Tower Building Technique on Elliptic Curve with Embedding Degree 54

ASSOUJAA ISMAIL, EZZOUAK SIHAM
Sidi Mohammed Ben Abdellah University
Faculty of science Dhar El Mahrez
Department of mathematics, Lab: LASMA
Fez, MOROCCO.

Abstract: Pairing based cryptography is one of the newest security solution that attract a lot of attention, because we can work with efficient and faster pairing to make the security a lot practical, also the working with extension finite field of the form $\mathbb{F}p^k$ is more useful and secure with $k \geq 12$ the implementation become more important. In this paper, we will presents cases studies of improving pairing arithmetic calculation on curves with embedding degree 54. We use the tower building technique, and study the case when using a degree 3 twist to carry out most operations in $\mathbb{F}p^3$ and $\mathbb{F}p^6$ or $\mathbb{F}p^9$ and $\mathbb{F}p^{18}$ or $\mathbb{F}p^{27}$, or when using a degree 2 twist to handle most of the operations in $\mathbb{F}p^2$ and $\mathbb{F}p^6$ and $\mathbb{F}p^{18}$.

Key-Words: —Optimal ate pairing, Miller Algorithm, Embedding degree 54, Twist curve

Received: April 22, 2024. Revised: September 13, 2024. Accepted: October 14, 2024. Published: November 14, 2024.

1. Introduction

After the discovering of pairing-based cryptography, developers and researchers have been studding and developing new techniques and methods for constructing more efficiently implementation of pairings protocols and algorithms.The first pairing is introduced by Weil Andre in 1948 called Weil pairing, after that more pairing are appear like tate pairing, ate pairing and a lot more. The benefice of Elliptic curve cryptosystems which was discovered by Neal Koblitz [1] and Victor Miller [2] are to reduce the key sizes of the keys utilize in public key cryptography. Some works like presented in [3] interested in signature numeric. The authors in [4] show that we can use the final exponentiation in pairings as one of the countermeasures against fault attacks. In [5], [6], [7], [13] Nadia El and others show a study case of working with elliptic curve with embedding degree 5,9,15 and 27. Also in [9], [10], [11], [12] researchers show the case of working with curve with embedding degree 18. In [8] they give a study of security level of optimal ate pairing.

In the present article, we seek to obtain efficient ways to pairing computation for curves of embedding degree 54. We will see how to improve arithmetic operation in curves with embedding degree 54 by using the tower building technique. We will give three cases studies that show, when we use a degree 2 twists, we can handle most operations in $\mathbb{F}_{p^2}$, $\mathbb{F}_{p^6}$ and $\mathbb{F}_{p^{18}}$, and when we use a degree 3 twists, we can handle most operations in $\mathbb{F}_{p^3}$, $\mathbb{F}_{p^6}$, $\mathbb{F}_{p^9}$, $\mathbb{F}_{p^{18}}$ and $\mathbb{F}_{p^{27}}$ instead. By making use of an tower building technique, we also improve the arithmetic of $\mathbb{F}_{p^6}$, $\mathbb{F}_{p^{18}}$ and $\mathbb{F}_{p^{54}}$ in order to get better results. Finally we will compare these cases to know which path is the optimal path.

In this paper, we will investigate and examine what will happens in case of optimal ate pairing with embedding degree 54.

The paper is organized as follow. Section 2 we recall some background on the main pairing proprieties also ate pairing, and Miller Algorithm. Section 3 presents our main theorem in this work. Section 4 will presents the results of our work. Finally, Section 5 concludes this paper.

2. Mathematical Background

In everything that follows, E will represent an elliptic curve with equation
$y^2 = x^3 + ax + b$ for $b \in \mathbb{F}_q$ with q prime number. The symbol a_{opt} will denote the optimal ate pairing. We shall use, without explicit mention, the following :

- $\mathbb{G}_1 \subset (E(\mathbb{F}_q))$: additive group of cardinal $n \in \mathbb{N}^*$.
- $\mathbb{G}_2 \subset (E(\mathbb{F}_{q^k}))$: additive group of cardinal $n \in \mathbb{N}^*$.
- $\mathbb{G}_3 \subset \mathbb{F}^*_{q^k} \subset \mu_n$: cyclic multiplicative group of cardinal $n \in \mathbb{N}^*$.
- $\mu_n = \{u \in \bar{\mathbb{F}_q} | u^n = 1\}$.
- P_∞ : the point at infinity of the elliptic curve.
- k : the embedding degree: the smallest integer such that r divides $q^k - 1$.
- $f_{s,P}$: a rational function associated to the point P and some integer s.
- m,s,i: multiplication, squaring, inversion in field $\mathbb{F}_p$.
- M_2, S_2, I_2: multiplication, squaring, inversion in field $\mathbb{F}_{p^2}$.
- M_3, S_3, I_3: multiplication, squaring, inversion in field $\mathbb{F}_{p^3}$.
- M_6, S_6, I_6: multiplication, squaring, inversion in field $\mathbb{F}_{p^6}$.
- M_9, S_9, I_9: multiplication, squaring, inversion in field $\mathbb{F}_{p^9}$.
- M_{18}, S_{18}, I_{18}: multiplication, squaring, inversion in field $\mathbb{F}_{p^{18}}$
- M_{27}, S_{27}, I_{27}: multiplication, squaring, inversion in field $\mathbb{F}_{p^{27}}$.

