New Fast Algorithms for Arithmetic on Elliptic Curves over Finite Fields of Characteristic Three

Kwang Ho Kim , So In Kim , and Ju Song Choe

Department of Algebra, Institute of Mathematics
National Academy of Sciences, D. P. R. of Korea
kimkhhj1980@yahoo.com.cn

Abstract: In this paper we propose new formulae and algorithms for arithmetic on ordinary elliptic curve with a point of order 3 over finite field of characteristic three, by which the cost of a point multiplication on the curves decreases about 10~20% .

Keywords: characteristic three elliptic curve, point addition, point doubling, point tripling, Hessian form, Weierstrass form

1. Introduction

Since the elliptic curve cryptography has been proposed by Neal Koblitz and Victor Miller in 1985 independently, research on speeding up the elliptic curve group operation continues to get increasing attraction. But the case of characteristic three has been considered relatively less than cases of fields of even characteristic and large prime fields.

To the best of our knowledge, for point multiplication on ordinary elliptic curve over field of characteristic three the most efficient way is known as one shown in [2].

In first portion of this paper we propose new fast algorithms for arithmetic on Hessian elliptic curves over finite field of characteristic three, which reduce costs of a doubling and a mixed point addition from **3M+3C** and **10M** (cf. [2]) to **3M+2C** and **9M+1C,** respectively. Here **M, C** are the costs of a multiplication and a cubing in the finite field, respectively. (It is noted that **1M** ≈ **10C** in the field.)

These algorithms can realize fast point multiplication nearly comparable with the case of even characteristic, on ordinary elliptic curves over finite field of characteristic three.

In next portion we propose a kind of projective coordinates we call ML coordinates and new algorithms for arithmetic on Weierstrass elliptic curve in it, which reduce costs of a tripling and a mixed point addition from **7M+4C** and **10M+2C** (cf. [2]) to **6M+6C** and **8M+2C,** respectively**.**

We note that in the case of ternary finite field, a field addition and subtraction can be negligible compared with a field multiplication (a squaring) or a cubing.(cf. [12])

So we do not take into account the costs for them, in all evaluations of this paper.

2. Arithmetic on elliptic curves over field of characteristic three

Ordinary elliptic curves over finite field F_{3^m} can be represented by :

$$y^2 = x^3 + ax^2 + c \ (a, c \in F_{3^m}{}^*) \qquad \textbf{(1)}$$

in Weierstrass form , or in the case of curves with group order divisible by 3, by :

$$x^3 + y^3 + 1 = Dxy \ (D \in F_{3^m}{}^*) \qquad \textbf{(2)}$$

in Hessian form. (cf. [2]) In this paper, we restrict our consideration to curves having Hessian representation, or with coefficient $a = 1$ in Weierstrass equation **(1)**.

Note 1. The restriction $a = 1$ eliminates a half of the curves in characteristic three, and is akin to the assumption for curves over large prime field to have the form $y^2 = x^3 - 3x + b$, or over field of even characteristic to have the form $y^2 + xy = x^3 + x^2 + b$.(cf. [2]) ▌

Using projective point representation, we can avoid all of inversions which are much more expensive than any other field operation (if required, except for only one needed to come back to affine) in the computation of point multiplication on the curve.

A projective coordinates (X, Y, Z) corresponds to affine (x, y) as follows: (cf. [7])

- Ordinary projective: $(x, y) = (X / Z, Y / Z)$
- Jacobian projective: $(x, y) = (X / Z^2, Y / Z^3)$ **(3)**
- Lopez Dahab projective: $(x, y) = (X / Z, Y / Z^2)$.

