International Journal of Recent Engineering Research and Development (IJRERD)
ISSN: 2455-8761
www.ijrerd.com || Volume 09 – Issue 03 || May - Jun 2024 || PP. 131-142

Improving Arithmetic Calculations on Elliptic Curves with Embedding Degree 2^i and 3^j

Assoujaa Ismail[1]
Sidi Mohammed Ben Abdellah University
Faculty of science Dhar El Mahrez
Department of mathematics, Lab: LASMA
Fez, Morocco

Ezzouak Siham[2]
Sidi Mohammed Ben Abdellah University
Faculty of science Dhar El Mahrez
Department of mathematics, Lab: LASMA
Fez, Morocco

Abstract: Pairing-based cryptography has gained significant attention in recent years due to its practical solution for achieving high levels of security using efficient and faster pairing-based techniques. However, ensuring this security requires working with extension finite fields of the form $\mathbb{F}_{p^k}$, where $k \geq 12$. Therefore, efficient implementation of these fields is crucial. This paper aims to improve the efficiency and security, by developing better arithmetic calculations on elliptic curves with embedding degree of the form 2^i and 3^j. The proposed approach employs the tower building technique, which constructs a sequence of extensions of the base field $\mathbb{F}_p$ by iteratively adjoining roots of polynomials to create new, larger fields. Additionally, we examine the use of a degree 2 and/or 3 twist to improve most operations in the fields $\mathbb{F}_{p^2}$ and/or $\mathbb{F}_{p^3}$. By exploring these techniques, our goal is to provide practical and efficient solutions for elliptic curve with embedding degree of the form 2^i and 3^j.

Index Terms: Elliptic curve, Embedding degree, Twist curve.

1 Introduction

Since the discovery of pairing-based cryptography, developers and researchers have been dedicating their efforts to studying and developing new techniques and methods to implement pairing protocols and algorithms more efficiently. Weil pairing was the first pairing introduced by Weil Andre in 1948, followed by others such as Tate pairing, Ate pairing, and many more. The benefits of elliptic curve cryptosystems, discovered by Neal Koblitz [1] and Victor Miller [2], include reducing the key sizes used in public key cryptography. Some works, such as the one presented in [3], are interested in signature numeric, while the authors in [4] demonstrate the use of the final exponentiation in pairings as a countermeasure against fault attacks. In [5],[6],[7], [13], Nadia El and others provide a study on working with elliptic curves with embedding degrees 5, 9, 15, and 27. Additionally, in [9],[10],[11],[12], and [13], researchers investigate working with curves with various embedding degrees. In [8], the security level of optimal ate pairing is studied, and other useful works (see [5]) are also presented. In this paper, we seek to obtain efficient ways to compute pairings for curves of embedding degree 2^i and 3^j. We will improve arithmetic operations in curves with embedding degree 2^i3^j by using the tower-building technique. Our investigation is divided into two parts. In the first part, we study elliptic curves with embedding degree 2^i. In the second and final part, we study elliptic curves with embedding degree 3^j. For other cases, such as $2^i.3$, $2^i.3^2$ and 2.3^3, we have already studied some of these cases for $k = 18,36,54,$ and 72 in previous articles [20], [21], and [22]. To provide some background for our investigation, Section 2 of this paper recalls some key properties of pairings, including ate pairing and Miller's Algorithm. In Section 3, we present our main theorem, which forms the basis of our investigation. Then, in Section 4, we present the results of our work, including improvements to arithmetic operations in $\mathbb{F}_{p^{3^j}}$ and $\mathbb{F}p^{2^i}$ by making use of the tower building technique. We also present three case studies, which show how using degree-2 or degree-3 twists can enable efficient handling of most operations in $\mathbb{F}p^2$ or $\mathbb{F}_{p^3}$. Finally, in Section 5, we conclude our paper by summarizing our main findings and discussing potential avenues for further research in this area.