- M_{54}, S_{54}, I_{54}: multiplication, squaring, inversion in field $\mathbb{F}_{p^{54}}$

Remark 1: In this paper, our main objective is to identify the optimal path with the lowest cost. Although the cost of multiplication remains the same in each path we choose, we aim to determine the path with the minimum cost of squaring or inversion.

Proposition 1:
We investigate these cases by following the process outlined below:

1) Transform the elliptic curve with embedding degree k using the variable change $(x, y) \to (xu^{2/d}, yu^{3/d})$
2) Choose an appropriate irreducible polynomial for tower building
3) Construct the twisted isomorphic rational point
4) Determine the cost of multiplication, squaring, and inversion in the corresponding field.

Twist of an Elliptic Curve

Definition 1: (Twist of an elliptic curve) [6]
Let E and E' be two elliptic curves defined over $\mathbb{F}_q$, for q, a power of a prime number p. Then, the curve E' is a twist of degree d of E if we can define an isomorphism Ψ_d over $\mathbb{F}_{q^d}$ from E' into E and such that d is minimal:

$$\Psi_d : E'(\mathbb{F}_q) \to E(\mathbb{F}_{q^d}).$$

Theorem 1: [6] Let E be an elliptic curve defined by the short Weiestrass equation $y^2 = x^3 + ax + b$ over an extension $\mathbb{F}_q$ of a finite field $\mathbb{F}_p$, for p a prime number, k a positive integer such that $q = p^k$. According to the value of k, the potential degrees for a twist are d =2, 3, 4 or 6 (in this paper, we are intersted with the case of d=2 and 3).

• $d = 2$, Let $v \in \mathbb{F}_{p^{k/2}}$ such that the polynomial $X^2 - v$ is irreducible in $\mathbb{F}_{p^{k/2}}$. The equation of the curve E' defined on $\mathbb{F}_{p^{k/2}}$ is $E' : vy^2 = x^3 + ax + b$. The morphism Ψ_2 is defined by:

$$\begin{aligned} \Psi_2 : E'(\mathbb{F}_{p^{k/2}}) &\longrightarrow E(\mathbb{F}_{p^k}) \\ (x, y) &\longrightarrow (x, yv^{1/2}) \end{aligned}$$

• $d = 3$, the curve E admits a twist of degree 3 if and only $a = 0$. Let $v \in \mathbb{F}_{p^{k/d}}$ be such that the polynomial $X^3 - v$ is irreducible in $\mathbb{F}_{p^{k/d}}$. The equation of E' is then $y^2 = x^3 + \frac{b}{v}$. The morphism is:

$$\begin{aligned} \Psi_3 : E'(\mathbb{F}_{p^{k/3}}) &\longrightarrow E(\mathbb{F}_{p^k}) \\ (x, y) &\longrightarrow (xv^{1/3}; yv^{1/2}) \end{aligned}$$

Cost calculation:
We use the cost of operation in Quadratic and cubic twisted curve to calculate the cost of operation in the field with embedding degree $2^i.3$ with the tower building technique for every path.

• Cost of operation in Quadratic twisted curve:
We already know that the cost of multiplication, squaring and inversion in the quadratic field $\mathbb{F}_{p^2}$ are:
$M_2 = 3m$, $S_2 = 2m$, $I_2 = 4m + i$ respectively ([17]).

• Cost of operation in Cubic twisted curve:
We already know that the cost of multiplication, squaring and inversion in in the cubic twisted field $\mathbb{F}_{p^3}$ are:
$M_3 = 6m$, $S_3 = 5s$, $I_3 = 9m + 2s + i$ respectively ([17]).

Vector representation point:
In order to construct a vector representation point in $\mathbb{F}_{p^k}$, we generally need the following set forms a basis of $\mathbb{F}_{p^k}$ over $\mathbb{F}_p$, $B_k = \{1, u, u^2, ..., u^{k-1}\}$, which is known as polynomial basis. An arbitrary element A in $\mathbb{F}_{p^k}$ is written as $A = a_0 + a_1u + a_2u^2 + ... + a_{k-1}u^{k-1}$. The vector representation of A is $v_A = (a_0, a_1, a_2, ..., a_{k-1})$.
We use the vector representation point of Quadratic and cubic twisted curve to know the vector representation point of operation in the field with embedding degree $2^i.3$ with the tower building technique for every path.

