Fast Point Multiplication Formulae on Elliptic Curves of Weierstrass Form

Rongquan Feng[1], Zilong Wang[1], Hongfeng Wu[2]
1. School of Mathematical Sciences, Peking University, Beijing 100871, China
2. Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100080
fengrq@math.pku.edu.cn,wzlmath@gmail.com,whfmath@gmail.com

Abstract

In this paper, we presented fast point multiplication formulae for two different families elliptic curve of Weierstrass form $y^2 = x^3 + ax^2 + bx$ and $y^2 = x^3 + ax^2 + 2atx + at^2$. The costs of doubling and tripling formulae are $5S+2M+3C$ and $6S+6M+4C$ respectively, even $5S+2M$ and $6S + 6M$ with the parameter of the curve suitably chosen.

Keywords: Elliptic curve, point multiplication, doubling, tripling.

1 Introduction

Efficient elliptic curve arithmetic is crucial for cryptosystems based on elliptic curves. Such cryptosystems often require computing kP for a given integer k and a curve point P. For example, if k is a secret key and P is another user's public key then kP is a Diffie-Hellman secret shared between the two users. So a main operation for elliptic curve cryptosystems is the point multiplication: $Q = kP$, where the multiplier k is generally a secret (or private) parameter. Many methods to speed up this operation have been actively studied. See [1] for the compared result for all kinds of elliptic curves. In particular, Doche, Icart and Kohel introduced the fastest doubling and tripling in two different families of curves [5]. They focus on two families curves $E_2 : y^2 = x^3 + ux^2 + 16ux$ and $E_3 : y^2 = x^3 + 3u(x+1)^2$. For the curves E_2, The doubling formula costs is $4S + 3M + 2C$, and if u is chosen such that a multiplication by u is negligible, the costs for doubling drop to $4S + 3M$, where S, M and C denote the costs of one squaring, one multiplication and one multiplication by a constant respectively. For the curves E_3, The tripling formula costs is $6S + 6M + 2C$, and if u is chosen

such that a multiplication by u is negligible, the costs for doubling drop to $6S + 6M$.

In this paper, we consider point multiplication formulae for two different families of Weierstrass form elliptic curves, $E^L_{a,t}$ form elliptic curve $y^2 = x^3 + ax^2 + 2atx + at^2$ and $E^S_{a,b}$ form elliptic curve $y^2 = x^3 + ax^2 + bx$. New doubling formula for $E^S_{a,b}$ costs $5S + 2M + 2C$. If constant multiplications is negligible, costs drop to $5S + 2M$. We get the fast tripling formulae when curve satisfy $E^L_{a,t}$ form. The costs of tripling formulae is $6S + 6M + 4C$, even $6S + 6M$ when the parameter of the curve suitably chosen.

This paper is organized as follows. We shower faster tripling formulae in Section 3, introduce new doubling formulae in Section 4, and draw our conclusions in Section 5.

2 Elliptic Curves with Weierstrass Form

Definition 1 *An elliptic curve E over a field K is defined by an equation*

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

where $a_1, a_2, a_3, a_4, a_5, a_6 \in K$,and $\triangle \neq 0$, where $\triangle$ is the discriminant of E.

The set $E(K)$ of rational points on an elliptic curve E defined over a field K is an abelian group, where the operation is defined by the well-known law of chord and tangent, and the identity element is the special point $\mathcal{O}$ called point at infinity.
In practice, the Weierstrass equation (1) can be greatly simplified by applying admissible changes of variables. If the characteristic of K is not equal to 2 and 3, we can define $\eta \leftarrow y + (a_1x + a_3)/2$, then (1) rewrites

$$E: \ \eta^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4} \tag{2}$$

where $b_2 = a_1^2 + 4a_2, b_4 = a_1a_3 + 2a_4, b_6 = a_3^2 + 4a_6$. In this paper we focus on the elliptic curves of the following form.

$$E: \ y^2 = x^3 + a_2x^2 + a_4x + a_6 \tag{3}$$

In the following, we will use I, S M to denote the costs of one inversion, one squaring and one multiplication respectively. The symbols C stands for the costs of multiplication by a constant. We shall always leave out the costs of field additions.