2 Mathematical background

Throughout the paper, we assume that E is an elliptic curve with equation $y^2 = x^3 + ax + b$, where $b \in \mathbb{F}_q$ and q is a prime number. Additionally, we will use the following conventions without explicitly stating them

- k : the embedding degree: the smallest integer such that r divides $q^k - 1$.
- m,s,i: multiplication, squaring, inversion in field $\mathbb{F}_p$.
- M_i, S_i, I_i : multiplication, squaring, inversion in field $\mathbb{F}_{p^i}$.
- B_k : basis
- a_i : i is the position of point a in the basis B_k with $i \in \mathbb{N}$.
- b_j : j is the position of point bin the basis B_k with $j \in \mathbb{N}$.
- $P_l = (x_l, y_l) = (a_l, b_l)_{B_k}$: point in $E(\mathbb{F}_{p^k})$ with $l \in \{1,2,3,4,5,6\}$

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:

$$\Psi_2 : E'(\mathbb{F}_{p^{k/2}}) \to E(\mathbb{F}_{p^k})$$
$$(x, y) \to (x, yv^{1/2})$$

- $d = 3$, 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:

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

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 ([18]).

- 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 ([18]).

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 $A = a_0 + a_1 u + a_2 u^2 + ... + a_{k-1} u^{k-1}$. 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:

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

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

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

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

$$E(\mathbb{F}_p) \to E(\mathbb{F}_{p^2})$$

$$(x, y) \to (x_1, y_1) = (x, yu)$$

- 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:

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

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

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

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:

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

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

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

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

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

- 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:

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

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

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

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:

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

and,

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

3 Tower Building Technique in Elliptic Curve with Embedding Degree 2^i

In this section, we will study the elliptic curve with embedding degree $2^i < 100$, i,e when k=2, 4, 8, 16, 32, 64.

We will follow the figure below for construction of these elliptic curves

Let

$$\mathbb{F}_{p^2}=\mathbb{F}_p[u]/(u^2-\beta) \text{ such that } \beta \text{ non-square}$$
$$\mathbb{F}_{p^4}=\mathbb{F}_{p^2}[v]/(v^2-u) \text{ such that } u \text{ non-square}$$
$$\mathbb{F}_{p^8}=\mathbb{F}_{p^4}[t]/(t^2-v) \text{ such that } v \text{ non-square}$$
$$\mathbb{F}_{p^{16}}=\mathbb{F}_{p^8}[w]/(w^2-t) \text{ such that } t \text{ non-square}$$
$$\mathbb{F}_{p^{32}}=\mathbb{F}_{p^{16}}[z]/(z^2-w) \text{ such that } w \text{ non-square}$$
$$\mathbb{F}_{p^{64}}=\mathbb{F}_{p^{32}}[c]/(c^2-z) \text{ such that } z \text{ non-square}$$

where $\beta=2$ is considered to be the best choice for efficient arithmetic. From the above towering construction we can find that $u=v^2=t^4=w^8=z^{16}=c^{32}$, where u is the basis element of the base extension field $\mathbb{F}_{p^2}$.

$$B_2=\{1,u\}$$
$$B_4=\{1,v,v^2,v^3\}=\{1,v,u,uv\}$$
$$B_8=\{1,t,t^2,...,t^7\}=\{1,u,v,uv,t,ut,vt,uvt\}$$
$$B_{16}=\{1,w,w^2,...,w^{15}\}=\{1,u,v,uv,t,ut,vt,uvt,w,uw,vw,uvw,$$

$tw, utw, vtw, uvtw\}$

$B_{32} = \{z, z, z^2, ..., z^{31}\} = \{1, u, v, uv, t, ut, vt, uvt, w, uw, vw, uvw,$
$tw, utw, vtw, uvtw, z, ..., uvtwz\}$