Vector representation point in Quadratic twisted curve:
We have E is $y^2 = x^3 + ax + b$.
Let $u \in \mathbb{F}_p$ such that the polynomial $x^2 - u$ is irreducible over $\mathbb{F}_p$.
The equation of E' is $uy^2 = x^3 + ax + b$.
So to map $E(\mathbb{F}_p)$ to $E'(\mathbb{F}_p)$,we have:

$$\begin{aligned} E(\mathbb{F}_p) &\to E'(\mathbb{F}_p) \\ (x, y) &\to (x_1, y_1) = (x, yu^{1/2}) \end{aligned}$$

Using $\psi_2(x, y) = (x, yu^{1/2})$ to map $E'(\mathbb{F}_p)$ to $E(\mathbb{F}_{p^2})$

$$\begin{aligned} E'(\mathbb{F}_p) &\to E(\mathbb{F}_{p^2}) \\ (x, y) &\to (x, yu^{1/2}) \end{aligned}$$

Hence, to map $E(\mathbb{F}_p)$ to $E(\mathbb{F}_{p^2})$, we have:

$$\begin{aligned} E(\mathbb{F}_p) &\to E(\mathbb{F}_{p^2}) \\ (x, y) &\to (x_1, y_1) = (x, yu) \end{aligned}$$

• Let map P to P_1:
Let $P = (x, y) = (a, b)$ and $P_1 = (x_1, y_1) = (a_1, b_1)_{B_2}$, where $x_1, y_1, a_1, b_1 \in \mathbb{F}_{p^2}$.
P_1 has a special vector representation with 2 $\mathbb{F}_p$ elements for each x_1 and y_1 coordinates. We have $B_2 = (1, u)$, $\psi_2 : E'(\mathbb{F}_p) \to E(\mathbb{F}_{p^2})$,
$\psi_2(x, y) = (x_1, y_1) = (x, yu)$, (see [9]) we have:

$$\begin{aligned} P &\to P_1 \\ E(\mathbb{F}_p) &\to E(\mathbb{F}_{p^2}) \\ (x, y) &\to (x_1, y_1) = (x, yu) = (a, bu)_{B_2} \end{aligned}$$
$$P_1 = (x_1, y_1) = (x, yu) = (a, bu)_{B_2} = ((a, 0), (0, b))$$

• Let remap P_1 to P: obtained easily by just placing a and b in the correct basis position.

$$\begin{aligned} P_1 &\to P \\ E(\mathbb{F}_{p^2}) &\to E(\mathbb{F}_p) \\ (x_1, y_1) &\to (x, y) = (a, b) \\ P &= (x, y) = (a, b) \end{aligned}$$

So we can easly map and remap between P and P_1.

Vector representation point in Cubic twisted curve:

The curve E admits a twist of degree 3 if and only if $a = 0$ i,e $y^2 = x^3 + b$.
Let $u \in \mathbb{F}_p$ such that the polynomial $x^3 - u$ is irreducible over $\mathbb{F}_p$.
The equation of E' is $y^2 = x^3 + b/u$.
So to map $E(\mathbb{F}_p)$ to $E'(\mathbb{F}_p)$,we have:

$$\begin{aligned} E(\mathbb{F}_p) &\to E'(\mathbb{F}_p) \\ (x, y) &\to (x_1, y_1) = (xu^{1/3}, yu^{1/2}) \end{aligned}$$

Using $\psi_3(x, y) = (xu^{2/3}, yu^{1/2})$ to map $E'(\mathbb{F}_p)$ to $E(\mathbb{F}_{p^3})$

$$\begin{aligned} E'(\mathbb{F}_p) &\to E(\mathbb{F}_{p^3}) \\ (x, y) &\to (xu^{2/3}, yu^{1/2}) \end{aligned}$$

Hence, to map $E(\mathbb{F}_p)$ to $E(\mathbb{F}_{p^3})$, we have:

$$\begin{aligned} E(\mathbb{F}_p) &\to E(\mathbb{F}_{p^3}) \\ (x, y) &\to (x_1, y_1) = (xu, yu) \end{aligned}$$

• Let map P to P_1:
Let $P = (x, y) = (a, b)$ and $P_1 = (x_1, y_1) = (a_1, b_1)_{B_3}$, where $x_1, y_1, a_1, b_1 \in \mathbb{F}_{p^3}$.
P_1 has a special vector representation with 3 $\mathbb{F}_p$ elements for each x_1 and y_1 coordinates.
We have $B_3 = (1, u, u^2)$, $\psi_3 : E'(\mathbb{F}_p) \to E(\mathbb{F}_{p^3})$,
$\psi_3(x, y) = (x_1, y_1) = (xu, yu)$, (see [9]) we have:

$$\begin{aligned} P &\to P_1 \\ E(\mathbb{F}_p) &\to E(\mathbb{F}_{p^3}) \\ (x, y) &\to (x_1, y_1) = (xu, yu) = (au, bu)_{B_3} \\ P_1 = (x_1, y_1) &= (xu, yu) = (au, bu)_{B_3} = ((0, a, 0), (0, b, 0)) \end{aligned}$$

• Let remap P_1 to P: obtained easily by just placing a and b in the correct basis position

$$\begin{aligned} P_1 &\to P \\ E(\mathbb{F}_{p^3}) &\to E(\mathbb{F}_p) \\ (x_1, y_1) &\to (x, y) = (a, b) \\ P = (x, y) &= (a, b) \end{aligned}$$

So we can easly map and remap between P and P_1.