We start by recalling the explicit group law on elliptic curves. Let $P = (x_1, y_1)$, $Q = (x_2, y_2)$, $P + Q = (x_3, y_3)$. let

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{if } P \neq Q, \\ \dfrac{3x_1^2 + 2a_2x_1 + a_4}{2y_1}, & \text{if } P = Q. \end{cases}$$

then $x_3 = \lambda^2 - x_1 - x_2 - a_2$, $y_3 = \lambda(x_1 - x_3) - y_1$.
Setting $P = (x_1, y_1)$, $2P = (x_3, y_3)$, we obtain the following proposition immediately by a few algebraic computation

Proposition 1

$$\begin{cases} x_3 &= \dfrac{x_1^4 - 2a_4x_1^2 - 8a_6x_1 - 4a_2a_6 + a_4^2}{4y_1^2}, \\ y_3 &= \dfrac{2x_1^6 + 4a_2x_1^5 + 10a_4x_1^4 + 4a_6x_1^3 + (40a_2a_6 - 10a_4^2)x_1^2 + bx_1 + d}{16y_1^3}. \end{cases}$$

where $b = 16a_2^2a_6 - 4a_2a_4^2 - 8a_4a_6$, $d = 2a_4(4a_2a_6 - a_4^2) - 16a_6^2$.

3 Two Families of Elliptic Curves

In the following sections, we suppose $p > 3$ be a prime and K be the finite field of characteristic p. For the elliptic curve $E/K: y^2 = x^3 + a_2x^2 + a_4x + a_6$, if $a_4^2 = 4a_2a_6$, then $\dfrac{a_4}{2a_2} = \dfrac{2a_6}{a_4}$, so there exist $t \in K$, $t \neq 0$ such that $a_4 = 2ta_2$, $a_6 = t^2a_2$. We rewrite the equation

$$E/K: y^2 = x^3 + ax^2 + 2tax + t^2a, \ a, t \in K.$$

Definition 2 *An elliptic curve defined by*

$$y^2 = x^3 + ax^2 + 2atx + at^2$$

is called $E_{a,t}^L$ *form elliptic curve. where* $a, t \in K$ *and* $a(16a + 27t^2 - 72at^3) \neq 0$. *A simple* $E_{a,t}^L$ *form elliptic curve is a* $E_{a,t}^L$ *form elliptic curve with parameter* $t = 1$, *in other word, it is given by the equation*

$$E_{a,1}^L: y^2 = x^3 + ax^2 + 2ax + a$$

where $a(27 - 56a) \neq 0$.

Any $E^L_{a,t}$ form elliptic curve given by $y^2 = x^3 + ax^2 + 2atx + at^2$ is birationally equivalent to short Weierstrass form elliptic curve $E_{a,b}: y^2 = x^3 + \left(2at - \frac{a^2}{3}\right)x + \left(at^2 - \frac{2a^2t}{3} + \frac{2a^3}{27}\right)$.

Definition 3 *An elliptic curve defined by*

$$y^2 = x^3 + ax^2 + bx = x^3 + ax^2 + atx$$

is called $E^S_{a,b}$ form or $E^S_{a,t}$ form elliptic curve, where $a, b, t \in K$, $b(a^2 - 4b) = a^2t(a - 4t) \neq 0$.

Then $\triangle(E^S_{a,t}) = 16(a^4t^2 - 4a^3t^3)$, $j = 16^2\frac{(a^2 - 3b)^3}{a^2b^2 - 4b^3}$. By applying admissible changes of variables, $E^S_{a,t}$ can be put in the form $E: y^2 = x^3 - \frac{16a^2 - 48b}{48}x + \frac{64a^3 - 288ab}{864}$.
To $E^S_{a,t}$, if t is a quadric element, say that $t = r^2$, $r \in K$, then it can be transformed to

$$\left(\frac{y}{r^3}\right)^2 = \left(\frac{x}{r^2}\right)^3 + \frac{a}{r^2}\left(\frac{x}{r^2}\right)^2 + \frac{a}{r^2}\left(\frac{x}{r^2}\right).$$

Therefore, if b/a be a quadric element, then $E^S_{a,t}$ form elliptic curves can be transformed to $E^S_{a,a}$ form curves. Since the probability of $\frac{b}{a} \in K$ being a quadric element for any finite field K is $1/2$, we can conclude that about half of all the $E^S_{a,t}$ form elliptic curves can be transformed to $E^S_{a,a}$ form. If b being a quartic element, then $E^S_{a,b}$ can be transformed to $E^S_{a,1}$ form curves. We can conclude that about quarter of all the $E^S_{a,b}$ form elliptic curves can be transformed to $E^S_{a,1}$ form elliptic curves.

