Studies on Tate Pairing computations on Edwards curves and A Strongly Unified Addition formula for Elliptic Curves

M. Tech. (CS) Dissertation

of

Anisur Rahaman Molla
Roll No: CS 0811

Supervised by

Professor Rana Barua
Stat-Math Unit

INDIAN STATISTICAL INSTITUTE
203, B. T. ROAD,
KOLKATA, INDIA - 700108.

Abstract

This report is a study of elliptic curves, group law on elliptic curves, scalar multiplications and then we focused on pairing computations on elliptic curves. Elliptic curves has wide application in Cryptography. This reports presents addition formula on elliptic curves in various coordinates and concentrates primarily on the Tate pairings on Edwards curves.

In this report, we propose a new addition formula on Weierstrass form elliptic curves in three coordinate systems namely, affine, Projective and Jacobian in chapter 2. The main advantage of our proposed addition algorithms is it is strongly unified. This means that the formulas work for all pairs of inputs except neutral element, simplifying protection against side-channel attacks. Then we extensively compute addition and doubling cost, compare with different forms of elliptic curves in different coordinate systems.

The Bilinear map or Pairing like Weil pairing or Tate pairing on elliptic curves has played a vital role in designing various cryptographic schemes. I have studied Tate pairing computations on Edwards curves. In chapter 3 we have summarized different proposed method of finding Tate pairing on Edwards curves. I do not have any contribution in this area.

Related Works: After we have obatined these formulas we noticed that Dier et. all [28] have obtained these earlier. However, such a detailed study was not carried out. Here, we provide much explicit results in three coordinates namely, affine, Projective, Jacobian. We also computed addition and doubling cost for each case and compared with usual addition rule.

Acknowledgment

First and foremost, with great pleasure, I express my heartfelt gratitude to my guide Professor Rana Barua, Stat-Math Unit, Indian Statistical Institute, Kolkata. He taught us three courses (Automata theory, General Cryptology and Advanced Cryptology) in our M.Tech. (CS) curriculum, which were mesmerizing beyond our expectation. Above all and the most needed, he provided me unflinching encouragement and support in various ways. I am highly indebted to him for providing me with the scope to work under his supervision and for his invaluable guidance.

I gratefully acknowledge Mr. Sumit Kumar Pandey for his patient help from the first stage. His substantial support and involvement made him a backbone of this work. He is really a cool and positive thinking person. His presence and rational attitude makes life more easy to tackle. I am also thankful to Butu Da (Mr. Subhabrata Samajder) for his crucial contribution and encouragement. He always helped me when I faced any problem with LaTeX at an early stage of this project. I would like to thank Mr. Sourav Sen Gupta and Mr. Santanu Sarkar, whom I could find beside me whenever I needed them.

I would like to extend my heartfelt gratitude to Dr. Avishek Adhikari for his help and encouragement during the project. I also sincerely thank all my class-mates, friends and well wishers who helped me directly or indirectly all throughout my entire M.Tech course.

Last but not the least, I take this opportunity to express my love and respect for my family, who always makes me feel that I am under a safe roof in this world.

Contents

Chapter 1

Elliptic Curve Cryptography

1.1 Introduction

Elliptic Curve Cryptography (ECC) was introduced by Victor Miller [13] and Neal Koblitz [11] in 1985. ECC proposed as an alternative to established public-key systems such as DSA and RSA.

Elliptic curve cryptography offers two major benefits over RSA namely; it has more security per bit and a suitable key size for hardware and modern communication. Thus, this results to smaller key certificates, lower power requirements and smaller hardware processors. At present, there are only three classes of public-key cryptosystems that are considered to be both secure and efficient. They are classified below according to the mathematical problem on which they are based. The systems are:

1. The integer factorization systems (of which RSA is the best known example),
2. The discrete logarithm systems,
3. The elliptic curve discrete logarithm systems (also known as elliptic curve cryptosystems).

The main attraction of elliptic curve cryptography (ECC) over competing technologies such as RSA and DSA is that the best algorithm known for solving the underlying hard mathematical problem in ECC, the elliptic curve discrete logarithm problem (ECDLP) takes fully exponential time. On the other hand, the best algorithms known for solving the underlying hard mathematical problem in RSA and DSA take sub-exponential time. This means that significantly smaller parameters can be used in ECC than in other systems such as RSA and DSA, but with equivalent levels of security. A typical example of the size in bits of the keys used in different public-key systems, with a comparable level of security (against known attacks), is that a 163-bit ECC key is equivalent to RSA and DSA with a modulus of 1024 bits. Due to lack of a sub-exponential attack on ECC offers potential reductions in processing power, storage space, bandwidth and electrical power. These advantages are specially important in applications on constrained devices such as smart cards, pagers, and cellular phones.

Another advantage that makes elliptic curves more attractive is the possibility of optimizing the arithmetic operations in the underlying field. An extensive amount of research has been done and being done to efficiently compute and accelerate and secure the group law.

1.2 Elliptic curves in Weierstrass form

Definition 1.2.1. *An elliptic curve E over a field K in Weierstrass form is defined by an equation*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_i \in K$ for $i \in \{1, 2, 3, 4, 5, 6\}$. The discriminant Δ of the curve E is defined as follows:

$$\begin{aligned}
\Delta &= -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6 \\
d_2 &= a_1^2 + 4a_2 \\
d_4 &= 2a_4 + a_1a_3 \\
d_6 &= a_3^2 + 4a_6 \\
d_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2
\end{aligned}$$

If L is any extension field of K, then the set of L-rational points on E is

$$E(L) = \{(x, y) \in L \times L : y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0\} \cup \{\mathcal{O}\}$$

where $\mathcal{O}$ is the point at infinity. The condition $\Delta \neq 0$ ensures that the elliptic curve is non-singular.

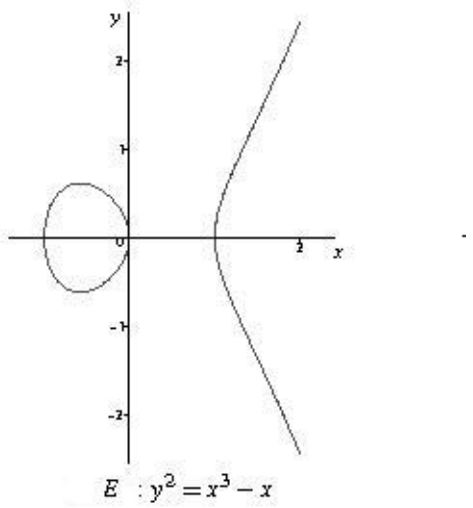

Figure 1.1: Elliptic curves over R.

1.3 Simplified Weierstrass Equations

Definition 1.3.1. *Two elliptic curves E_1 and E_2 defined over K in Weierstrass form are said to be isomorphic over K if there exist $u, r, s, t \in K, u \neq 0$, such that the change of variables*

$$(x, y) \mapsto (u^2x + r, u^3y + u^2sx + t)$$

transforms equation E_1 into equation E_2. This transformation is called an admissible change of variables.

A Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

defined over K can be simplified considerably by applying admissible changes of variables. The simplified equations will be used throughout the remainder of this book. We consider separately the cases where the underlying field K has characteristic different from 2 and 3, or has characteristic equal to 2 or 3.

- **Case 1:** $\text{Char}(K) \neq 2, 3$. Then the admissible change of variables

  $$(x, y) \mapsto \left(\frac{x - 3a_1^2 - 12a_2}{36}, \frac{y - 3a_1x}{216} - \frac{a_1^3 + 4a_1a_2 - 12a_3}{24}\right)$$

  transforms E to the curve

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

  where $a, b \in K$. The discriminant of this curve is $\Delta = -16(4a^3 + 27b^2)$.

- **Case 2:** $\text{Char}(K) = 2$. Then there are two subcases to consider.

  Subcase(I): If $a_1 \neq 0$, then the admissible change of variables

  $$(x, y) \mapsto \left(\frac{a_1^3x + a_3}{a_1}, \frac{a_1^6y + a_1^2a_4 + a_3^2}{a_1^3} - \frac{a_1^3 + 4a_1a_2 - 12a_3}{24}\right)$$

  transforms E to the curve

  $$y^2 + xy = x^3 + ax^2 + b$$

  where $a, b \in K$. Such a curve is said to be *non-supersingular* (cf. Definition 1.3) and has discriminant $\Delta = b$.

  Subcase(II): If $a_1 = 0$, then the admissible change of variables

  $$(x, y) \mapsto (x + a_2, y)$$

  transforms E to the curve

  $$y^2 + cy = x^3 + ax + b$$

  where $a, b, c \in K$. Such a curve is said to be *supersingular* (cf. Definition 1.3) and has discriminant $\Delta = c^4$.

- **Case 3:** $\text{Char}(K) = 3$. Then there are two subcases to consider.

  Subcase(I): If $a_1^2 \neq -a_2$, then the admissible change of variables

  $$(x, y) \mapsto \left(x + \frac{d_4}{d_2}, y + a_1x + a_1\frac{d_4}{d_2} + a_3\right),$$

  where $d_2 = a_1^2 + a_2$ and $d_4 = a_4 - a_1a_3$, transforms E to the curve

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

where $a, b \in K$. Such a curve is said to be *non-supersingular* and has discriminant $\Delta = -a^3 b$.

Subcase(II): If $a_1^2 = -a_2$, then the admissible change of variables

$$(x, y) \mapsto (x, y + a_1 x + a_3)$$

transforms E to the curve

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

where $a, b \neq K$. Such a curve is said to be *supersingular* and has discriminant $\Delta = -a^3$.

1.4 Group law- Geometric Concepts

Let E be an elliptic curve defined over the field K. There is a chord-and-tangent method for adding two points in $E(K)$ to give a third point in $E(K)$. Together with this addition operation, the set of points $E(K)$ forms an Abelian group with $\mathcal{O}$ as its identity element. This group is used in the construction of elliptic curve cryptographic systems.

The addition rule is best explained geometrically. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two distinct points on an elliptic curve E. Then the sum R, of P and Q, is defined as follows. First draw a line through P and Q; this line intersects the elliptic curve at a third point, as degree of this curve is 3. Then R is the reflection of this point about the x-axis. This is depicted in Figure 1.2.

The double R, of P, is defined as follows. First draw the tangent line to the elliptic curve at P. This line intersects the elliptic curve at a second point. Then R is the reflection of this point about the x-axis. This is depicted in Figure 1.2.

Algebraic formulas for the group law can be derived from the geometric description. These formulas are presented latter for elliptic curves E of the simplified Weierstrass form in affine coordinates, projective coordinates and Jacobian coordinates for different characteristics of the underlying field K. And there we provide corresponding unified or rather strongly unified addition formula for each coordinate system.

1.5 Group order and Supersingular curves

Let E be an elliptic curve defined over $\mathbb{F}_q$. The number of points in $E(\mathbb{F}_q)$, denoted by $\#E(\mathbb{F}_q)$ and is called the order of E over $\mathbb{F}_q$. Since the Weierstrass equation has at most two solutions for each $x \in \mathbb{F}_q$, we know that $\#E(\mathbb{F}_q) \in [1, 2q + 1]$. Hasses theorem provides tighter bounds for $\#E(\mathbb{F}_q)$.

Theorem 1.5.1. *(Hasse) Let E be an elliptic curve defined over $\mathbb{F}_q$. Then*

$$q + 1 - 2\sqrt{q} \leq \#\mathbb{F}_q \leq q + 1 + 2\sqrt{q}.$$

The interval $[q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}]$ is called the Hasse interval. An alternate formulation of Hasses theorem is the following: if E is defined over $\mathbb{F}_q$, then $\#\mathbb{F}_q = q + 1 - t$ where $|t| \leq 2\sqrt{q}$; t is called the trace of Frobenius.