$B_{64} = \{1, c, c^2, ..., c^{63}\} = \{1, u, v, uv, t, ut, vt, uvt, w, uw, vw, uvw, tw,$
$utw, vtw, uvtw, z, ..., uvtwzc\}.$

$$E(\mathbb{F}_{p^2}) \to E(\mathbb{F}_{p^4}) \to E(\mathbb{F}_{p^8}) \to E(\mathbb{F}_{p^{16}}) \to E(\mathbb{F}_{p^{32}}) \to E(\mathbb{F}_{p^{64}})$$
$$(x_1, y_1) \to (x_2, y_2) \to (x_3, y_3) \to (x_4, y_4) \to (x_5, y_5) \to (x_6, y_6)$$
$$(x, uy) \to (x, uvy) \to (x, uvty) \to (x, uvtwy) \to (x, uvtwzy)$$
$$\to (x, uvtwzcy)$$

$$P_1 = (x_1, y_1) = (x, uy) = (a, ub)_{B_2} = ((a,0), (0, b))$$
$$P_2 = (x_2, y_2) = (x, uvy) = (a, uvb)_{B_4} = ((a,0,0,0), (0,0,0, b))$$
$$P_3 = (x_3, y_3) = (x, uvty) = (a, uvtb)_{B_8} = ((a,0,...,0), (0,...,0, b))$$
$$P_4 = (x_4, y_5) = (x, uvtwy) = (a, uvtwb)_{B_{16}}$$
$$= ((a,0,...,0), (0,...,0, b))$$
$$P_5 = (x_5, y_5) = (x, uvtwzy) = (a, uvtwzb)_{B_{32}}$$
$$= ((a,0,...,0), (0,...,0, b))$$
$$P_6 = (x_6, y_6) = (x, uvtwzcy) = (a, uvtwzcb)_{B_{64}}$$
$$= ((a,0,...,0), (0,...,0, b))$$

Each rational point P_6 in the subgroup $\mathbb{G}_2 \subset E(\mathbb{F}_{p^{64}})$ can be represented by a special vector with 64 elements in $\mathbb{F}_p$ for both x_6 and y_6 coordinates. Starting from P_6, we can construct its quadratic twisted isomorphic rational point P_5 in $E(\mathbb{F}_{p^{32}})$, which also has a special vector representation with 32 elements in $\mathbb{F}_p$ for each x_5 and y_5 coordinates. Then, we can construct P_4 in $E(\mathbb{F}_{p^{16}})$, which has a special vector representation with 16 elements in $\mathbb{F}_p$ for both x_4 and y_4 coordinates, and its quadratic twisted isomorphic rational point P_3 in $E(\mathbb{F}_{p^8})$, which has a special vector representation with 8 elements in $\mathbb{F}_p$ for each x_3 and y_3 coordinates. We can continue this process to obtain P_2 in $E(\mathbb{F}_{p^4})$ with a special vector representation with 4 elements in $\mathbb{F}_p$ for each x_2 and y_2 coordinates, and its quadratic twisted isomorphic rational point P_1 in $E(\mathbb{F}_{p^2})$ with a special vector representation with 2 elements in $\mathbb{F}_p$ for each x_1 and y_1 coordinates. Finally, we obtain P in $E(\mathbb{F}_p)$ as the quadratic twisted isomorphic rational point of P_1, which also has a special vector representation with 2 elements in $\mathbb{F}_p$ for both x and y coordinates.

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 ([18]).

Cost of operation in Quartic twisted curve:

The cost of multiplication, squaring and inversion in in the Quartic twisted field $\mathbb{F}_{p^4}$ are:

$$M_4 = (M_2)_{\mathbb{F}_{p^2}} = (3m)_{\mathbb{F}_{p^2}} = 3M_2 = 3\times 3m = 9m,$$

$$S_4 = (S_2)_{\mathbb{F}_{p^2}} = (2m)_{\mathbb{F}_{p^2}} = 2M_2 = 2\times 3m = 6m,$$

$$I_4 = (I_2)_{\mathbb{F}_{p^2}} = (4m+i)_{\mathbb{F}_{p^2}} = 4M_2 + I_2 = 16m+i.$$