4 Efficient Point Multiplication on $E^L_{a,t}$

4.1 Doubling and Addition

In this subsection, we show the doubling and addition formulae on elliptic curve of $E^L_{a,t}: y^2 = x^3 + ax^2 + 2atx + at^2$. In Jacobian coordinates, the elliptic curve $E^L_{a,t}$ has the form $E^L_{a,t}; Y^2 = X^3 + aX^2Z^2 + 2atXZ^4 + at^2Z^6$. Let $P = (X_1, Y_1, Z_1), 2P = (X_3, Y_3, Z_3)$, then

$$\begin{aligned} X_3 &= (3X_1^2 + 2aX_1Z_1^2 + 2atZ_1^4)^2 - 8X_1Y_1^2 - aZ_3^2, \\ Y_3 &= (3X_1^2 + 2aX_1Z_1^2 + 2atZ_1^4)(4X_1Y_1^2 - X_3) - 8Y_1^4, \\ Z_3 &= 2Y_1Z_1. \end{aligned}$$

let $P = (X_1, Y_1, Z_1)$, $Q = (X_2, Y_2, Z_2)$, $P + Q = (X_3, Y_3, Z_3)$ then

$$\begin{aligned} X_3 &= (Y_2 Z_1^3 - Y_1 Z_2^3)^2 - (X_2 Z_1^2 - X_1 Z_2^2)^2 (X_1 Z_2^2 + X_2 Z_1^2 + a Z_1^2 Z_2^2), \\ Y_3 &= (Y_2 Z_1^3 - Y_1 Z_2^3)(X_1 Z_2^2 (X_2 Z_1^2 - X_1 Z_2^2)^2 - X_3) - Y_1 Z_2^3 (X_2 Z_1^2 - X_1 Z_2^2)^3, \\ Z_3 &= Z_1 Z_2 (X_2 Z_1^2 - X_1 Z_2^2). \end{aligned}$$

Therefore, we have the following efficient algorithms.

Doubling. Here are explicit formulae to compute $2(X_1, Y_1, Z_1) = (X_3, Y_3, Z_3)$.

$$\begin{aligned} A &= 3X_1^2,\ B = Z_1^2,\ W = 2aB(X_1 + tB), \\ D &= A + W,\ E = Y_1^2,\ F = D^2,\ G = 2((X_1 + E)^2 - A - F), \\ Z_3 &= (Y_1 + Z_1)^2 - D - B, \\ X_3 &= F - 2G - aZ_3^2,\ Y_3 = D(G - X_3) - 8F. \end{aligned}$$

These formulae cost $7S + 2M + 3C$. The $3C$ are multiplications by a and t.

Mixed Doubling. The following formulae, given $P = (X_1, Y_1, 1)$ compute the doubling $2P = (X_3, Y_3, Z_3)$.

$$\begin{aligned} A &= X_1^2,\ B = 2a(X_1 + t),\ D = 3A + B, \\ E &= Y_1^2,\ F = D^2,\ G = 2((X_1 + E)^2 - A - F), \\ X_3 &= F - 2G - 4aE,\ Y_3 = D(G - X_3) - 8F,\ Z_3 = 2Y_1 \end{aligned}$$

The formulae cost $5S + M + 2C$. The $2C$ are both multiplications by a.

Addition The following formulae, given $P = (X_1, Y_1, Z_1, Z_1^2)$ and $Q = (X_2, Y_2, Z_2, Z_2^2)$, compute the sum $P + Q = (X_3, Y_3, Z_3, Z_3^2)$.

$$\begin{aligned} M &= Z_1^2,\ N = Z_2^2,\ R = Z_1 M,\ S = Z_2 N,\ A = X_2 M - X_1 N, \\ B &= Y_2 R - Y_1 S,\ W = A^2,\ D = (A + Z_2)^2 - W - N,\ H = D^2, \\ E &= 8HX_1,\ Z_3 = (Z_1 + D)^2 - M - H,\ F = Z_3^2, \\ X_3 &= 16(B^2 - A \cdot W) - E - a \cdot F,\ Y_3 = 2B(E - 2X_3) - Y_1 \cdot D \cdot E. \end{aligned}$$

The formulae cost $6S + 11M + C$. The C is multiplications by a.