Weierstrass equation **(1)** of the curve can be expressed as

$$Y^2 = X^3 + X^2 Z^2 + cZ^6 \qquad \textbf{(4)}$$

in Jacobian projective coordinates and the Hessian equation **(2)** as

$$X^3 + Y^3 + Z^3 = DXYZ \qquad \textbf{(5)}$$

in ordinary projective coordinates, for example. The projective representations was used for Weierstrass and Hessian form of the curve in [2]. We again restrict our consideration for the point addition to the mixed case where one point is affine and the other point is in a projective representation, because the case is most important in practical applications.(cf. [7])

3. Previous algorithms for arithmetic on ordinary elliptic curve

3.1 Hessian form

Following formulae and algorithms were proposed in [2]. The projective equation of the curve is **(5)** and it's zero(infinity) is represented as $(1,-1,0)$. For a given point $Q = (X_2, Y_2, Z_2)$, we have

$-Q = (Y_2, X_2, Z_2)$. For given two points $P = (X_1, Y_1, 1)$ and $Q = (X_2, Y_2, Z_2)$ $(P \neq Q)$,

$P + Q = (X_3, Y_3, Z_3)$ is given by: $X_3 = Y_1^2 X_2 Z_2 - Y_2^2 X_1$,

$$Y_3 = X_1^2 Y_2 Z_2 - X_2^2 Y_1 \text{ ,} \qquad \textbf{(6)}$$

$$Z_3 = X_2 Y_2 - Z_2^2 X_1 Y_1 .$$

For a given point $P = (X_1, Y_1, Z_1)$, doubling $[2](X_1, Y_1, Z_1) = (X_3, Y_3, Z_3)$ is given by:

$$X_3 = Y_1(Z_1^3 - X_1^3)$$

$$Y_3 = X_1(Y_1^3 - Z_1^3) \qquad \textbf{(7)}$$

$$Z_3 = Z_1(X_1^3 - Y_1^3) .$$

- **Addition** $P + Q = (X_3, Y_3, Z_3)$ of $P = (X_1, Y_1, 1)$ and $Q = (X_2, Y_2, Z_2)$

$O_1 = Y_1 X_2$	**M**
$O_2 = X_1 Y_2$	**M**
$O_3 = X_1 Z_2$	**M**
$O_4 = Y_1 Z_2$	**M**
$O_5 = O_1 O_4$	**M**
$O_6 = O_2 O_3$	**M**
$O_7 = X_2 Y_2$	**M**
$O_8 = O_2 Y_2$	**M**
$O_9 = O_1 X_2$	**M**
$O_{10} = O_3 O_4$	**M**
$O_{11} = O_5 - O_8 = X_3$	**A**
$O_{12} = O_6 - O_9 = Y_3$	**A**
$O_{13} = O_7 - O_{10} = Z_3$	**A**
Total cost	**10M**

Table 1.(Table 11 of [2]**)** Hessian mixed point addition algorithm

- **Doubling** $[2](X_1, Y_1, Z_1) = (X_3, Y_3, Z_3)$ of (X_1, Y_1, Z_1)

$O_1 = X_1^3$	**C**
$O_2 = Y_1^3$	**C**
$O_3 = Z_1^3$	**C**
$O_4 = O_3 - O_1$	**A**

$O_5 = O_2 - O_3$	**A**
$O_6 = O_1 - O_2$	**A**
$O_7 = Y_1 O_4 = X_3$	**M**
$O_8 = X_1 O_5 = Y_3$	**M**
$O_9 = Z_1 O_6 = Z_3$	**M**
Total cost	**3M + 3C**

Table 2.(Table 12 of [2]**)** Hessian point doubling algorithm

3.2 Weierstrass form

Following formulae and algorithms were proposed for arithmetic on elliptic curve in Weierstrass form in [2].

-Formulae for point addition, doubling and tripling in affine coordinates

- **Addition:** $(x_1, y_1) + (x_2, y_2) = (x_3, y_3), x_1 \neq x_2$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

$$x_3 = \lambda^2 - a - x_1 - x_2 \qquad \textbf{(8)}$$

$$y_3 = \lambda(x_1 - x_3) - y_1 .$$

- **Doubling:** $[2](x, y) = (x_2, y_2)$

$$\lambda = \frac{ax}{y}$$

$$x_2 = \lambda^2 - a + x \qquad \textbf{(9)}$$

$$y_2 = \lambda(x - x_2) - y .$$

- **Tripling:** $[3](x, y) = (x_3, y_3)$

$$x_3 = \frac{(x^3 + c)^3 - a^3 c x^3}{a^2 (x^3 + c)^2} \qquad \textbf{(10)}$$

$$y_3 = \frac{y^9 - a^3 y^3 (x^3 + c)^2}{a^3 (x^3 + c)^3} .$$

- Algorithms for point addition and tripling in Jacobian projective coordinates

- **Addition** $P + Q = (X_3, Y_3, Z_3)$ of $P = (X_{1,}, Y_1, 1)$ and $Q = (X_2, Y_2, Z_2)$