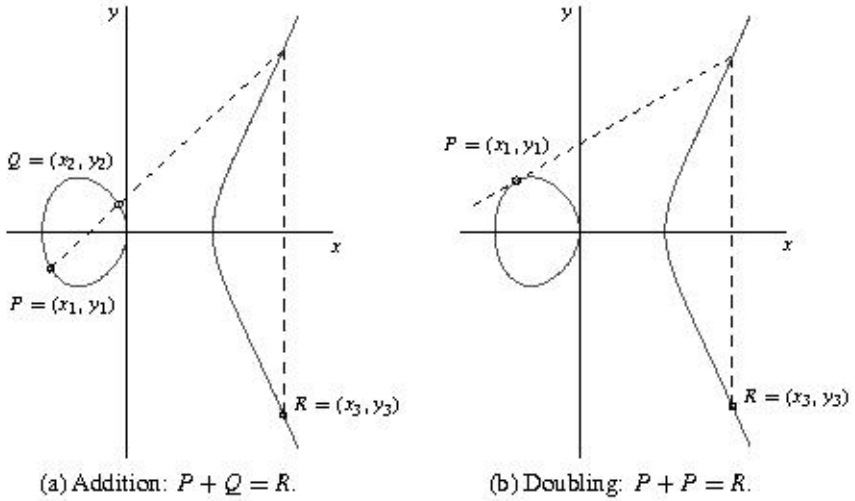

Figure 1.2: Geometric addition and doubling of elliptic curve points.

Definition 1.5.1. *Let p be the characteristic of $\mathbb{F}_q$. An elliptic curve E defined over $\mathbb{F}_q$ is supersingular if p divides t, where t is the trace of Frobenius. If p does not divide t, then E is non-supersingular.*

If E is an elliptic curve defined over $\mathbb{F}_q$, then E is also defined over any extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$. The group $E(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points is a subgroup of the group $E(\mathbb{F}_{q^n})$ of $\mathbb{F}_{q^n}$-rational points and hence $\#E(\mathbb{F}_q)$ divides $\#E(\mathbb{F}_{q^n})$.

Chapter 2

Unified Addition Formula on Elliptic Curves

After we have obatined these formulas we noticed that Dier et. all [28] have obtained these earlier. However, such a detailed study was not carried out.
The simplified formulae for the group law on elliptic curve take on different forms depending on the characteristic of the underlying field. We analyze the computational complexity of these formulae separately for different characteristic.

2.1 Elliptic Curves over Fields of Characteristic $p > 3$

2.1.1 Affine Coordinates

In Weierstrass form, Elliptic Curve over some field K of characteristic greater than three is defined as

$$E(K) = \{\mathcal{O}\} \cup \{(x, y) \in K \times K \mid y^2 = x^3 + ax + b\} \tag{2.1}$$

where $\{\mathcal{O}\}$ is the point at infinity and the negative element of $P = (x_1, y_1)$ is $-P = (x_1, -y_1)$. The addition operation on E is defined as follows:

Suppose $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are points on E. Then,

(I) $P + \mathcal{O} = \mathcal{O} + P = P$;

(II) $P + (-P) = (-P) + P = \mathcal{O}$;

(III) Otherwise, $P + Q = (x_3, y_3)$, where

$$x_3 \;=\; \lambda^2 \;-\; x_1 \;-\; x_2$$

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

and

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if} \quad P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1} & \text{if} \quad P = Q \end{cases} \tag{2.2}$$

We see that there are two different formula for doubling and addition of two different points P, Q, where $Q \neq \mathcal{O}, -P$ on Elliptic Curves. Now we want to combine these two formula to make it unified. For this we provide a single slope equation of λ as follows:

We have,

$$\begin{aligned} \lambda &= \frac{y_2 - y_1}{x_2 - x_1} \qquad [\text{ if } x_1 \neq x_2] \\ &= \frac{y_2^2 - y_1^2}{(x_2 - x_1)(y_2 + y_1)} \qquad [\text{ if } y_1 \neq -y_2] \\ &= \frac{x_2^3 - x_1^3 + a(x_2 - x_1)}{(x_2 - x_1)(y_2 + y_1)} \qquad [\text{ from 2.1}] \\ &= \frac{(x_2 - x_1)(x_2^2 + x_1x_2 + x_1^2 + a)}{(x_2 - x_1)(y_2 + y_1)} \\ &= \frac{x_2^2 + x_1x_2 + x_1^2 + a}{y_1 + y_2} \qquad [\text{ if } x_1 \neq x_2] \end{aligned} \tag{2.3}$$

If we consider points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ of the form $x_1 \neq x_2$ and $y_1 = -y_2$, then this λ will not work. In fact: for these points, from curve 2.1, we get $y_1^2 = x_1^3 + ax_1 + b$ and $y_1^2 = x_2^3 + ax_2 + b$.

Subtracting this two equation we get,

$$\begin{aligned} &x_2^3 - x_1^3 + a(x_2 - x_1) = 0 \\ \Rightarrow &(x_2 - x_1)(x_1^2 + x_2^2 + x_1x_2 + a) = 0 \end{aligned}$$

Since $(x_2 - x_1) \neq 0$, we get $x_1^2 + x_2^2 + x_1x_2 + a = 0$. Also $(y_1 + y_2) = 0$. So λ will not work in this case.

Now we want to modify λ such that it will work for all points on the elliptic curve 2.1 except identity and negative points.

Since,

$$\frac{a}{b} = \frac{c}{d} = \frac{a \pm c}{b \pm d} \qquad [\text{ if } (b \pm d) \neq 0]$$

So we from the above calculation we get,

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{x_2^2 + x_1x_2 + x_1^2 + a}{y_1 + y_2} = \frac{(x_2^2 + x_1(x_1 + x_2) + a) * (y_2 - y_1)}{(y_1 + y_2) * (x_2 - x_1)}$$

where, '$*$' is '$+$' if $(y_1 + y_2) \neq (x_1 - x_2)$, otherwise '$-$'.

Therefore the unified **Addition rule** is:

(I) $P + \mathcal{O} = \mathcal{O} + P = P$

(II) If $x_2 = x_1$ *and* $y_2 = -y_1$ i.e. $Q = -P$ then

$$P + Q = \mathcal{O}$$

(III) And for all other cases, $P + Q = (x_3, y_3)$,

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= \lambda(x_1 - x_3) - y_1 \\ \lambda &= \frac{(x_2^2 + x_1(x_1 + x_2) + a) * (y_2 - y_1)}{(y_1 + y_2) * (x_2 - x_1)} \end{aligned} \tag{2.4}$$

where, '$*$' is '$+$' if $(y_1 + y_2) \neq (x_1 - x_2)$, otherwise '$-$'.

Correctness of the Formula

We now show that this formula works for both doubling and addition as follows:

Case 1: $P = Q$. [Doubling]

Therefore, $x_1 = x_2$ and $y_1 = y_2$. Then putting these value in 2.4 and get

$$\lambda = \frac{3x_1^2 + a}{2y_1}$$

which is same as in the case of original doubling formula in 2.2.

Case 2: $P \neq Q$. [Addition]

- **Subcase 2.1** $x_1 \neq x_2$ and $y_1 = -y_2$

  Then from the curve 2.1, we get $y_1^2 = x_1^3 + ax_1 + b$ and $y_1^2 = x_2^3 + ax_2 + b$.

  Subtracting this two equation we get,

$$\begin{aligned} & x_2^3 - x_1^3 + a(x_2 - x_1) = 0 \\ \Rightarrow & (x_2 - x_1)(x_1^2 + x_2^2 + x_1x_2 + a) = 0 \end{aligned}$$

  Since $(x_2 - x_1) \neq 0$, we get $x_1^2 + x_2^2 + x_1x_2 + a = 0$. Again $(y_1 + y_2) = 0$.
  So from the equation 2.4, we get,

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

  which is as in the original case 2.2.

- **Subcase 2.2** $x_1 \neq x_2$ and $y_1 = y_2$

  Then $(y_2 - y_1) = 0$ and by the same calculation as above we get

$$x_1^2 + x_2^2 + x_1x_2 + a = 0$$

  Therefore the numerator of λ in 2.4 becomes 0 which is same as original case as in 2.2,

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

- **Subcase 2.3** $x_1 \neq x_2$ and $y_1 \neq \pm y_2$

  We have to show that

$$\lambda = \frac{(x_2^2 + x_1(x_1 + x_2) + a) * (y_2 - y_1)}{(y_1 + y_2) * (x_2 - x_1)} = \frac{y_2 - y_1}{x_2 - x_1} \qquad [* \text{ is defined as above }]$$

  Since, $x_1 \neq x_2$ and $y_1 \neq -y_2$, it follows that

$$\begin{aligned} & \frac{x_2^2 + x_1x_2 + x_1^2 + a}{y_1 + y_2} \\ &= \frac{(x_2 - x_1)(x_2^2 + x_1x_2 + x_1^2 + a)}{(x_2 - x_1)(y_2 + y_1)} \\ &= \frac{x_2^3 - x_1^3 + a(x_2 - x_1)}{(x_2 - x_1)(y_2 + y_1)} \\ &= \frac{(x_2^3 + ax_2 + b) - (x_1^3 + ax_1 + b)}{(x_2 - x_1)(y_2 + y_1)} \\ &= \frac{y_2^2 - y_1^2}{(x_2 - x_1)(y_2 + y_1)} \qquad [\text{ using the equation 2.1}] \\ &= \frac{y_2 - y_1}{x_2 - x_1} \end{aligned}$$

Hence we get the result,

$$\lambda = \frac{(x_2^2 + x_1(x_1 + x_2) + a) * (y_2 - y_1)}{(y_1 + y_2) * (x_2 - x_1)} = \frac{y_2 - y_1}{x_2 - x_1} \qquad \left[\text{Using the fact, } \frac{a}{b} = \frac{c}{d} = \frac{a \pm c}{b \pm d} \right]$$

- **Subcase 2.4** $x_1 = x_2$. Then we can say from the curve 2.1 that corresponding y-coordinate can take only two values viz. $y_1 = -y_2$ or $y_1 = y_2$[this is nothing but doubling].

  Therefore in this case we consider only $x_1 = x_2$ and $y_1 = -y_2$ and this is addition of P and $-P$. For this case we considered different addition formula [(II)] in the modified Addition rule.

2.1.2 Projective Coordinates

In cases where field inversions are significantly more expensive than multiplications, it is efficient to implement using Projective coordinates. A Projective point (X, Y, Z) on the curve satisfies the homogeneous Weierstrass equation

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

and when $Z \neq 0$, it corresponds to the affine point $(X/Z, Y/Z)$. The point at infinity $\mathcal{O}$ is represented by the triplet $(0, 1, 0)$, while the negative of $(X : Y : Z)$ is $(X : -Y : Z)$.

Let P_1, P_2 and P_3 be three points on the elliptic curves, where $P_1 = (X_1, Y_1, Z_1)$, $P_2 = (X_2, Y_2, Z_2)$ and $P_3 = (X_3, Y_3, Z_3)$. Now changing variables (x, y) to $(X/Z, Y/Z)$ and using the addition formula 2.4 for E in affine coordinates to obtain the following formulas for computing $(X_3 : Y_3 : Z_3)$ in Projective coordinates:

$$\begin{aligned}
X_3 = {} & Z_1Z_2(Y_2Z_1 + Y_1Z_2 + X_2Z_1 - X_1Z_2) \\
& [(X_1^2Z_2^2 + X_2Z_1(X_2Z_1 + X_1Z_2) + aZ_1^2Z_2^2 + (Y_2Z_1 - Y_1Z_2))^2 \\
& - Z_1Z_2(X_2Z_1 + X_1Z_2)(Y_2Z_1 + Y_1Z_2 + X_2Z_1 - X_1Z_2)^2]
\end{aligned}$$

$$\begin{aligned}
Y_3 = {} & (X_1^2Z_2^2 + X_2Z_1(X_2Z_1 + X_1Z_2) + aZ_1^2Z_2^2 + (Y_2Z_1 - Y_1Z_2)) \\
& [X_1Z_2Z_1Z_2(Y_2Z_1 + Y_1Z_2 + X_2Z_1 - X_1Z_2)^2 \\
& - (X_1^2Z_2^2 + X_2Z_1(X_2Z_1 + X_1Z_2) + aZ_1^2Z_2^2 + (Y_2Z_1 - Y_1Z_2))^2 \\
& + Z_1Z_2(X_2Z_1 + X_1Z_2)(Y_2Z_1 + Y_1Z_2 + X_2Z_1 - X_1Z_2)^2] \\
& - Y_1Z_2Z_1^2Z_2^2(Y_2Z_1 + Y_1Z_2 + X_2Z_1 - X_1Z_2)^3
\end{aligned}$$

$$Z_3 = (Z_1Z_2(Y_2Z_1 + Y_1Z_2 + X_2Z_1 - X_1Z_2))^3$$

One can easily check that this formula works for all inputs except point at infinity. So we get a strongly unified formula for elliptic curves in Weierstrass form.