Corollary 1: :
We can do an extension for the above vector representation, we have:

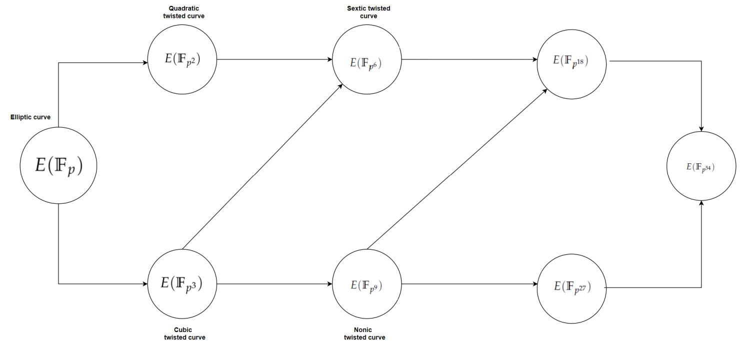
$$\begin{aligned} E(\mathbb{F}_{p^{k/2}}) &\to E(\mathbb{F}_{p^k}) \\ (x, y) &\to (x, yu) \end{aligned}$$

and,

$$\begin{aligned} E(\mathbb{F}_{p^{k/3}}) &\to E(\mathbb{F}_{p^k}) \\ (x, y) &\to (xu, yu) \end{aligned}$$

3. Tower Building Technique for Elliptic Curve with Embedding Degree 54

The figure below show all path possible for building an elliptic curve with embedding degree 54

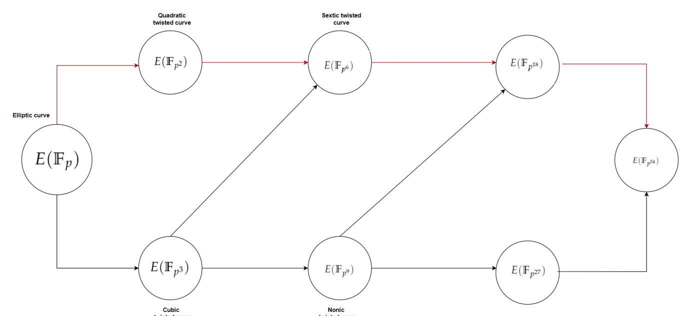


There is four path possible to building this curve

$$\begin{aligned} &\mathbb{F}_p \longrightarrow \mathbb{F}_{p^2} \longrightarrow \mathbb{F}_{p^6} \longrightarrow \mathbb{F}_{p^{18}} \longrightarrow \mathbb{F}_{p^{54}} \\ &\mathbb{F}_p \longrightarrow \mathbb{F}_{p^3} \longrightarrow \mathbb{F}_{p^6} \longrightarrow \mathbb{F}_{p^{18}} \longrightarrow \mathbb{F}_{p^{54}} \\ &\mathbb{F}_p \longrightarrow \mathbb{F}_{p^3} \longrightarrow \mathbb{F}_{p^9} \longrightarrow \mathbb{F}_{p^{18}} \longrightarrow \mathbb{F}_{p^{54}} \\ &\mathbb{F}_p \longrightarrow \mathbb{F}_{p^3} \longrightarrow \mathbb{F}_{p^9} \longrightarrow \mathbb{F}_{p^{27}} \longrightarrow \mathbb{F}_{p^{54}} \end{aligned}$$

Exploring the first path

$$\mathbb{F}_p \longrightarrow \mathbb{F}_{p^2} \longrightarrow \mathbb{F}_{p^6} \longrightarrow \mathbb{F}_{p^{18}} \longrightarrow \mathbb{F}_{p^{54}}$$



The appropriate choices of irreducible polynomial defined by:

$$\mathbb{F}_{p^2} = \mathbb{F}_p[u]/(u^2 - \beta), \text{ with } \beta \text{ a non-square and } u^2 = 2$$

$$\mathbb{F}_{p^6} = \mathbb{F}_{p^2}[v]/(v^3 - u), \text{ with } v \text{ a non-cube and } v^3 = 2^{1/2}$$

$$\mathbb{F}_{p^{18}} = \mathbb{F}_{p^6}[t]/(t^3 - v), \text{ with } t \text{ a non-cube and } t^3 = 2^{1/6}$$

$$\mathbb{F}_{p^{54}} = \mathbb{F}_{p^{18}}[w]/(w^3 - t), \text{ with } w \text{ a non-cube and } w^3 = 2^{1/18}$$

$$\begin{aligned} P^4(x^4, y^4) &= ((a, 0, ..., 0), (0, ..., 0, b)) \text{ with } x^4, y^4 \in \mathbb{F}_{p^{54}} \\ P'''(x''', y''') &= ((a, 0, ..., 0), (0, ..., 0, b)) \text{ with } x''', y''' \in \mathbb{F}_{p^{18}} \\ P''(x'', y'') &= ((a, 0, 0, 0, 0, 0), (0, 0, 0, 0, 0, b)) \text{ with } x'', y'' \in \mathbb{F}_{p^6} \\ P'(x', y') &= ((a, 0), (0, b)) \text{ with } x', y' \in \mathbb{F}_{p^2} \\ P(x, y) &= (a, b) \text{ with } x, y \in \mathbb{F}_p \end{aligned}$$

The cost of multiplication, squaring and inversion in in the 54^{th} twisted field $\mathbb{F}_{p^{54}}$ are:

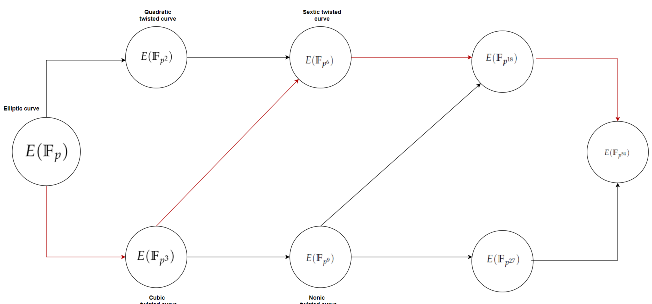
$$\begin{aligned} M_{54} &= (M_{18})_{\mathbb{F}_{p^3}} = (M_6)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = ((M_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} \\ &= ((3m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = ((3M_3)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = ((18m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} \\ &= (18M_3)_{\mathbb{F}_{p^3}} = (108m)_{\mathbb{F}_{p^3}} = 108M_3 = 648m, \end{aligned}$$

$$\begin{aligned} S_{54} &= (S_{18})_{\mathbb{F}_{p^3}} = (S_6)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = ((S_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} \\ &= ((2m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = ((2M_3)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = ((12m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} \\ &= (12M_3)_{\mathbb{F}_{p^3}} = (72m)_{\mathbb{F}_{p^3}} = 72M_3 = 432m, \end{aligned}$$

$$\begin{aligned} I_{54} &= (I_{18})_{\mathbb{F}_{p^3}} = (I_6)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = ((I_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} \\ &= ((4m+i)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = ((4M_3+I_3)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} \\ &= ((33m+2s+i)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = (33M_3+2S_3+I_3)_{\mathbb{F}_{p^3}} \\ &= (207m+12s+i)_{\mathbb{F}_{p^3}} = 207M_3+12S_3+I_3 \\ &= 1251m+62s+i, \end{aligned}$$

Exploring the second path

$$\mathbb{F}_p \longrightarrow \mathbb{F}_{p^3} \longrightarrow \mathbb{F}_{p^6} \longrightarrow \mathbb{F}_{p^{18}} \longrightarrow \mathbb{F}_{p^{54}}$$



The appropriate choices of irreducible polynomial defined by:

$$\mathbb{F}_{p^3} = \mathbb{F}_p[u]/(u^3-\beta), \text{ with } \beta \text{ a non-cube and } u^3 = 2$$

$$\mathbb{F}_{p^6} = \mathbb{F}_{p^3}[v]/(v^2-u), \text{ with } v \text{ a non-square and } v^2 = 2^{1/3}$$

$$\mathbb{F}_{p^{18}} = \mathbb{F}_{p^6}[t]/(t^3-v), \text{ with } t \text{ a non-cube and } t^3 = 2^{1/6}$$

$$\mathbb{F}_{p^{54}} = \mathbb{F}_{p^{18}}[w]/(w^3-t), \text{ with } w \text{ a non-cube and } w^3 = 2^{1/18}$$

$$\begin{aligned} P^4(x^4,y^4) &= ((a,0,...,0),(0,...,0,b)) \text{ with } x^4,y^4 \in \mathbb{F}_{p^{54}} \\ P'''(x''',y''') &= ((a,0,...0),(0,...,0,b)) \text{ with } x''',y''' \in \mathbb{F}_{p^{18}} \\ P''(x'',y'') &= ((a,0,0,0,0,0),(0,0,0,0,0,b)) \quad x'',y'' \in \mathbb{F}_{p^6} \\ P'(x',y') &= ((a,0,0),(0,0,b)) \text{ with } x',y' \in \mathbb{F}_{p^3} \\ P(x,y) &= (a,b) \text{ with } x,y \in \mathbb{F}_p \end{aligned}$$

The cost of multiplication, squaring and inversion in in the 54^{th} twisted field $\mathbb{F}_{p^{54}}$ are:

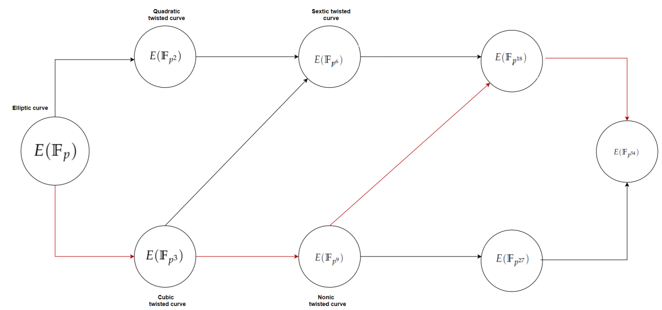
$$\begin{aligned} M_{54} &= (M_{18})_{\mathbb{F}_{p^3}} = (M_6)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = ((M_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} \\ &= ((6m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = ((6M_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = ((18m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} \\ &= (18M_3)_{\mathbb{F}_{p^3}} = (108m)_{\mathbb{F}_{p^3}} = 108M_3 = 648m, \end{aligned}$$

