2(X_2 + Y_2)(X_1 + Y_1)^2. \end{aligned}$$

Then $X_3W_3 = U_3Z_3$ and $Y_3W_3 = V_3Z_3$. Furthermore, at least one of the following cases occurs: $(X_3, Y_3, Z_3) \neq (0, 0, 0)$ or $(U_3, V_3, W_3) \neq (0, 0, 0)$.

Now we study the exceptional cases of addition formulae (11).

Theorem 12 *Let P_1 and P_2 be points on $E_a : Y^2Z = X^3 + X^2 - Z^3/a^3$. Then the addition formulae (11) do not work for the input P_1, P_2 if and only if $P_1 - P_2 = (1, -1, a)$.*

Proof. From lemma 10, we only need see $Z_1 \neq 0$ and $Z_2 \neq 0$. Without loss of generality, we can let $P_1 = (X_1, Y_1, a)$ and $P_2 = (X_2, Y_2, a)$ be two points on $E_a : Y^2Z = X^3 + X^2Z - Z^3/a^3$. Assume that the addition formulae (11) do not work for the input P_1 and P_2, then $X_3 = Y_3 = Z_3 = 0$. Similarly, we can assume that $P_1 \neq \pm P_2$. Since $(X_1 + Y_1)(X_2 - Y_2) = 1$ by lemma 10, Putting this relation into the equation (15), we obtain the relation $(X_1 - Y_1) = (X_1 + Y_1)(X_2 + Y_2)$, hence one can get

$$X_2 = \frac{Y_1 - X_1 - 1}{X_1 + Y_1} \text{ and } Y_2 = \frac{Y_1 - X_1 + 1}{X_1 + Y_1}.$$

Therefore, we can reach $P_1 - P_2 = (1, -1, a)$ by calculation. For the other direction, one only need see $P_1 = (X_1, Y_1, a)$ and $P_2 = (X_2, Y_2, a)$. If $P_1 - P_2 = (1, -1, a)$, then $P_2 = (Y_1 - X_1 - 1, Y_1 - X_1 + 1, a(X_1 + Y_1)$ which satisfy the relation $(X_1 + Y_1)(X_2 - Y_2) = 1$ and $(X_1 - Y_1) = (X_1 + Y_1)(X_2 + Y_2)$, which mean $X_3 = Y_3 = Z_3 = 0$. □

A practical solution is now provided for prevent exceptional cases of formulae (11).

Corollary 13 *Let G be a subgroup of $E_a(\mathbb{F}_{3^m})$ which is not containing point $(1, -1, a)$, Then the addition formula (11) work for all pairs of points in G.*

5 Efficiency Comparison and Timing Results

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.

5.1 Efficiency Comparison

We first recall the previous results on ordinary elliptic curves in characteristic three. In [7], 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, new doubling, mixed addition and tripling formulae in projective coordinates require $5M+3S+3C$, $8M+2C$ and $6M+6C$ respectively. It was noticed that a tripling algorithm cost $5M + 5C + 1D$ using Jacobian projective coordinates in [13].

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

Table 1. Costs of point operations for different systems on $y^2 = x^3 + x^2 + c$

Coordinate System	Mixed addition	Doubling	Tripling
Projective[15]	9M + 2S + 1C	6M + 3C	7M + 2S + 5C
Jacobian[15]	7M + 3S + 2C	6M + 2S + 3C	5M + 1S + 4C + 1D
López Dahab[15]	10M + 3S	7M + 4S + 2C	10M + 3S + 5C
Jacobian[13]	7M + 3S + 2C + 1D	5M +2S + 3C	3M + 2S + 5C + 1D
ML-coordinates [7]	8M + 2C	5M + 3S + 3C	6M + 6C
$\mathcal{A}$-projective	**8M + 1C + 1D**	**3M + 2C**	**4M + 4C + 1D**

5.2 Timing Results

We provide timing results of the various algorithms. By using Magma online-demo [3], we implement triple-and-add methods to compute point multiplication.

We denote by E-97 the ordinary elliptic curve in Sec. 5 of [15]. According to the methods in [14, 5], more ordinary curves over finite fields of characteristic three for high security level are also generated. We name them as E-151, E-181, E-263, E-331, and E-337 respectively. We denote by $|k|$ the approximate bit length of the random large integer k when computing scalar multiplication $[k]P$. All timing results(in ms) are presented in Table 2.