Addition: For addition of two different points, the operations can be organized as follows.

$$
\begin{aligned}
&T_1 = X_1Z_2,\ T_2 = X_2Z_1,\ T_3 = Y_1Z_2,\ T_4 = Y_2Z_1,\ T_5 = Z_1Z_2,\\
&T_6 = T_1 + T_2,\ T_7 = T_4 - T_3,\ T_8 = T_3 + T_4 + T_2 - T_1,\ T_9 = T_5T_8,\\
&T_{10} = T_1^2 + T_2T_6aT_5^2 + T_7,\ T_{11} = T_9T_8,\ T_{12} = T_{10}^2 - T_6.T_{11},\\
&X_3 = T_8.T_{12},\\
&Y_3 = T_{10}(T_1.T_{11} - T_{12}) - T_3T_{11}T_9,\\
&Z_3 = T_9^2.T_9
\end{aligned}
$$

The operation count shows that this formula costs $15\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$, where $\mathbf{M}$ denotes the cost of field multiplication, $\mathbf{S}$ the cost of field squiring and $\mathbf{D}$ the cost of multiplication by curve parameter.

Doubling: For doubling of a point, the operations can be organized as follows.

$$
\begin{aligned}
&T_1 = Z_1^2, T_2 = X_1Z_1,\ T_3 = Y_1Z_1,\ T_4 = 2T_1T_3,\\
&T_5 = 3T_2^2 + aT_1^2,\ T_6 = T_3T_4,\ T_7 = 4T_2T_6,\ T_8 = T_5^2 - T_7\\
&X_3 = T_4T_8,\\
&Y_3 = T_5(\frac{1}{2}T_5 - T_8) - 2T_6^2,\\
&Z_3 = T_4^2T_4
\end{aligned}
$$

The operation count shows that this formula costs $8\mathbf{M} + 6\mathbf{S} + 1\mathbf{D}$.

2.1.3 Jacobian Coordinates

The Projective point $(X : Y : Z), Z \neq 0$, corresponds to the affine point $(X/Z^2, Y/Z^3)$. The Projective form of the Weierstrass equation

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

defined over K in Jacobian coordinates is

$$Y^2 = X^3 + aXZ^4 + bZ^6.$$

The point at infinity $\mathcal{O}$ is represented by any triplet $(\alpha^2 : \alpha^3 : 0), \alpha \in K^*$, although in a practical implementation, since the coordinates of this point are never actually operated on, any triplet with $Z = 0$ would do. The negative of any point $(X : Y : Z)$ is $(X : -Y : Z)$.

Let P_1, P_2 and P_3 be three points on the elliptic curves, where $P_1 = (X_1, Y_1, Z_1)$, $P_2 = (X_2, Y_2, Z_2)$ and $P_3 = (X_3, Y_3, Z_3)$. Now changing variables (x, y) to $(X/Z^2, Y/Z^3)$ and using the addition formula 2.4 for E in affine coordinates to obtain the following formulas for computing

$(X_3 : Y_3 : Z_3)$ in Jacobian coordinates:

$$\begin{aligned} X_3 = &(X_1^2 Z_2^4 + X_2 Z_1^2 (X_2 Z_1^2 + X_1 Z_2^2) + a Z_1^4 Z_2^4 + Z_1 Z_2 (Y_2 Z_1^3 - Y_1 Z_2^3))^2 \\ &- (X_2 Z_1^2 + X_1 Z_2^2)(Y_2 Z_1^3 + Y_1 Z_2^3 + Z_1 Z_2 (X_2 Z_1^2 - X_1 Z_2^2))^2 \end{aligned}$$

$$\begin{aligned} Y_3 = &(X_1^2 Z_2^4 + X_2 Z_1^2 (X_2 Z_1^2 + X_1 Z_2^2) + a Z_1^4 Z_2^4 + Z_1 Z_2 (Y_2 Z_1^3 - Y_1 Z_2^3)) \\ &(X_1 Z_2^2 (Y_2 Z_1^3 + Y_1 Z_2^3 + Z_1 Z_2 (X_2 Z_1^2 - X_1 Z_2^2))^2 - X_3) \\ &- Y_1 Z_2^3 (Y_2 Z_1^3 + Y_1 Z_2^3 + Z_1 Z_2 (X_2 Z_1^2 - X_1 Z_2^2))^3 \end{aligned}$$

$$Z_3 = Z_1 Z_2 (Y_2 Z_1^3 + Y_1 Z_2^3 + Z_1 Z_2 (X_2 Z_1^2 - X_1 Z_2^2))$$

This formula also works for all inputs except point at infinity.

Addition: For addition of two different points, the operations are organized as follows.

$$\begin{aligned} &T_1 = X_1 Z_2^2,\ T_2 = X_2 Z_1^2,\ T_3 = Y_1 Z_2^3,\ T_4 = Y_2 Z_1^3,\ T_5 = Z_1 Z_2, \\ &T_6 = T_1 + T_2,\ T_7 = (T_2 - T_1) T_5,\ T_8 = T_3 + T_4 + T_7,\ T_9 = T_4 - T_3, \\ &T_{10} = T_1^2 + T_2 T_6 + a T_5^4 + T_9 T_5, \\ &X_3 = T_{10}^2 - T_6 T_7^2, \\ &Y_3 = T_{10}(T_1 . T_7^2 - X_3) - T_3 . T_7^2 . T_7, \\ &Z_3 = T_5 T_7 \end{aligned}$$

The operation count shows that this formula costs $16\mathbf{M} + 7\mathbf{S} + 1\mathbf{D}$, where $\mathbf{M}$ denotes the cost of field multiplication, $\mathbf{S}$ the cost of field squiring and $\mathbf{D}$ the cost of multiplication by curve parameter.

Doubling: For doubling of a point, the operations are organized as follows.

$$\begin{aligned} &T_1 = Z_1^2, T_2 = X_1 T_1,\ T_3 = Y_1 T_1 Z_1,\ T_4 = 3T_2^2 + a T_1^4,\ T_5 = T_2 T_3^2, \\ &X_3 = T_4^2 - 8T_5, \\ &Y_3 = T_4(4T_5 - X_3) - 8T_3^4, \\ &Z_3 = 2T_1 T_3 \end{aligned}$$

The operations costs $6\mathbf{M} + 7\mathbf{S} + 1\mathbf{D}$.

The costs for point addition and doubling in characteristic $p > 3$ are summarized in Table 2.1.

Operation	Affine	Projective	Jacobian
General Addition	$1I + 3M + 2S$	$15M + 4S + 1D$	$16M + 7S + 1D$
Point Doubling	$1I + 2M + 2S$	$8M + 6S + 1D$	$6M + 7S + 1D$

Table 2.1: Costs for point addition and doubling in different coordinate systems.

The key observation is that point addition can be done in Projective coordinates using field multiplications only, with no inversions required. Thus, inversions are deferred, and only one need to be performed at the end, a point multiplication operation, if it is required that the final result will be given in affine coordinates.

2.2 Elliptic Curves over Fields of Characteristic $p = 2$

2.2.1 Affine coordinates

For characteristic 2, there are two different types of elliptic curves in Weierstrass form. One is non-supersingular(ordinary) and another is supersingular. So we consider two cases here.

Non-Supersingular: In Weierstrass form, the ordinary elliptic curves over some field K of characteristic two is defined as

$$E(K) = \{\mathcal{O}\} \cup \{(x, y) \in K \times K \mid y^2 + xy = x^3 + ax^2 + b\} \tag{2.5}$$

with $a, b \in K, b \neq 0$ and $\{\mathcal{O}\}$ is the point at infinity, while the negative of a point $P = (x_1, y_1)$ is $-P = (x_1, x_1 + y_1)$. The addition operation on E is defined as follows:

Suppose $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are points on E. Then

(I) $P + \mathcal{O} = \mathcal{O} + P = P$;

(II) $P + (-P) = (-P) + P = \mathcal{O}$;

(III) Otherwise, $P + Q = (x_3, y_3)$, where

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a$$
$$y_3 = \lambda(x_1 + x_3) + x_3 + y_1$$

and

$$\lambda = \begin{cases} \dfrac{y_1 + y_2}{x_1 + x_2} & \text{if} \quad P \neq Q \\ \dfrac{y_1}{x_1} + x_1 & \text{if} \quad P = Q \end{cases} \tag{2.6}$$

We now combine these two formula for different λ to make it unified. For this we provide a single slope equation of λ as follows:

[Remember that here, $2 = 0, 1 = -1$]

Since the two points P and Q lies on the curve (2.5), so we get

$$y_1^2 + x_1 y_1 = x_1^3 + a x_1^2 + b$$
$$y_2^2 + x_2 y_2 = x_2^3 + a x_2^2 + b$$

Adding,

$$\begin{aligned}
&y_1^2 + y_2^2 + x_1y_1 + x_2y_2 = x_1^3 + x_2^3 + a(x_1^2 + x_2^2) \\
\Rightarrow &(y_1 + y_2)^2 + x_1y_1 + x_2y_2 + x_1y_2 + x_1y_2 = x_1^3 + x_2^3 + a(x_1^2 + x_2^2) \\
\Rightarrow &(y_1 + y_2)^2 + x_1(y_1 + y_2) = (x_1 + x_2)(x_1^2 + x_2^2 + x_1x_2) + a(x_1 + x_2)^2 + y_2(x_1 + x_2) \\
\Rightarrow &\frac{y_1 + y_2}{x_1 + x_2} = \frac{x_1^2 + x_2^2 + x_1x_2 + a(x_1 + x_2) + y_2}{y_1 + y_2 + x_1} \\
\Rightarrow &\frac{y_1 + y_2}{x_1 + x_2} = \frac{x_1^2 + (x_2 + a)(x_1 + x_2) + y_2}{y_1 + y_2 + x_1} \qquad [y_2 \neq x_1 + y_1]
\end{aligned}$$

Thus we get,

$$\lambda = \frac{y_1 + y_2}{x_1 + x_2} = \frac{x_1^2 + (x_2 + a)(x_1 + x_2) + y_2}{y_1 + y_2 + x_1} \qquad [y_2 \neq x_1 + y_1]$$

Therefore, we define the unified **Addition Rule** as:

For all $P = (x_1, y_1)$ and $Q = (x_2, y_2)$,

(I) $P + \mathcal{O} = \mathcal{O} + P = P$

(II) $P + (-P) = (-P) + P = \mathcal{O}$, [Remember that $Q = -P = (x_1, x_1 + y_1)$]

(III) Otherwise, $P + Q = (x_3, y_3)$, where

$$\begin{aligned}
x_3 &= \lambda^2 + \lambda + x_1 + x_2 + a \\
y_3 &= \lambda(x_1 + x_3) + x_3 + y_1
\end{aligned}$$

and

$$\lambda = \frac{x_1^2 + (x_2 + a)(x_1 + x_2) + y_2}{y_1 + y_2 + x_1} \tag{2.7}$$

Correctness of the Formula

We now show that this formula works for both doubling and addition as below. Note that for all the cases below we are not bothering about the condition $y_2 = y_1 + x_1$ as we considered different addition rule for it.

Case 1: $P = Q$. [Doubling]

Therefore, $x_1 = x_2$ and $y_1 = y_2$. Then putting these value in 2.7 and get

$$\lambda = \frac{x_1^2 + y_1}{x_1}$$

which is same as in the case of original doubling formula in 2.6.