$$\begin{aligned} S_{54} &= (S_{18})_{\mathbb{F}_{p^3}} = (S_6)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = ((S_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = ((5s)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} \\ &= ((5S_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = ((10m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = (10M_3)_{\mathbb{F}_{p^3}} = (60m)_{\mathbb{F}_{p^3}} \\ &= 60M_3 = 360m, \end{aligned}$$

$$\begin{aligned} I_{54} &= (I_{18})_{\mathbb{F}_{p^3}} = (I_6)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = ((I_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} \\ &= ((9m+2s+i)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = ((9M_2+2S_2+I_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} \\ &= ((35m+i)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = (35M_3+I_3)_{\mathbb{F}_{p^3}} = (219m+2s+i)_{\mathbb{F}_{p^3}} \\ &= 219M_3+2S_3+I_3 = 1323m+12s+i, \end{aligned}$$

Exploring the third path

$$\mathbb{F}_p \longrightarrow \mathbb{F}_{p^3} \longrightarrow \mathbb{F}_{p^9} \longrightarrow \mathbb{F}_{p^{18}} \longrightarrow \mathbb{F}_{p^{54}}$$



The appropriate choices of irreducible polynomial defined by:

$$\mathbb{F}_{p^3} = \mathbb{F}_p[u]/(u^3-\beta), \text{ with } \beta \text{ a non-cube and } u^3 = 2$$

$$\mathbb{F}_{p^9} = \mathbb{F}_{p^3}[v]/(v^3-u), \text{ with } v \text{ a non-cube and } v^3 = 2^{1/3}$$

$$\mathbb{F}_{p^{18}} = \mathbb{F}_{p^9}[t]/(t^2-v), \text{ with } t \text{ a non-square and } t^2 = 2^{1/9}$$

$$\mathbb{F}_{p^{54}} = \mathbb{F}_{p^{18}}[w]/(w^3-t), \text{ with } w \text{ a non-square and } w^3 = 2^{1/18}$$

$$\begin{aligned} P^4(x^4,y^4) &= ((a,0,...,0),(0,...,0,b)) \text{ with } x^4,y^4 \in \mathbb{F}_{p^{54}} \\ P'''(x''',y''') &= ((a,0,...,0),(0,...,0,b)) \text{ with } x''',y''' \in \mathbb{F}_{p^{18}} \\ P''(x'',y'') &= ((a,0,...,0),(0,,...,0,b)) \text{ with } x'',y'' \in \mathbb{F}_{p^9} \\ P'(x',y') &= ((a,0,0),(0,0,b)) \text{ with } x',y' \in \mathbb{F}_{p^3} \\ P(x,y) &= (a,b) \text{ with } x,y \in \mathbb{F}_p \end{aligned}$$

The cost of multiplication, squaring and inversion in in the 36^{th} twisted field $\mathbb{F}_{p^{36}}$ are:

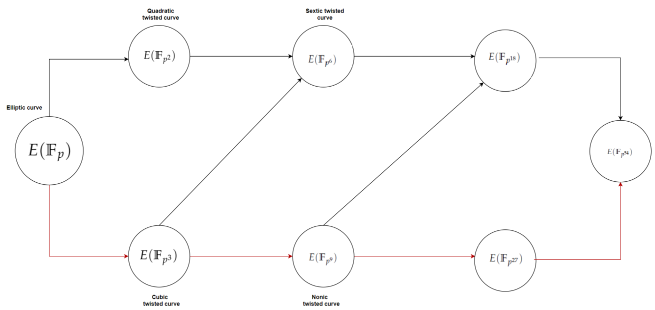
$$\begin{aligned} M_{54} &= (M_{18})_{\mathbb{F}_{p^3}} = (M_9)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = ((M_3)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\ &= ((6m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = ((6M_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = ((36m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\ &= (36M_2)_{\mathbb{F}_{p^3}} = (108m)_{\mathbb{F}_{p^3}} = 108M_3 = 648m, \end{aligned}$$

$$\begin{aligned} S_{54} &= (S_{18})_{\mathbb{F}_{p^3}} = (S_9)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = ((S_3)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = ((5s)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\ &= ((5S_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = ((25s)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\ &= (25S_2)_{\mathbb{F}_{p^3}} = (50m)_{\mathbb{F}_{p^3}} = 50M_3 = 300m, \end{aligned}$$

$$
\begin{aligned}
I_{54} &= (I_{18})_{\mathbb{F}_{p^3}} = ((I_9)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = (((I_3)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\
&= (((9m + 2s + i)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = ((9M_3 + 2S_3 + I_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\
&= ((63m + 12s + i)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = (63M_2 + 12S_2 + I_2)_{\mathbb{F}_{p^3}} \\
&= (227m + i)_{\mathbb{F}_{p^3}} = 227M_3 + I_3 = 1371m + 2s + i,
\end{aligned}
$$

Exploring the forth path

$$
\mathbb{F}_p \longrightarrow \mathbb{F}_{p^3} \longrightarrow \mathbb{F}_{p^9} \longrightarrow \mathbb{F}_{p^{27}} \longrightarrow \mathbb{F}_{p^{54}}
$$