$O_1 = Z_2^2$	**M**
$O_2 = Z_2^3$	**C**

$O_3 = X_1 O_1$	**M**
$O_4 = X_2 - O_3$	**A**
$O_5 = X_2 + O_3$	**A**
$O_6 = Y_1 O_2$	**M**
$O_7 = Y_2 - O_6$	**A**
$O_8 = O_4 z_2 = z_3$	**M**
$O_9 = X_2 + O_1 + O_3$	**2A**
$O_{10} = O_4^2$	**M**
$O_{11} = O_9 O_{10}$	**M**
$O_{12} = O_7^2$	**M**
$O_{13} = O_{12} - O_{11} = X_3$	**A**
$O_{14} = O_3 O_{10}$	**M**
$O_{15} = O_{14} - O_{13}$	**A**
$O_{16} = O_7 O_{15}$	**M**
$O_{17} = O_4^3$	**C**
$O_{18} = O_6 O_{17}$	**M**
$O_{19} = O_{16} - O_{18} = Y_3$	**A**
Total cost	**10M+2C**

Table 3.(Table 7 of [2]**)** Weierstrass mixed point addition algorithm

- **Tripling** [3]$(X,Y,Z) = (X_3, Y_3, Z_3)$ of (X,Y,Z)

$O_1 = X^3$	**C**
$O_2 = Y^3$	**C**
$O_3 = Z^3$	**C**
$O_4 = O_3^2$	**M**
$O_5 = cO_4$	**M**
$O_6 = O_4 O_5$	**M**
$O_7 = O_1 + O_5$	**A**
$O_8 = O_1 - O_5$	**A**

$O_9 = O_1 O_6$	**M**
$O_{10} = O_7^3$	**C**
$O_{11} = O_{10} - O_9 = X_3$	**A**
$O_{12} = O_3 O_7 = Z_3$	**M**
$O_{13} = O_6 O_8$	**M**
$O_{14} = O_{10} + O_{13}$	**A**
$O_{15} = O_2 O_{14} = Y_3$	**M**
Total cost	**7M+4C**

Table 4. (Table 9 of [2]**)** Weierstrass point tripling algorithm

Recently, in [11] C. Negre proposed a slightly modified variant of above tripling algorithm:

$A = (XZ)^3$	**1M+1C**
$B = cZ^9$	**1M+2C**
$D_1 = Y^3$	**1C**
$D_2 = D_1^2$	**1M**
$Z_3 = A + B$	
$X_3 = D_2 - AZ_3$	**1M**
$Y_3 = D_1^3 - YZ_3^2$	**2M+1C**
Total cost	**6M+5C**

Table 4.1.(cf. **Table 2** of [11]**)** Improved Weierstrass point tripling algorithm

This algorithm improves nearly by a multiplication the cost of algorithm in **Table 4**.

In [11], it was noticed that in the case of sparse coefficient c **,** a point tripling can be obtained at the cost **5M+5C** and the gain is not negligible .

4. New formulae for arithmetic on ordinary elliptic curve

4.1 Hessian form

We will consider the Hessian curve **(5)** in ordinary projective coordinates, as in [2]**.**

[Theorem 1] There exist algorithms that give the sum of two different points on characteristic three ordinary elliptic curve, at the cost **9M+1C** and the doubling of a point, at the cost **3M+2C**.

(Proof) Clearly**,** doubling $[2](X_1, Y_1, Z_1) = (X_3, Y_3, Z_3)$ of a given point (X_1, Y_1, Z_1) is obtained by:

$$X_3 = Y_1(Z_1 - X_1)^3$$
$$Y_3 = X_1(Y_1 - Z_1)^3 \qquad \textbf{(11)}$$
$$Z_3 = -Z_1[(Z_1 - X_1) + (Y_1 - Z_1)]^3 \textbf{,}$$

from **(7)** and properties of ternary finite field**.**

We will show that when $Q \neq 0$ sum $P + Q = (X_3, Y_3, Z_3)$ of $P = (X_1, Y_1, 1)$ and $Q = (X_2, Y_2, Z_2)$ is obtained by:

$$X_3 = (Y_1 Z_2)^2 X_2 - Y_2^2 (X_1 Z_2)$$
$$Y_3 = (X_1 Z_2)^2 Y_2 - X_2^2 (Y_1 Z_2) \qquad \textbf{(12)}$$
$$Z_3 = D^{-1}(X_2 + Y_2 - X_1 Z_2 - Y_1 Z_2)^3 \textbf{ .}$$

(When $Q = 0$, the addition is trivial.)