Case 2: $P \neq Q$. [Addition]

- **Subcase 2.1** $x_1 \neq x_2$ and $y_1 = y_2$

  Then from the curve (2.5), we get

  $$y_1^2 + x_1 y_1 = x_1^3 + a x_1^2 + b$$
  $$y_1^2 + x_2 y_1 = x_2^3 + a x_2^2 + b$$

  Adding these two equation we get,

  $$\begin{aligned}(x_1 + x_2)y_1 &= (x_1 + x_2)(x_1^2 + x_2^2 + x_1 x_2) + a(x_1 + x_2)^2 \\ \Rightarrow &(x_1 + x_2)(x_1^2 + x_2^2 + x_1 x_2 + a(x_1 + x_2) + y_1) = 0 \\ \Rightarrow &(x_1 + x_2)(x_1^2 + (x_2 + a)(x_1 + x_2) + y_1) = 0\end{aligned}$$

  Since $(x_1 + x_2) \neq 0$, we get

  $$(x_1^2 + (x_2 + a)(x_1 + x_2) + y_1) = 0$$

  Therefore the numerator of λ in 2.7 becomes 0 only which is same as original case in 2.6.

- **Subcase 2.2** $x_1 \neq x_2$ and $y_1 \neq y_2$

  We have to show that

  $$\lambda = \frac{x_1^2 + (x_2 + a)(x_1 + x_2) + y_2}{y_1 + y_2 + x_1} = \frac{y_1 + y_2}{x_1 + x_2}$$

  and this easily follows from the same calculation as above since $y_2 \neq x_1 + y_1$.

- **Subcase 2.3** $x_1 = x_2$. Then from the curve 2.5, we get either $y_1 = y_2$ or $y_2 = x_1 + y_1$.

  If $y_1 = y_2$ then this is nothing but doubling and another case is addition of P and $-P$ which is considered in the addition rule.

2.2.2 Projective Coordinates

The Projective point $(X : Y : Z), Z \neq 0$, corresponds to the affine point $(X/Z, Y/Z)$. The Projective equation of the elliptic curve is

$$Y^2 Z + XYZ = X^3 + aX^2 Z + bZ^3$$

The point at infinity $\mathcal{O}$ is represented by the triplet $(0, 1, 0)$, while the negative of $(X : Y : Z)$ is $(X : X + Y : Z)$.

Let P_1, P_2 and P_3 be three points on the elliptic curves, where $P_1 = (X_1, Y_1, Z_1)$, $P_2 = (X_2, Y_2, Z_2)$ and $P_3 = (X_3, Y_3, Z_3)$. So changing variables (x, y) to $(X/Z, Y/Z)$ and using the addition formula 2.7 for E in affine coordinates to obtain the following formulas for computing $(X3 : Y3 : Z3)$ in Projective coordinates:

$$\begin{aligned}
X_3 = {} & Z_1Z_2(Y_2Z_1 + Y_1Z_2 + X_1Z_2) \\
& [(X_1^2Z_2^2 + (X_2Z_1 + aZ_1Z_2)(X_2Z_1 + X_1Z_2) + Y_2Z_1Z_1Z_2)^2 \\
& + (Z_1Z_2(Y_2Z_1 + Y_1Z_2 + X_1Z_2))(X_1^2Z_2^2 + (X_2Z_1 + aZ_1Z_2)(X_2Z_1 + X_1Z_2) \\
& + Y_2Z_1Z_1Z_2) + Z_1Z_2(X_2Z_1 + X_1Z_2)(Y_2Z_1 + Y_1Z_2 + X_1Z_2)^2 \\
& + a(Z_1Z_2(Y_2Z_1 + Y_1Z_2 + X_1Z_2))^2]
\end{aligned}$$

$$\begin{aligned}
Y_3 = {} & (X_1^2Z_2^2 + (X_2Z_1 + aZ_1Z_2)(X_2Z_1 + X_1Z_2) + Y_2Z_1Z_1Z_2) \\
& (X_1Z_2Z_1Z_2(Y_2Z_1 + Y_1Z_2 + X_1Z_2)^2 \\
& + (X_1^2Z_2^2 + (X_2Z_1 + aZ_1Z_2)(X_2Z_1 + X_1Z_2) + Y_2Z_1Z_1Z_2)^2 \\
& + (Z_1Z_2(Y_2Z_1 + Y_1Z_2 + X_1Z_2))(X_1^2Z_2^2 + (X_2Z_1 + aZ_1Z_2)(X_2Z_1 + X_1Z_2) \\
& + Y_2Z_1Z_1Z_2) + Z_1Z_2(X_2Z_1 + X_1Z_2)(Y_2Z_1 + Y_1Z_2 + X_1Z_2)^2 \\
& + a(Z_1Z_2(Y_2Z_1 + Y_1Z_2 + X_1Z_2))^2) + X_3 + Y_1Z_2Z_1^2Z_2^2(Y_2Z_1 + Y_1Z_2 + X_1Z_2)^3
\end{aligned}$$

$$Z_3 = (Z_1Z_2(Y_2Z_1 + Y_1Z_2 + X_1Z_2))^3$$

Addition: For addition of two different points, the operations can be organized as follows.

$$\begin{aligned}
& T_1 = X_1Z_2,\ T_2 = X_2Z_1,\ T_3 = Y_1Z_2,\ T_4 = Y_2Z_1,\ T_5 = Z_1Z_2, \\
& T_6 = T_1 + T_2,\ T_7 = T_2 + aT_5,\ T_8 = T_4.T_5,\ T_9 = T_3 + T_4 + T_1, \\
& T_{10} = T_5.T_9,\ T_{11} = T_{10}(T_1 + T_7).T_9,\ T_{12} = T_1^2 + T_6.T_7 + T_8, \\
& T_{13} = T_{12}^2 + T_{10}.T_{12} + T_{11}, \\
& X_3 = T_{10}.T_{13}, \\
& Y_3 = T_{12}(T_1.T_{10}.T_9 + T_{13}) + X_3 + T_3.T_{10}^2.T_9, \\
& Z_3 = T_{10}^2.T_{10}
\end{aligned}$$

The operation count shows that this formula costs $18\mathbf{M} + 3\mathbf{S} + 1\mathbf{D}$, where $\mathbf{M}$ denotes the cost of field multiplication, $\mathbf{S}$ the cost of field squiring and $\mathbf{D}$ the cost of multiplication by curve parameter.

Doubling: For doubling of a point, the operations can be organized as follows.

$$\begin{aligned}
& T_1 = Z_1^2, T_2 = X_1Z_1,\ T_3 = Y_1Z_1,\ T_4 = T_1T_2, \\
& T_5 = T_1T_3,\ T_6 = T_2^2 + T_5,\ T_7 = T_6(T_6 + T_4) + aT_4^2, \\
& X_3 = T_4T_7, \\
& Y_3 = T_6(T_4 + T_7) + X_3 + T_5T_4T_2^2, \\
& Z_3 = T_4^2T_4
\end{aligned}$$

The operation count shows that this formula costs $10\mathbf{M} + 3\mathbf{S} + 1\mathbf{D}$.

2.2.3 Jacobian Coordinates

Let P_1, P_2 and P_3 be three points on the elliptic curves, where $P_1 = (X_1, Y_1, Z_1)$, $P_2 = (X_2, Y_2, Z_2)$ and $P_3 = (X_3, Y_3, Z_3)$. So changing variables (x, y) to $(X/Z^2, Y/Z^3)$ and using the addition formula 2.7 for E in affine coordinates to obtain the following formulas for computing $(X3 : Y3 : Z3)$ in Jacobian coordinates as:

$$\begin{aligned} X_3 = {} & (X_1^2Z_2^4 + (X_2Z_1^2 + aZ_1^2Z_2^2)(X_2Z_1^2 + X_1Z_2^2) + Y_2Z_1^3Z_1Z_2)^2 \\ & + Z_1Z_2(Y_2Z_1^3 + Y_1Z_2^3 + X_1Z_2^2Z_1Z_2)(X_1^2Z_2^4 + (X_2Z_1^2 + aZ_1^2Z_2^2)(X_2Z_1^2 + X_1Z_2^2) \\ & + Y_2Z_1^3Z_1Z_2) + (X_2Z_1^2 + X_1Z_2^2 + aZ_1^2Z_2^2)(Y_2Z_1^3 + Y_1Z_2^3 + X_1Z_2^2Z_1Z_2) \end{aligned}$$

$$\begin{aligned} Y_3 = {} & (X_1^2Z_2^4 + (X_2Z_1^2 + aZ_1^2Z_2^2)(X_2Z_1^2 + X_1Z_2^2) + Y_2Z_1^3Z_1Z_2) \\ & (X_1Z_2^2(Y_2Z_1^3 + Y_1Z_2^3 + X_1Z_2^2Z_1Z_2)^2 + X_3) \\ & + X_3Z_3 + Y_1Z_2^3(Y_2Z_1^3 + Y_1Z_2^3 + X_1Z_2^2Z_1Z_2)^3 \end{aligned}$$

$$Z_3 = Z_1Z_2(Y_2Z_1^3 + Y_1Z_2^3 + X_1Z_2^2Z_1Z_2)$$

Addition: For addition of two different points, the operations are organized as follows.

$$\begin{aligned} & T_1 = X_1Z_2^2,\ T_2 = X_2Z_1^2,\ T_3 = Y_1Z_2^3,\ T_4 = Y_2Z_1^3,\ T_5 = Z_1Z_2, \\ & T_6 = T_3 + T_4 + T_1T_5,\ T_7 = T_1 + T_2,\ T_8 = T_2 + aT_5^2,\ T_9 = T_7 + aT_5^2, \\ & T_{10} = T_5.T_6,\ T_{11} = T_1^2 + T_8T_7 + T_4T_5, \\ & X_3 = T_{11}(T_{11} + T_{10}) + T_9T_6^2, \\ & Y_3 = T_{11}(T_1.T_6^2 + X_3) + X_3T_{10} + T_3.T_6^2.T_6, \\ & Z_3 = T_{10} \end{aligned}$$

The operation count shows that this formula costs $18\mathbf{M} + 5\mathbf{S} + 1\mathbf{D}$, where $\mathbf{M}$ denotes the cost of field multiplication, $\mathbf{S}$ the cost of field squiring and $\mathbf{D}$ the cost of multiplication by curve parameter.

Doubling: For doubling of a point, the operations are organized as follows.

$$\begin{aligned} & T_1 = Z_1^2, T_2 = X_1T_1,\ T_3 = Y_1T_1Z_1,\ T_4 = T_1T_3, \\ & T_5 = T_2^2 + T_4,\ T_6 = T_2T_1^2,\ T_7 = T_6T_2^2, \\ & X_3 = T_5(T_5 + T_6) + aT_6^2, \\ & Y_3 = T_5(T_7 + X_3) + X_3T_6 + T_4T_7, \\ & Z_3 = T_6 \end{aligned}$$

The operations costs $10\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$.

The different costs for point addition and doubling of non-supersingular curves in characteristic $p = 2$ are summarized in Table 2.2.

Supersingular: In Weierstrass form, the supersingular elliptic curves over some field K of characteristic two is defined as

$$E(K) = \{\mathcal{O}\} \cup \{(x, y) \in K \times K \mid y^2 + cy = x^3 + ax + b\} \tag{2.8}$$

Operation	Affine	Projective	Jacobian
General addition	$1I + 3M + 2S$	$18M + 3S + 1D$	$18M + 5S + 1D$
Point Doubling	$1I + 2M + 2S$	$10M + 3S + 1D$	$10M + 4S + 1D$

Table 2.2: Costs for non-supersingular curves in characteristic $p = 2$.

with $a, b, c \in K, c \neq 0$ and $\{\mathcal{O}\}$ is the point at infinity, while the negative of a point $P = (x_1, y_1)$ is $-P = (x_1, y_1 + c)$. The addition operation on E is defined as follows.