Cost of operation in Octic twisted curve:

The cost of multiplication, squaring and inversion in in the Quartic twisted field $\mathbb{F}_{p^8}$ are:

$$M_8 = (M_4)_{\mathbb{F}_{p^2}} = (9m)_{\mathbb{F}_{p^2}} = 9M_2 = 27m,$$

$$S_8 = (S_4)_{\mathbb{F}_{p^2}} = (6m)_{\mathbb{F}_{p^2}} = 6M_2 = 18m,$$

$$I_8 = (I_4)_{\mathbb{F}_{p^2}} = (16m+i)_{\mathbb{F}_{p^2}} = 16M_2 + I_2 = 52m+i\,.$$

Cost of operation in 16^{th} twisted curve:

The cost of multiplication, squaring and inversion in in the 16^{th} twisted field $\mathbb{F}_{p^{16}}$ are:

$$M_{16} = (M_8)_{\mathbb{F}_{p^2}} = (27m)_{\mathbb{F}_{p^2}} = 27M_2 = 81m,$$

$$S_{16} = (S_8)_{\mathbb{F}_{p^2}} = (18m)_{\mathbb{F}_{p^2}} = 18M_2 = 54m,$$

$$I_{16} = (I_8)_{\mathbb{F}_{p^2}} = (52m+i)_{\mathbb{F}_{p^2}} = 52M_2 + I_2 = 160m+i\,.$$

Cost of operation in 32^{th} twisted curve:

The cost of multiplication, squaring and inversion in in the 32^{th} twisted field $\mathbb{F}_{p^{32}}$ are:

$$M_{32} = (M_{16})_{\mathbb{F}_{p^2}} = (81m)_{\mathbb{F}_{p^2}} = 81M_2 = 243m,$$

$$S_{32} = (S_{16})_{\mathbb{F}_{p^2}} = (54m)_{\mathbb{F}_{p^2}} = 54M_2 = 162m,$$

$$I_{32} = (I_{16})_{\mathbb{F}_{p^2}} = (160m+i)_{\mathbb{F}_{p^2}} = 160M_2 + I_2 = 484m+i\,.$$

Cost of operation in 64^{th} twisted curve:

The cost of multiplication, squaring and inversion in in the 64^{th} twisted field $\mathbb{F}_{p^{64}}$ are:

$$M_{64} = (M_3 2)_{\mathbb{F}_{p^2}} = (243m)_{\mathbb{F}_{p^2}} = 243M_2 = 729m,$$

$$S_{64} = (S_3 2)_{\mathbb{F}_{p^2}} = (162m)_{\mathbb{F}_{p^2}} = 162M_2 = 486m,$$

$$I_{64} = (I_3 2)_{\mathbb{F}_{p^2}} = (484m+i)_{\mathbb{F}_{p^2}} = 484M_2 + I_2 = 1456m+i\,.$$

Table 1: Cost of operations in each the tower fields of embedding degree 2^i

Field	Operations	Cost of M_{2^i}	Cost of S_{2^i}	Cost of I_{2^i}
$\mathbb{F}_{p^2}$:	M_2, S_2, I_2	3m	2m	4m+i
$\mathbb{F}_{p^4}$:	M_4, S_4, I_4	9m	6m	16m+i
$\mathbb{F}_{p^8}$:	M_8, S_8, I_8	27m	18m	52m+i
$\mathbb{F}_{p^{16}}$:	M_{16}, S_{16}, I_{16}	81m	54m	160m+i
$\mathbb{F}_{p^{32}}$:	M_{32}, S_{32}, I_{32}	243m	162m	484m+i
$\mathbb{F}_{p^{64}}$:	M_{64}, S_{64}, I_{64}	729m	486m	1456m+i

In the table above, we find a relationship between the operation cost and embedding degree 2^i as describe below