It will be sufficient to show that projective point representation **(6)** and **(12)** give the same affine point. From **(12)**, obviously

$$X_3 = Z_2(Y_1^2 X_2 Z_2 - Y_2^2 X_1),$$
$$Y_3 = Z_2(X_1^2 Y_2 Z_2 - X_2^2 Y_1),$$
$$Z_3 = D^{-1}(X_2 + Y_2 - Z_2 X_1 - Z_2 Y_1)^3$$
$$= D^{-1}(X_2 + Y_2 + Z_2 - Z_2(X_1 + Y_1 + 1))^3$$
$$= D^{-1}(X_2 + Y_2 + Z_2)^3 - D^{-1} Z_2^3 (X_1 + Y_1 + 1)^3$$
$$= X_2 Y_2 Z_2 - Z_2^3 X_1 Y_1 \ = Z_2(X_2 Y_2 - Z_2^2 X_1 Y_1) \ .$$

(**Note 2.** $DX_2 Y_2 Z_2 = (X_2 + Y_2 + Z_2)^3$, $DX_1 Y_1 = (X_1 + Y_1 + 1)^3$ because P, Q are on the curve.)

It means that X_3, Y_3, Z_3's in **(6)** and **(12)** are different only by a common factor $Z_2 \neq 0$, giving the same affine point. Using **(11)** and **(12)** we propose following algorithms for a point addition and doubling.

- **Addition** $P + Q = (X_3, Y_3, Z_3)$ of $P = (X_1, Y_1, 1)$ and $Q = (X_2, Y_2, Z_2)$

$O_1 = X_1 Z_2$ **M**

$O_2 = Y_1 Z_2$ **M**

$O_3 = O_1 Y_2$ **M**

$O_4 = O_2 X_2$ **M**

$O_5 = O_2 O_4$ **M**

$O_6 = O_3 Y_2$ **M**

$O_7 = O_1 O_3$	**M**
$O_8 = O_4 X_2$	**M**
$O_9 = O_5 - O_6 = X_3$	**A**
$O_{10} = O_7 - O_8 = Y_3$	**A**
$O_{11} = X_2 + Y_2 - O_1 - O_2$	**3A**
$O_{12} = O_{11}^3$	**C**
$O_{13} = O_{12} D^{-1} = Z_3$	**M**
Total cost	**9M+1C**

Table 5. Proposed Hessian mixed point addition algorithm

- **Doubling** $[2](X_1, Y_1, Z_1) = (X_3, Y_3, Z_3)$

$O_1 = Z_1 - X_1$	**A**
$O_2 = Y_1 - Z_1$	**A**
$O_3 = O_1^3$	**C**
$O_4 = O_2^3$	**C**
$O_5 = -(O_3 + O_4)$	**A**
$O_6 = Y_1 O_3 = X_3$	**M**
$O_7 = X_1 O_4 = Y_3$	**M**
$O_8 = Z_1 O_5 = Z_3$	**M**
Total cost	**3M+2C**

Table 6. Proposed Hessian point doubling algorithm

Note 3. In the above point addition algorithm D^{-1} is a constant which can be precomputed from the curve equation and the last multiplication is by the constant. In our experiences, a constant multiplication usually can be computed much faster than a general multiplication, at the cost of some storage, in practice. If D^{-1} is sparse, the constant multiplication is nearly free. So, in below tables for comparing costs, we show in a parenthesis the number of constant multiplications in the algorithm.

algorithm	**doubling**	**addition**
N. P. Smart et al. [2]	**3M+3C** (0)	**10M** (0)
Proposed	**3M+2C** (0)	**9M+1C** (1)

Table 7. Comparing costs of algorithms for arithmetic on Hessian curve

4.2 Weierstrass form

Before proceeding we propose a type of projective coordinates(ML-coordinates) which are made of four variables and the relationship between it and affine coordinates is as follows:

$$(X,Y,Z,T) \leftrightarrow (X/T, Y/Z^3), \ \textit{where} \ T = Z^2.$$

In this coordinates, considered curve equation is also **(4)** and formulae for affine arithmetic are given in subsection **3.2**.