Suppose $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are points on E. Then

(I) $P + \mathcal{O} = \mathcal{O} + P = P$;

(II) $P + (-P) = (-P) + P = \mathcal{O}$;

(III) Otherwise, $P + Q = (x_3, y_3)$, where

$$x_3 = \lambda^2 + x_1 + x_2$$
$$y_3 = \lambda(x_1 + x_3) + y_1 + c$$

and

$$\lambda = \begin{cases} \dfrac{y_1 + y_2}{x_1 + x_2} & \text{if} \quad P \neq Q \\ \dfrac{x_1^2 + a}{c} & \text{if} \quad P = Q \end{cases} \tag{2.9}$$

We now combine these two formula for different λ to make it unified. Calculations are given below:

Since the two points P and Q lies on the curve 2.8, so we get

$$y_1^2 + cy_1 = x_1^3 + ax_1 + b$$
$$y_2^2 + cy_2 = x_2^3 + ax_2 + b$$

Adding,

$$(y_1 + y_2)^2 + c(y_1 + y_2) = (x_1 + x_2)(x_1^2 + x_2^2 + x_1x_2 + a)$$
$$\Rightarrow \frac{y_1 + y_2}{x_1 + x_2} = \frac{x_1^2 + x_2(x_1 + x_2) + a}{y_1 + y_2 + c} \qquad [y_2 \neq y_1 + c]$$

Therefore we get,

$$\lambda = \frac{y_1 + y_2}{x_1 + x_2} = \frac{x_1^2 + x_2(x_1 + x_2) + a}{y_1 + y_2 + c} \qquad [y_2 \neq y_1 + c]$$

So, the unified **Addition Rule** is:

For all $P = (x_1, y_1)$ and $Q = (x_2, y_2)$,

(I) $P + \mathcal{O} = \mathcal{O} + P = P$

(II) $P + (-P) = (-P) + P = \mathcal{O}$, [Remember that $Q = -P = (x_1, y_1 + c)$]

(III) Otherwise, $P + Q = (x_3, y_3)$, where

$$x_3 = \lambda^2 + x_1 + x_2$$
$$y_3 = \lambda(x_1 + x_3) + y_1 + c$$

and

$$\lambda = \frac{x_1^2 + x_2(x_1 + x_2) + a}{y_1 + y_2 + c} \tag{2.10}$$

Correctness of the Formula

Now we show that this formula works for both doubling and addition as below. Note that for all the cases below we did not consider the case $y_2 = y_1 + c$ as we gave different addition rule for it.

Case 1: $P = Q$. [Doubling]

Therefore, $x_1 = x_2$ and $y_1 = y_2$. Then putting these value in 2.10 and get

$$\lambda = \frac{x_1^2 + a}{c}$$

which is same as in the case of original doubling formula in 2.9.

Case 2: $P \neq Q$. [Addition]

- **Subcase 2.1** $x_1 \neq x_2$ and $y_1 = y_2$

  Then from the curve 2.8, we get

  $$y_1^2 + cy_1 = x_1^3 + ax_1 + b$$
  $$y_1^2 + cy_1 = x_2^3 + ax_2 + b$$

  Adding these two equation we get,

  $$(x_1 + x_2)(x_1^2 + x_1x_2 + x_2^2 + a) = 0$$

Since $(x_1 + x_2) \neq 0$, we get

$$(x_1^2 + x_1x_2 + x_2^2 + a) = 0$$

Therefore the numerator of λ in 2.10 becomes 0 only which is same as in 2.9.

- **Subcase 2.2** $x_1 \neq x_2$ and $y_1 \neq y_2$

  We have to show that

$$\lambda = \frac{x_1^2 + x_2(x_1 + x_2) + a}{y_1 + y_2 + c} = \frac{y_1 + y_2}{x_1 + x_2}$$

  and this easily follows from the same calculation as above, since $y_2 \neq y_1 + c$.

- **Subcase 2.3** $x_1 = x_2$. Then from the curve 2.8, we get either $y_1 = y_2$ or $y_2 = y_1 + c$.

  If $y_1 = y_2$ then this is nothing but doubling and another case is addition of P and $-P$ which is considered in the addition rule.

2.2.4 Projective Coordinates

Let P_1, P_2 and P_3 be three points on the elliptic curves, where $P_1 = (X_1, Y_1, Z_1)$, $P_2 = (X_2, Y_2, Z_2)$ and $P_3 = (X_3, Y_3, Z_3)$. So changing variables (x, y) to $(X/Z, Y/Z)$ and using the addition formula 2.10 for E in affine coordinates to obtain the following formulas for computing $(X3 : Y3 : Z3)$ in Projective coordinates as:

$$\begin{aligned}
X_3 = {} & Z_1Z_2(Y_2Z_1 + Y_1Z_2 + cZ_1Z_2) \\
& [(X_1^2Z_2^2 + X_2Z_1(X_2Z_1 + X_1Z_2) + aZ_1^2Z_2^2)^2 \\
& + Z_1Z_2(X_2Z_1 + X_1Z_2)(Y_2Z_1 + Y_1Z_2 + cZ_1Z_2)^2]
\end{aligned}$$

$$\begin{aligned}
Y_3 = {} & (X_1^2Z_2^2 + X_2Z_1(X_2Z_1 + X_1Z_2) + aZ_1^2Z_2^2) \\
& [X_1Z_2Z_1Z_2(Y_2Z_1 + Y_1Z_2 + cZ_1Z_2)^2 \\
& + (X_1^2Z_2^2 + X_2Z_1(X_2Z_1 + X_1Z_2) + aZ_1^2Z_2^2)^2 \\
& + Z_1Z_2(X_2Z_1 + X_1Z_2)(Y_2Z_1 + Y_1Z_2 + cZ_1Z_2)^2] \\
& + Z_1^2Z_2^2(Y_2Z_1 + cZ_1Z_2)(Y_2Z_1 + Y_1Z_2 + cZ_1Z_2)^3
\end{aligned}$$

$$Z_3 = (Z_1Z_2(Y_2Z_1 + Y_1Z_2 + cZ_1Z_2))^3$$

Addition: For addition of two different points, the operations can be organized as follows.

$$
\begin{aligned}
&T_1 = X_1Z_2,\ T_2 = X_2Z_1,\ T_3 = Y_1Z_2,\ T_4 = Y_2Z_1,\ T_5 = Z_1Z_2,\\
&T_6 = T_3 + T_4 + cT_1,\ T_7 = T_1^2 + T_2(T_1 + T_2) + aT_5^2,\ T_8 = T_5.T_6,\ T_9 = T_8T_6,\\
&T_{10} = T_7^2 + T_9(T_1 + T_2),\\
&X_3 = T_8T_{10},\\
&Y_3 = T_7(T_1T_9 + T_{10}) + T_9T_8(T_6 - T_4),\\
&Z_3 = T_8^2.T_8
\end{aligned}
$$

The operation count shows that this formula costs $15\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$, where $\mathbf{M}$ denotes the cost of field multiplication, $\mathbf{S}$ the cost of field squiring and $\mathbf{D}$ the cost of multiplication by curve parameter.

Doubling: For doubling of a point, the operations can be organized as follows.

$$
\begin{aligned}
&T_1 = Z_1^2, T_2 = X_1Z_1,\ T_3 = Y_1Z_1,\ T_4 = cT_1,\\
&T_5 = T_2^2 + aT_1^2,\ T_6 = T_1T_4,\\
&X_3 = T_6T_5^2,\\
&Y_3 = T_5(T_2T_6T_4 + T_5) + T_6^2(T_3 + T_4)T_4,\\
&Z_3 = T_6^2T_6
\end{aligned}
$$

The operation count shows that this formula costs $10\mathbf{M} + 5\mathbf{S} + 2\mathbf{D}$.

2.2.5 Jacobian Coordinates

Let P_1, P_2 and P_3 be three points on the elliptic curves, where $P_1 = (X_1, Y_1, Z_1)$, $P_2 = (X_2, Y_2, Z_2)$ and $P_3 = (X_3, Y_3, Z_3)$. So changing variables (x, y) to $(X/Z^2, Y/Z^3)$ and using the addition formula 2.10 for E in affine coordinates to obtain the following formulas for computing $(X3 : Y3 : Z3)$ in Jacobian coordinates as:

$$
\begin{aligned}
X_3 = {} & (X_1^2Z_2^4 + X_2Z_1^2(X_2Z_1^2 + X_1Z_2^2) + aZ_1^4Z_2^4)^2\\
& + (X_2Z_1^2 + X_1Z_2^2)(Y_2Z_1^3 + Y_1Z_2^3 + cZ_1^3Z_2^3)^2
\end{aligned}
$$

$$
\begin{aligned}
Y_3 = {} & (X_1^2Z_2^4 + X_2Z_1^2(X_2Z_1^2 + X_1Z_2^2) + aZ_1^4Z_2^4)\\
& (X_1Z_2^2(Y_2Z_1^3 + Y_1Z_2^3 + cZ_1^3Z_2^3)^2 + X_3)\\
& + (Y_1Z_2^3 + cZ_1^3Z_2^3)(Y_2Z_1^3 + Y_1Z_2^3 + cZ_1^3Z_2^3)^3
\end{aligned}
$$

$$
Z_3 = Z_1Z_2(Y_2Z_1^3 + Y_1Z_2^3 + cZ_1^3Z_2^3)
$$

Addition: For addition of two different points, the operations are organized as follows.

$$
\begin{aligned}
&T_1 = X_1 Z_2^2,\ T_2 = X_2 Z_1^2,\ T_3 = Y_1 Z_2^3,\ T_4 = Y_2 Z_1^3,\ T_5 = Z_1 Z_2,\\
&T_6 = T_1 + T_2,\ T_7 = cT_5^2 T_5,\ T_8 = T_3 + T_4 + T_7,\ T_9 = T_1^2 + T_2 T_6 + a(T_5^2)^2,\\
&X_3 = T_9^2 + T_8^2 T_6,\\
&Y_3 = T_9(T_1.T_8^2 + X_3) + (T_3 + T_7)T_8^2.T_8,\\
&Z_3 = T_5 T_8
\end{aligned}
$$

The operations costs $15\mathbf{M} + 7\mathbf{S} + 2\mathbf{D}$, where $\mathbf{M}$ denotes the cost of field multiplication, $\mathbf{S}$ the cost of field squiring and $\mathbf{D}$ the cost of multiplication by curve parameter.

Doubling: For doubling of a point, the operations are organized as follows.

$$
\begin{aligned}
&T_1 = Z_1^2,\ T_2 = T_1 Z_1,\ T_3 = X_1 T_1,\ T_4 = Y_1 T_2,\ T_5 = T_3^2 + a(T_1^2)^2,\ T_6 = cT_2^2,\\
&X_3 = T_5^2,\\
&Y_3 = T_5(T_3 T_6^2 + T_5) + (T_4 + T_6)T_6^2 T_6,\\
&Z_3 = T_1 T_6
\end{aligned}
$$

The operations costs $8\mathbf{M} + 7\mathbf{S} + 2\mathbf{D}$.

The different costs for point addition and doubling of supersingular curves in characteristic $p = 2$ are summarized in Table 2.3.

Operation	Affine	Projective	Jacobian
General addition	$1I + 3M + 2S$	$15M + 4S + 2D$	$15M + 7S + 2D$
Doubling	$1M + 2S + 1D$	$10M + 5S + 2D$	$8M + 7S + 2D$

Table 2.3: Costs for supersingular curves in characteristic $p = 2$.

2.3 Comparison

Now we wish to compare our proposed addition law with the other existing formula in literature. The EFD [27] is meant to provide an up-to-date database with all curve forms and coordinate systems ever proposed. A comparison in a paper can only give a snap-shot of what is known today. For the case of characteristic greater than 3, in general addition algorithm needs $1\mathbf{I} + 2\mathbf{M} + 1\mathbf{S}(1\mathbf{I} + 2\mathbf{M} + 2\mathbf{S})$ for addition(doubling) in affine coordinates, $12\mathbf{M} + 2\mathbf{S}(6\mathbf{M} + 5\mathbf{S})$ for addition(doubling) in Projective coordinates and $12\mathbf{M} + 4\mathbf{S}(3\mathbf{M} + 6\mathbf{S})$ for addition(doubling) in Jacobian coordinates. In the case of characteristic two, the cost of squaring operation is much lower than that of a general multiplication. We get from [27] for characteristic 2, general addition algorithm in non-supersingular curves needs $1\mathbf{I} + 2\mathbf{M} + 1\mathbf{S}(1\mathbf{I} + 2\mathbf{M} + 1\mathbf{S})$ for addition(doubling) in affine coordinates, $14\mathbf{M} + 1\mathbf{S}(7\mathbf{M} + 4\mathbf{S})$ for addition(doubling) in Projective coordinates and $14\mathbf{M}+5\mathbf{S}(4\mathbf{M}+5\mathbf{S})$ for addition(doubling) in Jacobian coordinates. Thus we see that our formula takes more costs for Projective and Jacobian coordinates, but provides you a unified formulas. By choosing curve parameters appropriately one can reduce these costs. In Edwards coordinates, highest speed can be achieved. In [26], shows that the algorithm for doubling uses $3\mathbf{M} + 4\mathbf{S}$, and for addition uses $10\mathbf{M} + 1\mathbf{S}$. For inverted Edwards coordinates [25], doubling formulas use $3\mathbf{M} + 4\mathbf{S}$, and addition formulas use $9\mathbf{M} + 1\mathbf{S}$. Also addition formula in Edwards coordinates are strongly unified.