Mixed-Addition let $P = (X_1, Y_1, Z_1, Z_1^2)$, $Q = (X_2, Y_2, 1, 1^2)$, $P + Q = (X_3, Y_3, Z_3, Z_3^2)$, then the operations can be organized as follows.

$$\begin{aligned} V &= Z_1^2,\ A = X_2 M,\ R = Z_1 M,\ B = Y_2 \cdot R, \\ D &= X_1 - A,\ E = 2(Y_1 - B),\ G = D^2,\ H = 4D \cdot G, \\ M &= 4A \cdot G,\ Z_3 = (Z_1 + D)^2 - V - G,\ F = Z_3^2 \\ X_3 &= E^2 - H - a_2 \cdot F - 2M,\ Y_3 = E \cdot (M - X_3) - B \cdot H. \end{aligned}$$

The formulae cost $4S + 7M + C$. The C is multiplications by a.

Affine-Jacobian Addition Given $P = (X_1, Y_1, 1)$ and $Q = (X_2, Y_2, 1)$, The following formulae compute the sum $P + Q = (X_3, Y_3, Z_3)$.

$$\begin{aligned} A &= X_2 - X_1,\ B = 2(Y_2 - Y_1),\ D = A^2,\ E = 4D, \\ F &= A \cdot E,\ G = X_2 \cdot E,\ X_3 = B^2 - 2G - F - a \cdot E, \\ Y_3 &= B \cdot (G - X_3) - 2Y_2 \cdot F,\ Z_3 = 2A. \end{aligned}$$

The formulae cost $2S + 4M + C$. The C is multiplications by a.

4.2 Tripling Formula on $E^L_{a,t}$

In this subsection, we show the tripling formulae on elliptic curve of $E^L_{a,t}$: $y^2 = x^3 + ax^2 + 2atx + at^2$. In Jacobian coordinates, the elliptic curve $E^L_{a,t}$ has the form $E^L_{a,t}; Y^2 = X^3 + aX^2Z^2 + 2atXZ^4 + at^2Z^6$. Let $P = (X_1, Y_1, Z_1), 3P = (X_3, Y_3, Z_3)$. Then

$$\begin{aligned} X_3 &= 8Y_1^2(8Y_1^4 - BE) + X_1E^2, \\ Y_3 &= Y_1[4(BE - 8Y_1^4)(16Y_1^4 - BE) - E^3], \\ Z_3 &= Z_1E. \end{aligned}$$

where

$$\begin{aligned} B &= 3X_1^2 + 2a_2X_1Z_1^2 + a_4Z_1^4, \\ E &= 12X_1Y_1^2 + 4a_2Y_1^2Z_1^2 - B^2\ . \end{aligned}$$

Theorem 1 *Let $P = (X_1, Y_1, Z_1)$, $3P = (X_3, Y_3, Z_3)$, defining*

$$\begin{aligned} U &= Y_1\left(Y_1^2 - aX_1^2Z1^2 - 6atX_1Z_1^4 - 9at^2Z_1^6\right), \\ V &= -aX_1^2Z_1^2\left(\left(\frac{4a}{3} - 9t\right)X_1^2Z_1^2 - \left(Y_1^2 + \frac{a}{3}X_1^2Z_1^2 + 2atX_1Z_1^4 + 3at^2Z_1^6\right)\right)^2, \\ W &= 3Y_1^2 + aZ_1^2(X_1^2 + 6tX_1Z_1^2 + 9t^2Z_1^4). \end{aligned}$$

then

$$\begin{cases} X_3 &= U^2 + V, \\ Y_3 &= U(X_3 - 4V), \\ Z_3 &= X_1Z_1W. \end{cases}$$

Proof:

Since

$$\begin{aligned}
E &= 12X_1Y_1^2 + 4aY_1Y_1^2Z_1^2 - B^2 \\
&= 12X_1^4 + 12aX_1^3Z_1^2 + 24atX_1^2Z_1^4 + 12at^6X_1Z_1^6 + 4aX_1^3Z_1^2 + 4a^2X_1^2Z_1^4 \\
&\quad +8a^2tX_1Z_1^6 + 4a^2t^2Z_1x - 9X_1^4 - 4a^2X_1^2Z_1^4 - 4a^2t^2Z_1^8 - 12aX_1^3Z_1^2 \\
&\quad -12atX_1^2Z_1^4 - 8a^2tX_1Z_1^6 \\
&= 3X_1(X_1^3 + aX_1^2Z_1^2 + 2atX_1Z_1^4 + at^2Z_1^6) + aX_1^3Z_1^2 + 6atX_1^2Z_1^4 \\
&\quad +9at^2X_1Z_1^6 \\
&= 3X_1Y_1^2 + aX_1Z_1^2(X_1 + 3tZ_1^2)^2
\end{aligned}$$

Therefore $X_1Z_1W = Z_1E = Z_3$. We compute $U^2 + V$ and X_3.

$$\begin{aligned}
&U^2 + V \\
= \ & X^9 - 24atX^7Z^4 - 96at^2X^6Z^6 - 96a^2t^2X^5Z^8 - 48a^2t^3X^4Z^{10} \\
&+48a^2t^4X^3Z^{12} - 16a^2tX^6Z^6 + 64a^3t^3X^3Z^{12} + 192a^3t^4X^2Z^{14} \\
&+192a^3t^5XZ^{16} + 64a^3t^6Z^{18},
\end{aligned}$$

and

$$\begin{aligned}
&X^3 \\
= \ & 8Y_1^2(8Y_1^4 - BE) + X_1E^2 \\
= \ & X^9 - 24atX^7Z^4 - 96at^2X^6Z^6 - 96a^2t^2X^5Z^8 - 48a^2t^3X^4Z^{10} \\
&+48a^2t^4X^3Z^{12} - 16a^2tX^6Z^6 + 64a^3t^3X^3Z^{12} + 192a^3t^4X^2Z^{14} \\
&+192a^3t^5XZ^{16} + 64a^3t^6Z^{18}
\end{aligned}$$

So $X_3 = U^2 + V$. We compute $U(X_3 - 4V)$ and Y_3.

$$\begin{aligned}
&U(X_3 - 4V \\
= \ & Y_1(44atX^{10}Z^4 - 1056a^2t^3X^7Z^{10} + 220at^2X^9Z^6 - 177a^2t^4X^6Z^{12} \\
&-2496a^3t^4X^5Z^{14} - 832a^3t^3X^6Z^{12} - 1920a^3t^5X^4Z^{16} - 320a^3t^6X^3Z^{18} \\
&-512a^4t^8Z^{24} + X^{12} - 1280a^4t^4X^4Z^{16} - 256a^4t^3X^5Z^{14} - 2560a^4t^5X^3Z^{18} \\
&-2816a^4t^6X^2Z^{20} - 1792a^4t^7X^7Z^{22} + 4aX_{11}Z^2),
\end{aligned}$$

and

$$\begin{aligned}
&Y^3 \\
= \ & Y_1[4(BE - 8Y_1^4)(16Y_1^4 - BE) - E^3] \\
= \ & Y_1(44atX^{10}Z^4 - 1056a^2t^3X^7Z^{10} + 220at^2X^9Z^6 - 177a^2t^4X^6Z^{12} \\
&-2496a^3t^4X^5Z^{14} - 832a^3t^3X^6Z^{12} - 1920a^3t^5X^4Z^{16} - 320a^3t^6X^3Z^{18} \\
&-512a^4t^8Z^{24} + X^{12} - 1280a^4t^4X^4Z^{16} - 256a^4t^3X^5Z^{14} - 2560a^4t^5X^3Z^{18} \\
&-2816a^4t^6X^2Z^{20} - 1792a^4t^7X^7Z^{22} + 4aX_{11}Z^2),
\end{aligned}$$

So $Y_3 = U(X_3 - 4V)$. The Theorem 1 follows.