[Theorem 2] In ML- projective coordinates there exist algorithms that give the sum of two different point , at the cost **8M+2C** and the tripling of a point, at the cost **6M+6C**.

(Proof) First of all, we will show that the sum $P+Q=(X_3,Y_3,Z_3)$ of $P=(X_1,Y_1,1)$ and $Q=(X_2,Y_2,Z_2)$ is obtained by: $Z_3=(X_2-X_1Z_2^{\,2})Z_2$,

$$X_3=(Y_2-Y_1Z_2^{\,3})^2-(X_2-X_1Z_2^{\,2})^3-Z_3^{\,2}+X_1Z_3^{\,2}, \qquad \textbf{(13)}$$

$$Y_3=(X_1Z_3^{\,2}-X_3)(Y_2-Y_1Z_2^{\,3})-Y_1Z_2^{\,3}(X_2-X_1Z_2^{\,2})^3$$

and tripling $[3](X,Y,Z)=(X_3,Y_3,Z_3)$ of a given point (X,Y,Z) by:

$$Z_3=cZ^9+X^3Z^3, \ X_3=[X^3+Z^6(c^2+c^3)^{\frac{1}{3}}]^3-cZ^9Z_3, \ Y_3=Y^3(X_3-cZ_3Z^9) \qquad \textbf{(14)}$$

in Jacobian projective coordinates**.**

Affine point representation corresponding to **(13)** is**:**

$$\begin{aligned}
x_3 &= X_3/Z_3^{\,2}=[(Y_2-Y_1Z_2^{\,3})^2-(X_2-X_1Z_2^{\,2})^3-Z_3^{\,2}+X_1Z_3^{\,2}]/[(X_2-X_1Z_2^{\,2})^2Z_2^{\,2}]\\
&=\{(Y_2-Y_1Z_2^{\,3})/[(X_2-X_1Z_2^{\,2})Z_2]\}^2-(X_2-X_1Z_2^{\,2})/Z_2^{\,2}-1+X_1\\
&=[(y_2-y_1)/(x_2-x_1)]^2-(x_2-x_1)-1+x_1=[(y_2-y_1)/(x_2-x_1)]^2-1-x_2-x_1,\\
y_3 &= Y_3/Z_3^{\,3}=[(X_1Z_3^{\,2}-X_3)(Y_2-Y_1Z_2^{\,3})-Y_1Z_2^{\,3}(X_2-X_1Z_2^{\,2})^3]/Z_3^{\,3}\\
&=[(X_1Z_3^{\,2}-X_3)(Y_2-Y_1Z_2^{\,3})]/Z_3^{\,3}-Y_1=[(X_1Z_3^{\,2}-X_3)/Z_3^{\,2}][(Y_2-Y_1Z_2^{\,3})/Z_3]-Y_1\\
&=[(y_2-y_1)/(x_2-x_1)](x_1-x_3)-y_1.
\end{aligned}$$

This is identical with **(8)** under the condition $a=1$**.**

And affine point representation corresponding to **(14)** is**:**

$$\begin{aligned}
x_3 &= X_3/Z_3^{\,2}=[X^9+Z^{18}(c^2+c^3)-cZ^9Z_3]/(cZ^9+X^3Z^3)^2\\
&=[X^9+c^3Z^{18}-cX^3Z^{12}]/(cZ^9+X^3Z^3)^2=[(x^3+c)^3-cx^3)]/(x^3+c)^2,\\
y_3 &= Y_3/Z_3^{\,3}=Y^3(X_3-cZ_3Z^9)/Z_3^{\,3}=Y^3(X^9+c^3Z^{18}+cX^3Z^{12}-c^2Z^{18})/(cZ^9+X^3Z^3)^3\\
&=Y^3(X^9+c^3Z^{18}+cX^3Z^{12}-c^2Z^{18})/(cZ^9+X^3Z^3)^3=y^3(x^9+c^3+cx^3-c^2)/(c+x^3)^3
\end{aligned}$$