Chapter 3

Tate Pairings on Edwards curves

3.1 Introduction

Pairing on elliptic curves are recently of great interest due to their applications in several cryptographic schemes such as Diffie-protocol [8], Short Signatures [6], Group Signatures [7], Signcryption [18] , Identity Based Encryption (IBE) [5], Identity Based Signature (IBS) [16] etc. The basic algorithm used in pairing computation was first described by Miller and is an extension of the double-and-add method for finding a point multiple, and was subsequently published in [14]. Tate pairing computation on some supersingular curves in Weierstrass form was studied in [1].

In 2007, Harold M. Edwards [10] proposed a new normal form for Elliptic Curves called Edwards Curve and their application to cryptography was first developed by Bernstein and Lange [2]. Edwards curves have lot of attention due to the fact that their group law can be computed very efficiently. Bernstein and Lange pointed out several advantages of the Edwards form in comparison to the more well known Weierstrass form. One remarkable advantage is the addition formulas on Edwards form is complete. This is very useful in providing resistance to side-channel attacks. In view of the advantages of Edwards curves, a designer may wish to implement a pairing based protocol using such curves. The difficulty comes when trying to express Miller's algorithm in Edwards coordinates is that it is difficult to find the equations of rational functions that need to be evaluated at each addition step. On a curve in Weierstrass form, these functions are readily given by the line functions in the usual addition and doubling. For curves in Edwards form matters are more complex as Edwards curves have degree 4 and thus any line passes through 4 curve points instead of 3.

So far three paper have attempted to compute pairings efficiently on Edwards curve: The first paper by Das and Sarkar [20] in 2008. Das and Sarkar use the birational equivalence to Weierstrass curves to map the points on the Edwards curve to a Weierstrass curve on which the usual line functions are then evaluated. Then they develop explicit formulas on supersingular curves with embedding degree $k = 2$. Because of this transformation from Edwards form to Weierstrass form and again back to Edwards form, this approach comes at a huge performance penalty. Then Ionica and Joux [21] come up with different approach in the same year 2008. They use a different map to a curve of degree 3 and compute the 4-th power of the Tate pairing. This does not create any problem for usage in protocols as long as all participating parties perform the same type of pairing computation. Their results are faster than Das and Sarkar's but they are still much slower than pairings on Weierstrass curves. And the third paper by Arene, Lange,

Naehrig and Ritzenthaler [22] in 2009. They provide a geometric interpretation of the addition law for twisted Edwards curves by presenting the functions which arise in addition and doubling. Then they develop explicit formulas for computing the Tate pairing on twisted Edwards curves using these functions in Miller's algorithm. This results much faster than previous two works.

3.2 Preliminaries

3.2.1 Edwards Coordinates

Edwards showed in [10] that every elliptic curve E defined over an algebraic number field is birationally equivalent over some extension field to a curve given by the equation

$$x^2 + y^2 = c^2(1 + x^2y^2),\ c \neq 0$$

Then Bernstein and Lange studied this equation over finite fields and introduced a curve parameter d getting an elliptic curve in Edwards form as

$$x^2 + y^2 = c^2(1 + dx^2y^2),\ c, d \neq 0$$

A simple and symmetric addition formula is defined on such a curve as

$$(x_1, y_1), (x_2, y_2) \mapsto \left(\frac{x_1y_2 + y_1x_2}{c(1 + dx_1x_2y_1y_2)}, \frac{y_1y_2 - x_1x_2}{c(1 - dx_1x_2y_1y_2)} \right) \tag{3.1}$$

The neutral element of this addition law is $(0, c); (0, -c)$ has order 2; $(\pm c, 0)$ have order 4. For every point $P = (x, y)$, the negative element is $-P = (-x, y)$.

It has been observed in [2] that the form $X^2 + Y^2 = C^2(1 + DX^2Y^2)$ is isomorphism with the form $x^2 + y^2 = 1 + dx^2y^2$ by the transformation $X = Cx$ and $Y = Cy$ with the condition that $C^4D = d$.

An extension, called the twisted Edwards form has been studied in [3]. The curve equation in this case has the form $ax^2+y^2 = 1+dx^2y^2$ for distinct non zero elements a and d in a finite field K with $\mathrm{char}(K) \neq 2$. It has been proved in [3] that the set of twisted Edwards form curves over the field K is birationally equivalent to the set of Montgomery form, $Bv^2 = u^3+Au^2+u,\ B \neq 0$ over K. Actually birational equivalence between Weierstrass and Edwards form use the Montgomery form as an intermediate stepping stone. The map

$$(x, y) \mapsto (u, v) = ((1 + y)/(1 - y), (1 + y)/(x(1 - y))) \tag{3.2}$$

transforms $ax^2 + y^2 = 1 + dx^2y^2$ to $Bv^2 = u^3 + Au^2 + u$, where $A = 2(a + d)/(a - d)$ and $B = 4/(a - d)$. Since a and d are distinct and non zero, A is not 2 or -2 and $B \neq 0$. The inverse map is given by $(u, v) \mapsto (x, y) = (u/v, (u - 1)/(u + 1))$.

The case $a = 1$ in twisted Edwards curve is the Edwards curve as considered in [2]. The following theorem (proof is given in [3]) shows that an elliptic curve is birationally equivalent to an Edwards form curve if and only if it has a point of order 4.

Theorem 3.2.1. *Let E be an elliptic curve over some finite field K with char(K) $\neq$ 2. Then E is birationally equivalent to a curve $x^2 + y^2 = 1 + dx^2y^2$ over k if and only if E has a point of order 4.*

Let the curve $s^2 = r^3 + a_2r^2 + a_4r$ in Weierstrass form has a point (r_1, s_1) of order 4. Then it is possible to exhibit a birational equivalence between the Weierstrass and Edwards forms. The map

$$(x, y) \mapsto (r, s) = ((r_1(1 + y))/(1 - y), (s_1(1 + y))/(x(1 - y))) \tag{3.3}$$

transforms $x^2 + y^2 = 1 + dx^2y^2$ to $s^2 = r^3 + a_2r^2 + a_4r$, where $a_2 = s_1^2/r_1^2 - 2r_1$; $a_4 = r_1^2$ and $d = 1 - 4r_1^3/s_1^2$ [2].

3.2.2 Background on Pairings

Here, we discuss some basics of Tate pairing. First we explain some fundamentals on divisors on elliptic curves. Let E be an elliptic curve over $\mathbb{F}_q$, with identity $\mathcal{O}$. Points on elliptic curves are denoted by P, Q, etc, while the corresponding places are denoted by (P), (Q), etc. (P), (Q) are just notations. The function field of E is the quotient field of the coordinate ring of E. Elements of this field are called functions over E.

Divisors of E are formal integer-linear combinations of places. Any non-constant function has finitely many zeros and poles at places, of some finite positive order. The collection of zeros and poles of a function, expressed as a divisor is called its principal divisor. For a function f, its principal divisor is denoted by $div(f) = (f)_0 - (f)_\infty$. The divisor $(f)_0$ is called the zero divisor of f and $(f)_\infty$ its pole divisor.

The computation of Tate pairing depends on the addition rule on the elliptic curve group. The main task of Tate pairing computations is to find a function with divisor $(P)+(Q)-(P+Q)-(\mathcal{O})$ for two input points P and Q, their sum $P + Q$, and identity element $\mathcal{O}$ as we need this function in Miller's algorithm.
Consider r a large prime dividing $\#E(\mathbb{F}_q)$ and k the corresponding embedding degree, i.e. the smallest positive integer such that r divides $q^k - 1$. Let $\mathcal{O}$ denote the neutral element on the elliptic curve. Let P be an r-torsion point. Then the Tate pairing is defined [1] as follows.

Definition 3.2.1. *Let $G := E(\mathbb{F}_q)$. The Tate pairing is defined as*

$$e_r(.,.) : G[r] \times G/rG \longrightarrow \mathbb{F}_{q^k}^*/\mathbb{F}_{q^k}^{*r}$$

with $e_r(P, Q) := f_P(Q)^{\frac{q^k-1}{r}}$. The function f_P is such that $div(f_P) = r(P) - r(\mathcal{O})$.

Let $h_{P,Q}$ denote the rational function corresponding to the addition of P and Q. Let $r = (r_{l-1} \dots r_0)$ the binary representation of r. With this setup, one efficient algorithm for computing the Tate pairing $e_r(P, Q)$ on an elliptic curve is Miller's Algorithm. The rational function appearing in the algorithm depends on the form of the elliptic curve. Miller's algorithm computes in the i-th iteration a function $f_{i,P}$ having divisor $div(f_{i,P}) = i(P) - ([i]P) - (i-1)(\mathcal{O})$, called Millers functions. At each step, the Millers functions are evaluated at the second argument. After $l-1$ iterations, the evaluation at Q of the function f having divisor $r(P)-r(\mathcal{O})$ is obtained.

3.3 Existing Techniques for Computing Tate Pairings

Remember that the main task of Tate pairing computation is that given $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, points on an elliptic curve, find a point P_3 and a function h such that $div(h) =$

$(P_1) + (P_2) - (P_3) - (\mathcal{O})$. i. e. finding Miller function. In Weierstrass form elliptic curve, this task can be easily handled using the chord-tangent rule. But for Edwards forms, things are not so simple.

Method proposed by Das and Sarkar [20]

Das and Sarkar [20] first computed Miller function for twisted Edwards form elliptic curve corresponding to addition of $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ by the following theorem.

Theorem 3.3.1. *Let $\mathbb{F}_q$ be a field of characteristic not equal to 2 and $ax^2 + y^2 = 1 + dx^2y^2$ be a twisted Edwards form curve where a and d are distinct non-zero elements of $\mathbb{F}_q$. Let $P_0 = (0, 1)$. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on it. Let $P_3 = (x_3, y_3)$ be the sum of P_1 and $P2$. Then the Miller function $h(x, y)$ such that*

$$div(h) = (P_1) + (P_2) - (P_3) - (P_0)$$

is given by

$$h(x, y) = \frac{(1 - y_3)}{x(yy_3)}((1 + y) - x(\lambda(1 + y) + \theta(1 - y))). \tag{3.4}$$

where $A = (2(a + d))/(a - d), B = 4/(a - d)$ and

$$\lambda = \begin{cases} \dfrac{x_1(A(y_1^2 - 1) - 2(1 + y_1 + y_1^2))}{B(y_1^2 - 1)} & \text{if} \quad P = Q \\ \dfrac{x_1(y_1 - 1)(y_2 + 1) - x_2(y_1 + 1)(y_2 - 1)}{2x_1x_2(y_1 - y_2)} & \text{if} \quad P \neq Q \end{cases}$$

and $\theta = 2(1 + y_1)/(x(1 - y_1))\lambda(1 + y_1)/(1 - y_1)$ is given by

$$\theta = \begin{cases} \dfrac{(y_1^2 - 1)(Ax_1^2 - B) - 2x_1^2(1 + y_1 + y_1^2)}{Bx_1(y_1^2 - 1)} & \text{if} \quad P = Q \\ \dfrac{(x_1 - x_2)(1 + y_1)(1 + y_2)}{2x_1x_2(y_1 - y_2)} & \text{if} \quad P \neq Q \end{cases}$$

For this function computation they did not assume anything on embedding degree.