The cost of multiplication in elliptic curve with embedding degree 2^i is:

$$M_{2^i} = 3^i m$$

The cost of squaring in elliptic curve with embedding degree 2^i is:

$$S_{2^i} = 2.3^{i-1} m$$

The cost of inversion in elliptic curve with embedding degree 2^i is:

$$I_{2^i} = (3^i \times 2 - 2)m + i$$

Proof 1 *By recurrence relation we will prove the above formulas.*

i- for i=1 we have $M_2 = 3m$, $S_2 = 2m$ and $I_2 = 4m + i$, and that is correct.

ii- Let for i=n $M_{2^n} = 3^n m$, $S_{2^n} = 2.3^{n-1} m$ and $I_{2^n} = (3^n \times 2 - 2)m + i$ are correct.

iii- We will prove the same for i=n+1 are also correct,

We have

$$M_{2^{n+1}} = M_{2^n.2} = (M_{2^n})_{\mathbb{F}_2} = 3^n M_2 = 3^n.3m = 3^{n+1} m.$$

$$S_{2^{n+1}} = S_{2^n.2} = (S_{2^n})_{\mathbb{F}_2} = 2.3^{n-1} M_2 = 2.3^{n-1}.3m = 2.3^n m.$$

$$I_{2^{n+1}} = I_{2^n.2} = (I_{2^n})_{\mathbb{F}_2} = (3^n \times 2 - 2)M - 2 + I_2$$

$$= (3^n \times 2 - 2)3m + 4m + i = (3^{n+1} \times 2 - 2)m + i$$

4 Tower Building Technique in Elliptic Curve with Embedding Degree 3^j

In this section, we will study the elliptic curve with embedding degree $3^j < 100$, i,e when k=3, 9, 27, 81.

We will follow the figure below for construction of these elliptic curves

Let

$$\mathbb{F}_{p^3} = \mathbb{F}_p[u]/(u^3 - \beta) \textit{such that } \beta \textit{ non-cube}$$

$$\mathbb{F}_{p^9} = \mathbb{F}_{p^3}[v]/(v^3 - u) \textit{such that } u \textit{ non-cube}$$

$$\mathbb{F}_{p^{27}} = \mathbb{F}_{p^9}[t]/(t^3 - v) \textit{such that } v \textit{ non-cube}$$

$$\mathbb{F}_{p^{81}} = \mathbb{F}_{p^{27}}[w]/(w^3 - t) \textit{such that } t \textit{ non-cube}$$

where $\beta = 2$ is considered to be the best choice for efficient arithmetic. From the above towering construction we can find that $u = v^3 = t^9 = w^{27}$, where u is the basis element of the base extension field $\mathbb{F}_{p^3}$.

$$B_3 = \{1, u, u^2\}$$
$$B_9 = \{1, v, v^2, ..., v^8\} = \{1, v, v^2, u, uv, uv^2, u^2, u^2v, u^2v^2\}$$
$$B_{27} = \{1, t, t^2, ..., t^{26}\} = \{1, t, t^2, ..., u^2v^2t^2\}$$
$$B_{81} = \{1, w, w^2, ..., w^{80}\} = \{1, w, w^2, ..., u^2v^2t^2w^2\}$$

$$E(\mathbb{F}_{p^3}) \to E(\mathbb{F}_{p^9}) \to E(\mathbb{F}_{p^{27}}) \to E(\mathbb{F}_{p^{81}})$$
$$(x_1, y_1) \to (x_2, y_2) \to (x_3, y_3) \to (x_4, y_4)$$
$$(ux, uy) \to (uvx, uvy) \to (uvtx, uvty) \to (uvtwx, uvtwy)$$