From Theorem 1, we have the following formula,

$$X_3 = U^2 + V,\ Y_3 = U(X_3 - 4V),\ Z_3 = 3EJ.$$

where $A = Z_1^2,\ B = \frac{a}{3}A,\ D = 3tA,\ E = X_1Z_1,\ F = E^2,\ G = (X_1 + D)^2,$ $H = BG,\ J = Y_1^2 + H,\ M = 3H,\ R = \frac{a}{3}F,\ S = 9tF,\ U = Y_1(Y_1^2 - M),$ $V = 3R(12R - S - J)^2.$
The cost is $6S + 6M + 4C$. The $4C$ are multiplications by $a/3$, $a/3$, $3t$ and $9t$. It is the same as [5] when $t = 1$.

5 Efficient Point Multiplication on $E_{a,t}^S$

By the proposition 1, we have

Proposition 2 *let $P = (x_1, y_1) \in E_{a,t}^S$, then*

$$2P = \left(\left(\frac{x_1^2 - b}{2y_1} \right)^2,\ \frac{\left(x_1^2 - b\right)\left(x_1^4 + 2ax_1^3 + 6bx_1^2 + 2abx_1 + b^2\right)}{8y_1^3} \right).$$

Using López-Dahab coordinates, a point (x_1, y_1) in affine coordinates on elliptic curve E will be represented by (X_1, Y_1, Z_1), where $x_1 = X_1/Z_1$ and $y_1 = Y_1/Z_1^2$. In López-Dahab coordinates, the elliptic curve E has the form $E:\ Y^2 = X^3Z + aX^2Z^2 + bXZ^3$.

Doubling Formula Let $P = (X_1, Y_1, Z_1)$ and $2P = (X_3, Y_3, Z_3)$, then

$$\begin{aligned} X_3 &= (X_1^2 - bZ_1^2)^2, \\ Y_3 &= 2Y_1(X_1^2 - bZ_1^2)(X_1^4 + 2aX_1^3Z_1 + 6bX_1^2Z_1^2 + 2abX_1Z_1^3 + b^2Z_1^4), \\ Z_3 &= 4Y_1^2. \end{aligned}$$

For

$$\begin{aligned} & X_1^4 + 2aX_1^3Z_1 + 6bX_1^2Z_1^2 + 2abX_1Z_1^3 + b^2Z_1^4 \\ = \ & X_3 + 2a(Y_1^2 + (8t - a)X_1^2Z_1^2) \end{aligned}$$

we have the following algorithm.

$$\begin{aligned} X_3 &= (A - D)^2, \\ Y_3 &= F(X_3 + 2a(E + (8t - a)X_1^2 \cdot Z_1^2)), \\ Z_3 &= 4E. \end{aligned}$$

where $A = X_1^2,\ B = Z_1^2,\ D = bB = atZ_1^2,\ E = Y_1^2,\ F = 2Y_1(A - D) = (Y_1 + (A - D))^2 - Y_1^2 - X_3.$

The formulae cost $5S + 2M + 3C$. The $3C$ are multiplications by $b = ta$, a and $8t - a$.

Mixed Doubling. Given $P = (X_1, Y_1, 1)$ compute the doubling $2P = (X_3, Y_3, Z_3)$.

$$\begin{aligned} X_3 &= (A - at)^2, \\ Y_3 &= F(X_3 + 2a(E + (8t - a)A)), \\ Z_3 &= 4E. \end{aligned}$$

where $A = X_1^2$, $E = Y_1^2$, $F = (Y_1 + (A - at))^2 - Y_1^2 - X_3$.
The formulae cost $4S + M + 2C$. The $2C$ are multiplications by a and $8t - a$.

Addition Formula Let $P = (X_1, Y_1, Z_1)$, $Q = (X_2, Y_2, Z_2)$, $P + Q = (X_3, Y_3, Z_3)$, then

$$\begin{aligned} X_3 &= (Y_2Z_1^2 - Y_1Z_2^2)^2 - Z_1Z_2(X_1Z_2 + X_2Z_1)(X_2Z_1 - X_1Z_2)^2 - aZ_3, \\ Y_3 &= Z_1Z_2(X_2Z_1 - X_1Z_2)((Y_2Z_1^2 - Y_1Z_2^2)(X_1Z_1Z_2^2(X_2Z_1 - X_1Z_2)^2 - X_3) \\ &\quad -Y_1(X_2Z_1 - X_1Z_2)^3Z_1Z_2^3), \\ Z_3 &= (Z_1Z_2)^2(X_2Z_1 - X_1Z_2)^2. \end{aligned}$$