$= y^3[(x^3+x^2+c)^3 - x^6 + cx^3 - c^2]/(x^3+c)^3 = y^3[(x^3+x^2+c)^3 - (x^3+c)^2]/(x^3+c)^3$

$= [y^9 - y^3(x^3+c)^2]/(x^3+c)^3$ from the curve equation**.**

This is identical with **(10)** under the condition $a = 1$**.**

From **(13)** and **(14)**, it is clear that in ML-coordinates, the sum $P + Q = (X_3, Y_3, Z_3, T_3)$ of given two points $P = (X_1, Y_1, 1, 1)$ and $Q = (X_2, Y_2, Z_2, T_2)$ is obtained by:

$$Z_3 = (X_2 - X_1T_2)Z_2,\ T_3 = {Z_3}^2,$$
$$X_3 = (Y_2 - Y_1{Z_2}^3)^2 - (X_2 - X_1T_2)^3 - T_3 + X_1T_3, \qquad \textbf{(15)}$$
$$Y_3 = (X_1T_3 - X_3)(Y_2 - Y_1{Z_2}^3) - Y_1{Z_2}^3(X_2 - X_1T_2)^3$$

and tripling [3]$(X, Y, Z, T) = (X_3, Y_3, Z_3, T_3)$ of a given a point (X, Y, Z, T) by:

$$Z_3 = cZ^9 + X^3Z^3,\ T_3 = {Z_3}^2,\ X_3 = [X^3 + T^3(c^2 + c^3)^{\frac{1}{3}}]^3 - cZ^9Z_3,\ Y_3 = Y^3(X_3 - cZ_3Z^9) \qquad \textbf{(16)}$$

in ML- projective coordinates**.**

Using **(15)** and **(16)** we obtain following algorithms for point addition on the curve in ML- coordinates.

- **Addition** $P + Q = (X_3, Y_3, Z_3, T_3)$ of $P = (X_1, Y_1, 1, 1)$ and $Q = (X_2, Y_2, Z_2, T_2)$

$O_1 = Z_2^3$	**C**
$O_2 = X_1T_2$	**M**
$O_3 = X_2 - O_2$	**A**
$O_4 = Y_1O_1$	**M**
$O_5 = Y_2 - O_4$	**A**
$O_6 = O_3Z_2 = Z_3$	**M**
$O_7 = Z_3^2 = T_3$	**M**
$O_8 = O_3^3$	**C**
$O_9 = O_5^2$	**M**
$O_{10} = X_1T_3$	**M**
$O_{11} = O_9 - O_8 - T_3 + O_{10} = X_3$	**3A**
$O_{12} = O_4O_8$	**M**
$O_{13} = O_{10} - X_3$	**A**
$O_{14} = O_{13}O_5$	**M**

$O_{15} = O_{14} - O_{12} = Y_3$	**A**
Total cost	**8M+2C**

Table 8. New mixed point addition algorithm on Weierstrass curve using ML- coordinates

- **Tripling** $[3](X, Y, Z, T) = (X_3, Y_3, Z_3, T_3)$

$O_1 = X^3$	**C**
$O_2 = Z^3$	**C**
$O_3 = O_2^3$	**C**
$O_4 = cO_3$	**M**
$O_5 = O_1 O_2$	**M**
$O_6 = O_4 + O_5 = Z_3$	**A**
$O_7 = O_4 Z_3$	**M**
$O_8 = T^3$	**C**
$O_9 = O_8 (c^2 + c^3)^{\frac{1}{3}}$	**M**
$O_{10} = O_1 + O_9$	**A**
$O_{11} = O_{10}^3$	**C**
$O_{12} = O_{11} - O_7 = X_3$	**A**
$O_{13} = Y^3$	**C**
$O_{14} = X_3 - O_7$	**A**
$O_{15} = O_{13} O_{14} = Y_3$	**M**
$O_{16} = O_6^2 = T_3$	**M**
Total cost	**6M+6C**

Table 6. New point doubling algorithm using ML-coordinates

Note 4. In the above point tripling algorithm, $(c^2 + c^3)^{\frac{1}{3}}$ is a constant which can be precomputed from the curve equation and both of the new tripling algorithms from **(14)** and **(16)** have two multiplications with constant as a multiplier.