The appropriate choices of irreducible polynomial defined by:

$$
\begin{aligned}
\mathbb{F}_{p^3} &= \mathbb{F}_p[u]/(u^3 - \beta), \text{ with } \beta \text{ a non-cube and } u^3 = 2 \\
\mathbb{F}_{p^9} &= \mathbb{F}_{p^3}[v]/(v^3 - u), \text{ with } v \text{ a non-cube and } v^3 = 2^{1/3} \\
\mathbb{F}_{p^{27}} &= \mathbb{F}_{p^9}[t]/(t^3 - v), \text{ with } t \text{ a non-cube and } t^3 = 2^{1/9} \\
\mathbb{F}_{p^{54}} &= \mathbb{F}_{p^{27}}[w]/(w^2 - t), \text{ with } w \text{ a non-square and } w^2 = 2^{1/27}
\end{aligned}
$$

$$
\begin{aligned}
P^4(x^4, y^4) &= ((a, 0, ..., 0), (0, ..., 0, b)) \text{ with } x^4, y^4 \in \mathbb{F}_{p^{54}} \\
P'''(x''', y''') &= ((a, 0, ..., 0), (0, ..., 0, b)) \text{ with } x''', y''' \in \mathbb{F}_{p^{27}} \\
P''(x'', y'') &= ((a, 0, ..., 0), (0, ..., 0, b)) \text{ with } x'', y'' \in \mathbb{F}_{p^9} \\
P'(x', y') &= ((a, 0, 0), (0, 0, b)) \text{ with } x', y' \in \mathbb{F}_{p^3} \\
P(x, y) &= (a, b) \text{ with } x, y \in \mathbb{F}_p
\end{aligned}
$$

The cost of multiplication, squaring and inversion in in the 54^{th} twisted field $\mathbb{F}_{p^{54}}$ are:

$$
\begin{aligned}
M_{54} &= (M_{27})_{\mathbb{F}_{p^2}} = ((M_9)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = (((M_3)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\
&= (((6m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = ((6M_3)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = ((36m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\
&= (36M_3)_{\mathbb{F}_{p^2}} = (216m)_{\mathbb{F}_{p^2}} = 216M_2 = 648m,
\end{aligned}
$$

$$
\begin{aligned}
S_{54} &= (S_{27})_{\mathbb{F}_{p^2}} = ((S_9)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = (((S_3)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\
&= (((5s)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = ((5S_3)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = ((25s)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\
&= (25S_3)_{\mathbb{F}_{p^2}} = (125s)_{\mathbb{F}_{p^2}} = 125S_2 = 250m,
\end{aligned}
$$

$$
\begin{aligned}
I_{54} &= (I_{27})_{\mathbb{F}_{p^2}} = ((I_9)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = (((I_3)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\
&= (((9m + 2s + +i)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = ((9M_3 + 2S_3 + I_3)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\
&= ((63m + 12s + i)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = (63M_3 + 12S_3 + I_3)_{\mathbb{F}_{p^2}} \\
&= (387m + 62s + i)_{\mathbb{F}_{p^2}} = 387M_2 + 62S_2 + I_2 \\
&= 1289m + i,
\end{aligned}
$$

4. Comparison

TABLE I
COST OF OPERATIONS IN EACH THE TOWER FIELDS

Path	O	Cost
1	M_{54}	648m
	S_{54}	432m
	I_{54}	1251m+62s+i
2	M_{54}	648m
	S_{54}	360m
	I_{54}	1323m+12s+i
3	M_{54}	648m
	S_{54}	300m
	I_{54}	1371m+2s+i
4	M_{54}	648m
	S_{54}	250m
	I_{54}	1289m+i

The table above give the overall cost of operations in each the tower fields.
We found that the cost of multiplication and squaring is the same for any path chosen, however the cost of inversion change on the path, so we can see that the minimal cost for inversion is 1289m+i.

5. Conclusion

In this paper, we give some methods for tower building of extension of finite field of embedding degree 54. We show that there are four efficients paths for constructions of these extensions of degree 54. We show that by using a degree 2 or 3 twist we handle to perform most of the operations in $\mathbb{F}_p^6$, $\mathbb{F}_{p^9}$, $\mathbb{F}_{p^{18}}$, $\mathbb{F}_{p^{27}}$ and $\mathbb{F}_{p^{54}}$. By using this tower building technique, we also improve the arithmetic of $\mathbb{F}_{p^{54}}$, in order to get better results of calculate the cost of their multiplication, squaring and inversion.