So we have the following algorithm

$$\begin{aligned} X_3 &= A^2 - D - X_2Z_1N - aZ_3, \\ Y_3 &= MA(D - X_3) - Y_1Z_2^2NB, \\ Z_3 &= M^2. \end{aligned}$$

where $A = Y_2Z_1^2 - Y_1Z_2^2$, $B = X_2Z_1 - X_1Z_2$, $M = Z_1Z_2 \cdot B$, $N = MB$, $D = X_1Z_2 \cdot N$, the cost is $4S + 13M + C$. If we use coordinates (X_1, Y_1, Z_1, Z_1^2) then the cost is $3S+13M+C$. By expand Y_3, we have the following algorithm

$$\begin{aligned} X_3 &= A^2 - D - X_2Z_1 \cdot N - aZ_3, \\ Y_3 &= MA(D - X_3) - Y_1Z_2^2 \cdot N^2, \\ Z_3 &= M^2. \end{aligned}$$

where $A = Y_2Z_1^2 - Y_1Z_2^2$, $B = X_2Z_1 - X_1Z_2$, $M = Z_1Z_2 \cdot B$, $N = MB$, $D = X_1Z_2 \cdot N$, the cost is $5S + 12M + C$, If we use the coordinates (X_1, Y_1, Z_1, Z_1^2) then the cost will drop to $4S + 12M + C$.

Mixed-Addition let $P = (X_1, Y_1, Z_1)$, $Q = (X_2, Y_2, 1)$, $P+Q = (X_3, Y_3, Z_3)$, then the operations can be organized as follows.

$$\begin{aligned} A &= Y_2Z_1^2 - Y_1,\ B = X_2Z_1 - X_1,\ M = Z_1 \cdot B,\ N = MB, \\ D &= X_1Z_2 \cdot N,\ X_3 = A^2 - D - X_2Z_1 \cdot N - aZ_3, \\ Y_3 &= MA(D - X_3) - Y_1Z_2^2 \cdot N^2,\ Z_3 = M^2. \end{aligned}$$

The formulae cost $4S + 9M + C$. The C is multiplications by a.

5.1 Conclusion

In this paper, we considered fast point multiplication formulae for two different families elliptic curve of Weierstrass form $y^2 = x^3 + ax^2 + bx$ and $y^2 = x^3 + ax^2 + 2atx + at^2$. The cost of doubling and tripling formulae are $5S + 2M + 3C$ and $6S + 6M + 4C$ respectively, even $5S + 2M$ and $6S + 6M$ with the parameter of the curve suitably chosen. We would expect further results in the future. For example, designing direct formulae for $2P + Q$ and $3P + Q$ would lead to further improvements. It is also an interesting to find fast quintupling formula for $E^L_{a,t}$ form elliptic curve.

References

[1] Daniel J. Bernstein, Tanja Lange, Faster addition and doubling on elliptic curves, in Asiacrypt 2007, LNCS 4833, 29-50, Springer-Verlag, 2007.

[2] M. Ciet, M. Joye, K. Lauter, and P.L. Montgomery, Trading inversions for multiplications in elliptic curve cryptography, Design, Codes and Cryptography 39(2), 189-206, 2006.

[3] H. Cohen, Atsuko Miyaji, Takatoshi Ono, Efficient elliptic curve exponentiation using mixed coordinates, ASIACRYPT'98, LNCS 1514, 51C65, Spriger-Verlag, 1998.

[4] V.S. Dimitrov, L. Imbert, and P.K. Mishra, Efficient and secure elliptic curve point multiplication using double-base chains. ASIACRYPT 2005, LNCS 3788, 59-78, Springer-Verlag, 2005.

[5] C. Doche,T. Icart and D.R. Kohel, Efficient Scalar Miltiplication by Isogeny Decompositions, PKC 2006, LNCS 3958, 191-206, Spriger-Verlag, 2006.

[6] J.H. Silverman. The Arithmetic of Elliptic Curves, GTM 106, Springer-Verlag, Berlin, 1986.