So, in practice our tripling algorithms offer more speedup than Negre's algorithm which has only one multiplication by the constant c **,** though total numbers of multiplications are the same in both algorithms.

If c is sparse, $(c^2 + c^3)^{\frac{1}{3}}$ also is sparse and we can obtain a point tripling in Jacobian coordinates at the cost of **4M+5C** by using formula **(14)**, which is cheap by a multiplication than the cost of Negre's algorithm for sparse c (cf. [11]).

Algorithm	Coordinates System	Tripling	Addition
N. P. Smart et al. [2]	**Jacobian**	**7M+4C** (1)	**10M+2C** (0)
C. Negre [11]	**Jacobian**	**6M+5C** (1)	**10M+2C** (0)
Proposed	**Jacobian**	**6M+5C** (2)	**9M+2C** (0)
Proposed	**ML**	**6M+6C** (2)	**8M+2C** (0)

Table 10. Comparing costs of algorithms for arithmetic on ordinary Weierstrass curves

5. Conclusion

We have proposed new formulae and algorithms for arithmetic on ordinary elliptic curve with a point of order 3 over finite field of characteristic three, by which the cost of a point multiplication on the curves decreases about 10~20% .

Omitting the details, we mention that point multiplication based on Hessian form and addition-doubling ladder is more efficient than one based on Weierstrass form and addition-tripling ladder in characteristic three.

In conclusion, we can say that ternary elliptic curves are another alternative to existing technology for elliptic curve cryptosystems .

6. References

[1] N. P. Smart. The Hessian form of an elliptic curve. In Cryptographic Hardware and Embedded Systems – CHES 2002, Springer LNCS 2162, 118-125, 2001.

[2] N. P. Smart, E. J. Westwood. Point multiplication on ordinary elliptic curves over fields of characteristic three. Applicable Algebra in Engineering, Communication and Computing – AAECC, 13, 485-497, 2003.

[3] D. Page and N. P. Smart. Hardware implementation of finite fields of characteristic three. In 4th Workshop on Cryptographic Hardware and Embedded Systems(CHES), LNCS 2523, 529-539, Springer-Verlag 2002.

[4] K. Harrison, D. Page and N. P. Smart. Software implementation of finite fields of characteristic three, for use in pairing based cryptosystems. In LMS Journal of Computation and Mathematics, 5(1), 181-193, London Mathematical Society, 2002.

[5] R. Granger, D. Page and M. Stam. Hardware and software normal basis arithmetic for pairing based cryptography in characteristic three. Cryptology ePrint Archive, Report 157/2004, 2004. http://eprint.iacr.org/2004/157.

[6] P. S. L. M. Barreto. A note on efficient computation of cube roots in characteristic 3. Cryptology ePrint Archive, Report 035/2004, 2004. http://eprint.iarc.org/2004/305.

[7] I. F. Blake, G. Seroussi and N. P. Smart. Elliptic Curves in Cryptography, vol. 265 of London Mathematical Lecture Note Series, Cambridge University Press, 1999.

[8] I. F. Blake, G. Seroussi and N. P. Smart. Advances in Elliptic Curve Cryptography. vol. 317 of London Mathematical Lecture Note Series, Cambridge University Press, 2005.

[9] G. Bertoni, J. Guajardo, S. Kumar, G. Orlando, C. Paar and T. Wollinger. Efficient $GF(p^m)$ arithmetic architectures for cryptographic applications. In Topics In Cryptology – CT RSA 2003 LNCS 2612, 158-175. Springer-Verlag 2003.

[10] M. Barbosa, A. Moss and D. Page. Compiler assisted elliptic curve cryptography. Cryptology ePrint Archive, Report 053/2007, 2007. http://eprint.iacr.org/2007/081.

[11] C. Negre. Scalar multiplication on elliptic curves defined over fields of small odd characteristic, INDOCRYPT 2005, LNCS 3797, 389-402, 2006.

[12] O. Ahmadi, D. Hankerson, and A. Menezes. Software implementation of arithmetic in F_{3^m}. WAIFI 2007, to appear.