Then they provide *supersingular curves* in Edwards Form. For this, they consider a well known supersingular curves $y^2 = x^3 + ax$ in Weierstrass form of embedding degree 2. Then using a birational equivalence map they compute corresponding Edwards forms

$$x^2 + y^2 = 1 - x^2y^2.$$

over $\mathbb{F}_q$ with $p \equiv 3 \bmod 4$, provided a is a square modulo p.

Then they follow the idea [1] of using distortion map $\phi(x, y) = (-x, iy)$, where $i^2 = -1$ for the curve $y^2 = x^3 + a$ over $\mathbb{F}_q$. They obtain a distortion map for the Edwards form curve by proving the following results.

Theorem 3.3.2. *The function $\phi : E(\mathbb{F}_q)[r] \mapsto E[\mathbb{F}_q^2]$ given by*

$$\phi(x, y) = \left(ix, \frac{1}{y}\right), \tag{3.5}$$

is a distortion map on the Edwards form curve $x^2 + y^2 = 1 - x^2y^2$.

Under this distortion map, the output of the Tate pairing $e(P, Q)$ is defined to be $e(P, \phi(Q))$. Each Miller iteration takes two points P_1 and P_2 and obtains $P_3 = P_1 + P_2$ and evaluates $h(\phi(Q))$, where h is the rational function obtained earlier. In other words, to compute

$$\begin{aligned} h\left(ix_Q, \frac{1}{y_Q}\right) &= \frac{(1-y_3)\left(\left(1+\frac{1}{y_Q}\right) - ix_Q\left(\lambda\left(1+\frac{1}{y_Q}\right) + \theta\left(1-\frac{1}{y_Q}\right)\right)\right)}{ix_Q(\frac{1}{y_q} - y_3)} \\ &= \frac{i(y_3-1)}{x_Q(1-y_Qy_3)}((y_Q+1) - ix_Q(\lambda(y_Q+1) + \theta(y_Q-1))) \qquad (3.6) \\ &= \frac{(y_Q+1)(y_3-1)}{x_Q(1-y_Qy_3)}(x_Q\lambda + \alpha_Q\theta + i) \end{aligned}$$

where $\alpha_Q = x_Q(y_Q - 1)/(y_Q + 1)$ and λ and θ are defined earlier. The value of α_Q depends only on Q and can be computed before starting the actual pairing computation. Finally they used technique as in [1] and some simplifications to get a inversion free efficient pairing.

Method proposed by Ionica and Joux [21]

Ionica and Joux [21] computed Tate pairing in a different way. Their idea is to describe a map of degree 4 from the Edwards curve E to a curve $E_{s,p} : s^2p = (1 + dp)^2 - 4p$. This curve has an equation of total degree 3 and, as in the Weierstrass case, we can easily compute the equations of the two lines that appear naturally when adding two points P_1 and P_2, i.e. the line l passing through P_1 and P_2 and the vertical line v that passes through $P_1 + P_2$. Then they pullback l and v to the Edwards curve. The output of their algorithm is essentially the desired pairing. They actually compute the 4-th power of the Tate pairing. This creates no problem for usage in protocols as long as all participating parties perform the same type of pairing computation. They first look at the action of the 4-torsion subgroup defined over a field $\mathbb{F}$ (odd characteristic) on a fixed point $P = (x, y)$, with $xy \neq 0$ on the Edwards curve. A simple computation shows that $P + T_4 = (y, -x)$, $P + T_2 = (-x, -y)$ and $P - T_4 = (-y, x)$, where $T_2 = (0, -1)$ the point of order 2 and $T_4 = (1, 0)$, $-T_4 = (-1, 0)$ the two points of order 4 on the Edwards curve. They consider the map

$$\begin{aligned} \phi : E &\to E_{s,p} \\ (x, y) &\to ((xy)^2, x/y - y/x). \end{aligned}$$

from the Edwards curve E to the curve $E_{s,p} : s^2p = (1 + dp)^2 - 4p$. Then they define addition rule on the curve $E_{s,p}$ as

Definition 3.3.1. *Let* $P_1, P_2 \in E_{s,p}$, *L the line connecting P_1 and P_2 (tangent line to $E_{s,p}$ if $P_1 = P_2$), and R the third point of intersection of L with E. Let L' be the vertical line through R. Then $P_1 + P_2$ is the point such that L' intersects $E_{s,p}$ at R and $P_1 + P_2$ (the point symmetric to R with respect to the p-axis).*

Note that one can extend ϕ to the 4-torsion points by $\phi(\mathcal{O}) = \phi(T_2) = \phi(T_4) = \phi(-T_4) = \mathcal{O}_{s,p}$.

Then the following theorem [21] proves that the addition law induced by ϕ is the same as the standard addition law on the elliptic curve, so it corresponds to the addition law described in the above definition 3.3.1.

Theorem 3.3.3. *Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on the Edwards curve and P_3 their sum. Then $\phi(P_3)$ is the sum of $\phi(P_1)$ and $\phi(P_2)$ in the addition law of Definition 3.3.1.*

Then they shows that the map $\phi : E \to E_{s,p}$ is separable of degree 4. Finally they compute 4-th of the Tate pairing in following way:

Let P be an r-torsion point on the Edwards curve. They consider slightly modified functions $f_{i,P}^{(4)}$:

$$\begin{aligned} f_{i,P}^{(4)} = \; & i\left((P) + (P+T_4) + (P+T_2) + (P-T_4)\right) - \left((iP) + (iP+T_4) + (iP-T_2) + (iP-T_4)\right) \\ & -(i-1)\left((\mathcal{O}) + (T_4) + (T_2) + (-T_4)\right) \end{aligned}$$

Then $f_{r,P}^{(4)} = r\left((P) + (P+T_4) + (P+T_2) + (P-T_4)\right) - r\left((\mathcal{O}) + (T_4) + (T_2) + (-T_4)\right)$, which means computing the Tate pairing up to a 4-th power:

$$T_r(P,Q)^4 = f_{i,P}^{(4)}(Q)^{\frac{q^k-1}{r}}.$$

They also got the following Miller equation:

$$f_{i+j,P}^{(4)} = f_{i,P}^{(4)} f_{j,P}^{(4)} \frac{l}{v},$$

where l/v is the function of divisor:

$$\begin{aligned} div(l/v) = & \left((iP) + (iP+T_4) + (iP+T_2) + (iPT_4)\right) \\ & + \left((jP) + (jP+T_4) + (jP+T_2) + (jPT_4)\right) \\ & - \left(((i+j)P) + ((i+j)P+T_4) + ((i+j)P+T_2) + ((i+j)PT_4)\right) \\ & - \left((O) + (T_4) + (T_2) + (T_4)\right). \end{aligned}$$

Method proposed by Bernstein and Lange [26]

Bernstein and Lange [26] used the geometric interpretation of the group law on twisted Edwards curves to propose another method for Tate pairing computations. But first, we require some background on twisted Edwards curve, presented as follows.

In this section K denotes a field of characteristic different from 2. A twisted Edwards curve over K is a curve given by an affine equation of the form $E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$ for $a, d \in K$ and $a \neq d$. Twisted Edwards curves were introduced by Bernstein et al. in [5] as a generalization of Edwards curves [7] which are included as $E_{1,d}$. An addition law on points of the curve $E_{a,d}$ is given by

$$(x_1, y_1), (x_2, y_2) \mapsto \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

The neutral element is $\mathcal{O} = (0, 1)$, and the negative of (x_1, y_1) is $(-x_1, y_1)$. The point $\mathcal{O}' = (0, -1)$ has order 2. The points at infinity $\Omega_1 = (1 : 0 : 0)$ and $\Omega_2 = (0 : 1 : 0)$ are singular and blow up to two points each.

Edwards curves received a lot of attention because the above addition can be computed very efficiently, resulting in highly efficient algorithms to carry out scalar multiplication, a basic tool for many cryptographic protocols.

The name twisted Edwards curves comes from the fact that the set of twisted Edwards curves is invariant under quadratic twists while a quadratic twist of an Edwards curve is not necessarily an Edwards curve. In particular, let $\delta \in K \backslash K_2$ and let $\alpha^2 = \delta$ for some α in a quadratic extension K_2 of K. The map $\epsilon : (x, y) \mapsto (\alpha x, y)$ defines a K_2-isomorphism between the twisted Edwards curves $E_{a\delta,d\delta}$ and $E_{a,d}$. Hence, the map ϵ is the prototype of a quadratic twist. Note that twists change the x-coordinate unlike on Weierstrass curves where they affect the y-coordinate.

Let $\mathbb{P}^2(K)$ be the two-dimensional projective space over K, and let $P = (X_0 : Y_0 : Z_0) \in \mathbb{P}^2(K)$ with $Z_0 \neq 0$. Let $L_{1,P}$ be the line through P and Ω_1, i. e. $L_{1,P}$ is defined by $Z_0Y - Y_0Z = 0$; and let $L_{2,P}$ be the line through P and Ω_2, i. e. $L_{2,P}$ is defined by $Z_0X - X_0Z = 0$.
Let $\phi(X, Y, Z) = c_{X^2}X^2 + c_{Y^2}Y^2 + c_{Z^2}Z^2 + c_{XY}XY + c_{XZ}XZ + c_{YZ}YZ \in K[X, Y, Z]$ be a homogeneous polynomial of degree 2 and $C : \phi(X, Y, Z) = 0$, the associated plane (possibly degenerate) conic. Since the points $\Omega_1, \Omega_2, \mathcal{O}'$ are not on a line, a conic C passing through these points cannot be a double line and ϕ represents C uniquely up to multiplication by a scalar. Evaluating ϕ at $\Omega_1, \Omega_2,$ and $\mathcal{O}'$, we see that a conic C through these points has the form

$$C : c_{Z^2}(Z^2 + YZ) + c_{XY}XY + c_{XZ}XZ = 0 \tag{3.7}$$

where $(c_{Z^2} : c_{XY} : c_{XZ}) \in P^2(K)$.

Theorem 3.3.4. *Let $E_{a,d}$ be a twisted Edwards curve over K, and let $P_1 = (X_1 : Y_1 : Z_1)$ and $P_2 = (X_2 : Y_2 : Z_2)$ be two points on $E_{a,d}(K)$. Let C be the conic passing through $\Omega_1, \Omega_2, \mathcal{O}', P_1,$ and P_2 , i. e. C is given by an equation of the form (3.7). If some of the above points are equal, we consider C and $E_{a,d}$ to intersect with at least that multiplicity at the corresponding point. Then the coefficients in (3.7) of the equation ϕ of the conic C are uniquely (up to scalars) determined as follows:*

(a) If $P_1 \neq P_2, P_1 \neq \mathcal{O}'$ and $P_2 \neq \mathcal{O}'$, then

$$\begin{aligned} c_{Z^2} &= X_1X_2(Y_1Z_2 - Y_2Z_1), \\ c_{XY} &= Z_1Z_2(X_1Z_2 - X_2Z_1 + X_1Y_2 - X_2Y - 1), \\ c_{XZ} &= X_2Y_2Z_1^2 - X_1Y_1Z_2^2 + Y_1Y_2(X_2Z_1 - X_1Z_2). \end{aligned}$$

(b) If $P_1 \neq P_2 = \mathcal{O}'$, then $c_{Z^2} = -X_1, c_{XY} = Z_1, c_{XZ} = Z_1$.
(c) If $P_1 = P_2$, then

$$\begin{aligned} c_{Z^2} &= X_1Z_1(Z_1 - Y_1), \\ c_{XY} &= dX_1^2Y_1 - Z_1^3, \\ c_{XZ} &= Z_1(Z_1Y_1 - aX_1^2). \end{aligned}$$

Let P_1 and P_2 be two K-rational points on a twisted Edwards curve $E_{a,d}$, and let $P_3 = (X_3 : Y_3 : Z_3) = P_1 + P_2$ be their sum. Let

$$l_1 = Z_3Y - Y_3Z, l_2 = X$$

be the polynomials of the horizontal line L_{1,P_3} through P_3 and the vertical line $L_{2,\mathcal{O}}$ through $\mathcal{O}$ respectively,and let

$$\phi = c_{Z^2}(Z^2 + YZ) + c_{XY}XY + c_{XZ}XZ$$

be the unique polynomial (up to multiplication by a scalar) defined by Theorem 3.3.4. The following theorem shows that the group law on a twisted Edwards curve indeed has a geometric interpretation involving the above equations. It gives us an important ingredient to compute Miller functions.