Table 2. Timing Results for Different Coordinate Systems on Ordinary Curves in Characteristic Three

Coordinate System	E-97	E-151	E-181	E-263	E-331	E-337
	$\|k\| = 150$	$\|k\| = 230$	$\|k\| = 280$	$\|k\| = 410$	$\|k\| = 530$	$\|k\| = 530$
Projective[15]	11	15	21	27	31	42
Jacobian[13]	2	11	18	23	26	36
$\mathcal{A}$-projective	2	8	15	18	21	28

6 Conclusions

In this paper, a new point representation $\mathcal{A}$-projective is introduced for Weierstrass elliptic curves in characteristic three. We derive efficient basic group operations and discuss the exceptional cases. We then compare their performance to the previously best results for different coordinates systems. Our count shows that the new formulae is faster than the previously known approach. 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. Barreto, P.S.L.M., Galbraith, S.D., O'Eigeartaigh, C., Scott, M.: Efficient pairing computation on supersingular abelian varieties. Des. Codes Cryptography 42(3), 239–271. (2007)
2. Blake, I.F., Seroussi, G., Smart, N.P.: Elliptic Curves in Cryptography, vol. 265. Cambridge University Press, New York, NY, USA (1999)
3. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symbolic Comput. 24(3-4), 235–265 (1997)

4. Cohen, H., Frey, G. (eds.): Handbook of elliptic and hyperelliptic curve cryptography. CRC Press (2005)
5. Fouquet, M., Gaudry, P., R., H.: An extension of satoh's algorithm and its implementation. J. Ramanujan Math. Soc. 15, 281–318 (2000)
6. Hankerson, D., Menezes, A.J., Vanstone, S.: Guide to Elliptic Curve Cryptography. Springer-Verlag, pub-SV:adr (2004)
7. 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)
8. Kim, K.H.: A Note on Point Multiplication on Supersingular Elliptic Curves over Ternary Fields. Cryptology ePrint Archive, Report 2007/310 (2007)
9. Koblitz, N.: Elliptic curve cryptosystems. Mathematics of Computation 48, 203–209. (1987)
10. 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)
11. L$\acute{o}$pez, 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)
12. Miller, V.S.: Use of elliptic curves in cryptography. In: In Advances in Cryptology - Crypto'85. pp. 417–426. LNCS 218, Springer-Verlag (1986)
13. 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)
14. 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)
15. 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 Magma Code for Unified Addition Formulae

We can use the following script for the magma computer algebra system checks the formulae in theorem. Note that x3,y3,z3 in script equal to X_3, Y_3, Z_3 respectively. And (u3,v3,w3) $= P+Q$ from the affine addition formula in Section 2.

```
clear;
F:=GF(3);
```

```
K<a,x1,x2,y1,y2>:=FieldOfFractions(PolynomialRing(F,5));
R<z1,z2>:=PolynomialRing(K,2);
S:=quo<R|y1^2*z1-(x1^3+x1^2*z1-z1^3/a^3),
 y2^2*z2-(x2^3+x2^2*z2-z2^3/a^3)>;
A1:=x1+y1; B1:=x1-y1; C1:=z1/a;
A2:=x2+y2; B2:=x2-y2; C2:=z2/a;
D:=A1*A2; E:=B1*B2; F:=C1*C2;
G:=A2*C1; H:=A1*B2; I:=B1*C2;
x3:=F*(I-G)+H*(E-D);
y3:=F*(I+G)-H*(E+D);
z3:=a*(E*I-D*G);

A:=x1*z2; B:=x2*z1;
D:=y1*z2; E:=y2*z1;
F:=A+B; G:=A-B;H:=D+E; I:=D-E;
J:=z1*z2; K:=(I+G)*(I-G); L:=J*K;
u3:=G*L-G^3*F;
v3:=-I*L+G^3*H;
w3:=G^3*J;

S!(x3*w3-u3*z3);
S!(y3*w3-v3*z3);
```

A.2 Ordinary Elliptic Curves over Finite Fields with Characteristic Three

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

m The extension degree of the field $\mathbb{F}_{3^m}$.

$f(z)$ The reduction polynomial of degree m.

c The coefficients of the elliptic curve $E:\ y^2 = x^3 + x^2 + c$.

r The prime order of the base point P.

h The cofactor, that is $\sharp E(\mathbb{F}_{3^m}) = hr$.

Table 3. Parameters for Ordinary Elliptic Curves in Characteristic Three

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