References

[1] Victor S. Miller. Use of elliptic curves in cryptography. Crypto 1985, LNCS 218, pp. 417-426, 1985.
[2] Neal Koblitz. Elliptic curve cryptosystems. Mathematics of Computation, Vol. 48, No. 177, pp. 203-209, 1987.
[3] R.L. Rivest, A. Shamir, and L.M. Adleman. A method for obtaining digital signatures and publickey cryptosystems. Commun. ACM, Vol. 21, No. 2, pp. 120-126, 1978.
[4] Whelan, C., Scott, M.: The Importance of the Final Exponentiation in Pairings When Considering Fault Attacks. In: Takagi, T., Okamoto, T., Okamoto, E., Okamoto, T. (eds.) Pairing 2007. LNCS, vol. 4575, pp. 225-246. Springer, Heidelberg (2007).
[5] Nadia El Mrabet, Nicolas Guillermin, and Sorina Ionica. A study of pairing computation for curves with embedding degree 15. DBLP volume 2009.
[6] Nadia El Mrabet and Marc Joye. GUIDE TO PAIRING-BASED CRYPTOGRAPHY. Chapman and Hall/CRC CRYPTOGRAPHY AND NETWORK SECURITY, 2018.
[7] Emmanuel Fouotsa, Nadia El Mrabet and Aminatou Pecha. Optimal Ate Pairing on Elliptic Curves with Embedding Degree 9; 15 and 27. journal of Groups, Complexity, Cryptology, Volume 12, issue 1 (April 17, 2020)
[8] Narcisse Bang Mbiang, Diego De Freitas Aranha, Emmanuel Fouotsa. Computing the optimal ate pairing over elliptic curves with embedding degrees 54 and 48 at the 256-bit security level. Int. J. Applied Cryptography, Vol. 4, No. 1, 2020.
[9] Md. Al-Amin Khandaker, Taehwan Park, Yasuyuki Nogami, and Howon Kim, Member, KIICE. A Comparative Study of Twist Property in KSS Curves of Embedding Degree 16 and 18 from the Implementation Perspective. J. lnf. Commun. Converg. Eng. 15(2): 97-103, Jun. 2017.

[10] Md. Al-Amin Khandaker, Yasuyuki NOGAMI. Isomorphic Mapping for Ate-based Pairing over KSS Curve of Embedding Degree 18. 10.1109/CANDAR.2016.0113 November 2016.

[11] Rahat Afreen, S.C. Mehrotra. A REVIEW ON ELLIPTIC CURVE CRYPTOGRAPHY FOR EMBEDDED SYSTEMS. International Journal of Computer Science & Information Technology (IJCSIT), Vol 3.

[12] Md. Al-Amin Khandaker, Yasuyuki NOGAMI. A Consideration of Towering Scheme for Efficient Arithmetic Operation over Extension Field of Degree 18. 19th International Conference on Computer and Information Technology, December 18-20, 2016, North South University, Dhaka, Bangladesh.

[13] Nadia El Mrabet, Aurore Guillevic, and Sorina Ionica. Efficient Multiplication in Finite Field Extensions of Degree 5. DBLP 10.1007/978-3-642-21969-6-12 June 2011.

[14] Michael Scott, Aurore Guillevic. A New Family of Pairing-Friendly elliptic curves. May 21, 2018.

[15] Michael Scott, On the Efficient Implementation of Pairing-Based Protocols, in cryptography and coding, pp. 296-308, Springer, 2011.

[16] Joseph H. Silverman, The Arithmetic of Elliptic Curves, Second Edition, 2000.

[17] Augusto Jun Devegili1, Colm Eigeartaigh, Michael Scott, and Ricardo Dahab, Multiplication and Squaring on Pairing-Friendly Fields, 2006.

[18] ISMAIL ASSOUJAA, SIHAM EZZOUAK, HAKIMA MOUANIS. Compression Point in Field of Characteristic 3. Springer, I4CS 2022, CCIS 1747, pp. 104111, 2022 https://doi.org/10.1007/978-3-031-23201-5_7.

[19] ISMAIL ASSOUJAA, SIHAM EZZOUAK, HAKIMA MOUANIS. Tower Building Technique on Elliptic Curve with Embedding Degree 36. WSEAS TRANSACTIONS ON COMPUTERS. DOI: 10.37394/23205.2022.21.39.

[20] ISMAIL ASSOUJAA, SIHAM EZZOUAK, HAKIMA MOUANIS. Tower Building Technique on Elliptic Curve with Embedding Degree 72. WSEAS Transactions on Computer Research 10:126-138 DOI: 10.37394/232018.2022.10.17

[21] ISMAIL ASSOUJAA, SIHAM EZZOUAK, HAKIMA MOUANIS. TOWER BUILDING TECHNIQUEON ELLIPTIC CURVEWITH EMBEDDING DEGREE 18. Tatra mountains mathematical publications, DOI: 10.2478/tmmp-2023-0008Tatra Mt. Math. Publ. 83 (2023), 103118.

[22] ISMAIL ASSOUJAA, SIHAM EZZOUAK, HAKIMA MOUANIS. Pairing based cryptography New random point exchange key protocol. Conference: 2022 7th International Conference on Mathematics and Computers in Sciences and Industry (MCSI), DOI: 10.1109/MCSI55933.2022.00017.

[23] ISMAIL ASSOUJAA, SIHAM EZZOUAK. New Compression Point Reducing Memory Size in Field of Characteristic Different From 2 And 3.International Journal of Scientific Research and Innovative Studies. https://doi.org/10.5281/zenodo.11244720.

[24] ISMAIL ASSOUJAA, SIHAM EZZOUAK. Improving arithmetic calculations on elliptic curves with embedding degree 2i.3. Journal of Xidian University. https://doi.org/10.5281/Zenodo.11505701. ISSN No:1001-2400.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The authors equally contributed in the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.