Theorem 3.3.5. *Let $a, d \in K$ with $a \neq d$ and let $E_{a,d}$ be a twisted Edwards curve over K. Let $P_1, P_2 \in E_{a,d}(K)$. Define $P_3 = P_1 + P_2$. Let ϕ, l_1, l_2 be defined as above. Then*

$$div\left(\frac{\phi}{l_1 l_2}\right) \leftrightarrow (P_1) + (P_2) - (P_3) - (\mathcal{O}).$$

Proof. Let us consider the intersection divisor $(C.E_{a,d})$ of the conic $C : \phi = 0$ and the singular quartic $E_{a,d}$. Bezouts Theorem [24] tells us that the intersection of C and $E_{a,d}$ should have $2 \cdot 4 = 8$ points counting multiplicities over K. We note that the two points at infinity Ω_1 and Ω_2 are singular points of multiplicity 2. Moreover, by definition of the conic C, $(P_1) + (P + 2) + (\mathcal{O}') + 2(\Omega_1) + 2(\Omega_2) \leq (C.E_{a,d})$. Hence there is an eighth point Q in the intersection. Let $L_{1,Q} : l_Q = 0$ be the horizontal line going through Q. Since the inverse for addition on twisted Edwards curves is given by $(x, y) \mapsto (-x, y)$, we see that $(L_{1,Q}.E_{a,d}) = (Q) + (-Q) - 2(\Omega_2)$. On the other hand $(L_{2,\mathcal{O}}.E_{a,d}) = (\mathcal{O}) + (\mathcal{O}') - 2(\Omega_1)$. Hence by combining the above divisors we get $div\left(\frac{\phi}{l_1 l_2}\right) \leftrightarrow (P_1) + (P_2) - (-Q) - (\mathcal{O})$. By unicity of the group law with neutral element $\mathcal{O}$ on the elliptic curve $E_{a,d}$, the last equality means that $P_3 = -Q$. Hence $(L_{1,P_3}E_{a,d}) = (P_3)+(-P_3)-2(\Omega_2) = (-Q)+(Q)-2(\Omega_2)$ and $l_1 = l_Q$. So $div\left(\frac{\phi}{l_1 l_2}\right) \leftrightarrow (P_1)+(P_2)-(P_3)-(\mathcal{O})$ □

One can notice that $P_1 + P_2$ is obtained as the mirror image with respect to the y-axis of the eighth intersection point of $E_{a,d}$ and the conic C passing through $\Omega_1, \Omega_2, \mathcal{O}', P_1$, and P_2.

And finally they provide efficient formulas for Pairings on Edwards Curves. They use the geometric interpretation of the group law to compute pairings. For that they assume that k is even and that the second input point Q is chosen by using the tricks in [1]: Let $\mathbb{F}_{q^k}$ have basis $\{1, \alpha\}$ over $\mathbb{F}_{q^{k/2}}$ with $\alpha^2 = \delta \in \mathbb{F}_{q^{k/2}}$ and let $Q' = (X_0 : Y_0 : Z_0) \in E_{a\delta,d\delta}(\mathbb{F}_{q^{k/2}})$. Twisting Q' with α ensures that the second argument of the pairing is on $\mathbb{F}_{q^k}$ (and no smaller field) and is of the form $Q = (X_0\alpha : Y_0 : Z_0)$, where $X_0, Y_0, Z_0 \in \mathbb{F}_{q^{k/2}}$.

By the theorem 3.3.5, one can also say that $g_{R,S} = \frac{\phi}{l_1 l_2}$. In each step of the Miller loop first $g_{R,S}$ is computed, it is then evaluated at $Q = (X_0\alpha : Y_0 : Z_0)$ and finally f is updated as $f \leftarrow f g_{R,P}(Q)$ (addition) or as $f \leftarrow f^2 g_{R,R}(Q)$ (doubling). Given the shape of ϕ and the point $Q = (X_0\alpha : Y_0 : Z_0)$, we need to compute

$$\begin{aligned}\frac{\phi}{l_1 l_2}(X_0\alpha : Y_0 : Z_0) &= \frac{c_{Z^2}(Z_0^2 + Y_0 Z_0) + c_{XY} X_0 \alpha Y_0 + c_{XZ} X_0 Z_0 \alpha}{(Z_3 Y_0 - Y_3 Z_0) X_0 \alpha} \\ &= \frac{c_{Z^2}\frac{Z_0+Y_0}{X_0\delta}\alpha + c_{XY} y_0 + c_{XZ}}{Z_3 y_0 - Y_3} \\ &\in (c_{Z^2}\eta\alpha + c_{XY} y_0 + c_{XZ})\mathbb{F}^*_{q^{k/2}},\end{aligned}$$

where $(X_3 : Y_3 : Z_3)$ are coordinates of the point $R + P$ or $R + R$, $y_0 = Y_0/Z_0$, and $\eta = (Z_0 + Y_0)/X_0\delta$. Note that $\eta, y_0 \in \mathbb{F}_{q^{k/2}}$ and that they are fixed for the whole computation, so they can be precomputed. The coefficients c_{Z^2}, c_{XY}, and c_{XZ} are defined over $\mathbb{F}_q$, thus the evaluation at Q given the coefficients of the conic can be computed in km (multiplications by η and y_0 need $\frac{k}{2}$ m each).

Then they used the technique of addition formulas for twisted Edawrds curves from [4]. They compute line function and addition of two points and line function and doubling of a point at the same time in Miller's algorithm. Their approach is significantly faster than previous two works.

Chapter 4

Conclusion

We have proposed unified addition formula in Weierstrass form elliptic curves. Then we explicitly computes addition and doubling cost in three different coordinates namely, affine, Projective and Jacobian. From the comparison we conclude that the cost of addition and doubling is more than the usual addition and doubling in Projective and Jacobian coordinates. But its very close to the cost in affine coordinates. Readers should remember that our formula is strongly unified and strongly unified formula prevents side-channel attacks. So it is quite expected that the costs would be more.

Peoples are more interested in Edwards form elliptic curves as the addition formula in Edwards curves is simple and symmetric and one of the attractive features of the Edwards addition law is that it is strongly unified. Even Bernstein and Lange showed in [26] that, when curve parameters are chosen properly, the addition law is even complete, means it works for all inputs, with no exceptional cases, simplifying side-channel attacks. But handling with elliptic curves in Weierstrass form is much more easy than Edwards curves. As an example, one can consider pairing computation on elliptic curves. Computation of the line function in Miller's Algorithm is very easy and can be computed very efficiently by chord-tangent method, but in Edwards curves it is not so easy [22] as the degree of the curve is 4. Barreto et. all [1] efficiently computes Tate pairing on supersingular elliptic curves of embedding degree $k = 2, 4, 6$. So if unified formula is available in Weierstrass form elliptic curves then people would not be worry about side-channel attacks. Note that unified laws are useful even if slower than Edwards!

For further study, one may think about computing Tate pairing in elliptic curves with this unified addition formula. In 2005, Chatterjee, Sarkar, and Barua [19] introduce a nice idea for computing Tate pairing in Projective coordinates over general characteristic fields. One can try this approach with our unified addition formula.

Bibliography

[1] Barreto, P.S.L.M., Kim, H.Y., Lynn, B., Scott. Efficient algorithms for pairing-based cryptosystems. In Yung, M. (ed) CRYPTO 2002. LNCS, vol. 2442, pp. 354-369. Spinger, Heidelberg(2002).

[2] Daniel J. Bernstein and Tanja Lange. Faster addition and doubling on elliptic curves. In Asiacrypt 2007 [10], pages 2950, 2007. http://cr.yp.to/newelliptic/.

[3] Daniel J. Bernstein, P. Birkner, T. Lange and C. Peters. Twisted Edwards curve. AFRICACRYPT 2008. ePrint Archive, 2008(013).

[4] Huseyin Hisil, Kenneth Koon-HoWong, Gary Carter, and Ed Dawson. Twisted Edwards curves revisited. In ASIACRYPT 2008 [30], pages 326343, 2008.

[5] D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. In Advances in Cryptology-CRYPTO 2001, LNCS 2218, pp. 213-229, Springer-Verlag 2001.

[6] D. Boneh, B. Lynn and Hovav Shacham. Short Signatures from the Weil pairing. In Colin Boyd, editor, Advances in Cryptology $-ASIACRYPT2001$.

[7] D. Boneh, B. Lynn and H. Shacham. Group Signatures with verifier-local revocation. In Vijayalakshmi Atluri, Bigrit Pftizmann and Patrick McDaniel, pages 168 − 177, ACM press, 2004.

[8] Antoine Joux. A one round protocol for tripartite Diffie-Hellmann. Journal of cryptology, 17(4):235-261, September 2004.

[9] Vassil Dimitrov, Laurent Imbert, and Pradeep K. Mishra. Efficient and secure elliptic curve point multiplication using double-base chains. In ASIACRYPT 2005, PAGES 59-78, 2005.

[10] Harold M. Edwards. A normal form for elliptic curves. Bulletin of the American Mathematical Society, 44:393422, 2007. http://www.ams.org/bull/2007-44-03/S0273-0979-07-01153-6/home.html.

[11] N. Koblitz. Introduction To Elliptic Curves And Modular Forms, Second Edition. Springer.

[12] N. Koblitz. Elliptic curve cryptosystems. Mathematics of Computation 48, 1987, pp. 203-209.

[13] V. Miller. Use of elliptic curves in cryptography, CRYPTO 85, 1985.

[14] V. Miller. The Weil pairing and its efficient calculation. J. Cryptology 17(4), 235-261, 2004.

[15] R. Sakai, K. Ohgishi and M. Kasahara. Cryptosystems Based on Pairing. In Symposium on Cryptography and Information Security-SCIS, 2000

[16] A. Shamir. Identity Based Cryptosystems and Signature Schemes. In Advances in Cryptology-CRYPTO 1984, LNCS 196, pp. 47-53, Springer Verlag 1984.

[17] Lawrence C. Washington. ELLIPTIC CURVES : Number Theory and Cryptography. CHAPMAN & HALL/CRC, 2003.

[18] Yuliang Zheng, and Hideki Imai. How to construct efficient signcryption schemes on elliptic curves. Information Processing Letters, Vol.68, pp.227-233, Elsevier Inc., 1998.

[19] Sanjit Chatterjee, Palash Sarkar, and Rana Barua. Efficient computation of Tate pairing in Projective coordinate over general characteristic fields. In ICISC 2004 [29], pages 168181, 2005.

[20] M. Prem Laxman Das and Palash Sarkar. Pairing computation on twisted Edwards form elliptic curves. In Pairing 2008 [19], pages 192-210, 2008.

[21] Sorina Ionica and Antoine Joux. Another approach to pairing computation in Edwards coordinates. In INDOCRYPT 2008 [10], pages 400-413, 2008. http://eprint.iacr.org/2008/292

[22] C. Arene, T. Lange, M. Naehrig, and C. Ritzenthaler. Faster computation of the Tate pairing. ECRYPT II

[23] D. Hankerson, A. Menezes, and S. Vanstone. Guide to Elliptic Curve Cryptography. Springer.

[24] William Fulton. Algebraic Curves. W. A. Benjamin, Inc., 1969.

[25] D. J. Bernstein, and T. Lange. Inverted Edwards coordinates. http://eprint.iacr.org/2007/410.pdf

[26] D. J. Bernstein, and T. Lange. Faster addition and doubling on elliptic curves. In Asiacrypt 2007 [10], pages 2950, 2007. http://cr.yp.to/newelliptic/.

[27] D. J. Bernstein, and T. Lange. Explicit-formulas database. Accessible through: http://hyperelliptic.org/EFD (2007)

[28] Brier, E., Dechene, I., Joye, M. Unified point addition formulae for elliptic curve cryptosystems. Embedded Cryptographic Hardware: Methodologies and Architectures. Nova Science Publishers (2004) 247256