$$P_1 = (x_1, y_1) = (ux, uy) = (ua, ub)_{B_3} = ((0, a, 0), (0, b, 0))$$
$$P_2 = (x_2, y_2) = (uvx, uvy) = (a, uvb)_{B_9}$$
$$= ((0,0,0,0, a,0,0,0,0), (0,0,0,0, b,0,0,0,0))$$
$$P_3 = (x_3, y_3) = (uvtx, uvty) = (a, uvtb)_{B_{27}}$$
$$= ((0,...,0, a_{13},0,...,0), (0,...,0, b_{13},0,...,0))$$
$$P_4 = (x_4, y_5) = (uvtwx, uvtwy) = (a, uvtwb)_{B_{81}}$$
$$= ((0,...,0, a_{40},0,...,0), (0,...,0, b_{40},0,...,0))$$

Each rational point $P_4 \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{81}})$ can be represented by a special vector with 81 elements in $\mathbb{F}_p$ for each x_4 and y_4 coordinate. The following construction shows that starting from $P_4 \in E(\mathbb{F}_{p^{81}})$ and its cubic twisted isomorphic rational point $P_3 \in E(\mathbb{F}_{p^{27}})$, which also has a cubic twisted isomorphic rational point $P_2 \in E(\mathbb{F}_{p^9})$, we can find a cubic twisted isomorphic rational point $P_1 \in E(\mathbb{F}_{p^3})$ and finally a cubic twisted isomorphic rational point $P \in E(\mathbb{F}_p)$.

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 ([18]).

Cost of operation in Nonic twisted curve:

The cost of multiplication, squaring and inversion in in the Nonic twisted field $\mathbb{F}_{p^9}$ are:

$$M_9 = (M_3)_{\mathbb{F}_{p^3}} = (6m)_{\mathbb{F}_{p^3}} = 6M_3 = 36m,$$
$$S_9 = (S_3)_{\mathbb{F}_{p^3}} = (5s)_{\mathbb{F}_{p^3}} = 5S_3 = 25s,$$
$$I_9 = (I_3)_{\mathbb{F}_{p^3}} = (9m + 2s + i)_{\mathbb{F}_{p^3}} = 9M_3 + 2S_3 + I_2 = 63m + 12s + i.$$

Cost of operation in 27^{th} twisted curve:

The cost of multiplication, squaring and inversion in in the 27^{th} twisted field $\mathbb{F}_{p^{27}}$ are:

$$M_{27} = (M_9)_{\mathbb{F}_{p^3}} = (36m)_{\mathbb{F}_{p^3}} = 36M_3 = 216m,$$
$$S_{27} = (S_9)_{\mathbb{F}_{p^3}} = (25s)_{\mathbb{F}_{p^3}} = 25S_3 = 125s,$$
$$I_{27} = (I_9)_{\mathbb{F}_{p^3}} = (63m + 12s + i)_{\mathbb{F}_{p^3}} = 63M_3 + 12S_3 + I_3 = 387m + 62s + i\,.$$

Cost of operation in 81^{th} twisted curve:

The cost of multiplication, squaring and inversion in in the 81^{th} twisted field $\mathbb{F}_{p^{81}}$ are:

$$M_{81} = (M_{27})_{\mathbb{F}_{p^3}} = (216m)_{\mathbb{F}_{p^3}} = 216M_3 = 1296m$$
$$S_{81} = (S_{27})_{\mathbb{F}_{p^3}} = (125s)_{\mathbb{F}_{p^3}} = 125S_3 = 725s$$
$$I_{81} = (I_{27})_{\mathbb{F}_{p^3}} = (387m + 62s + i)_{\mathbb{F}_{p^3}} = 387M_3 + 62S_3 + I_3$$
$$= 2331m + 312s + i.$$

Table 2: Cost of operations in each the tower fields of embedding degree 3^j

Field	Operations	Cost of M_{3^j}	S_{3^j}	Cost of I_{3^j}
$\mathbb{F}_{p^3}$:	M_3, S_3, I_3	6m	5s	9m+2s+i
$\mathbb{F}_{p^9}$:	M_9, S_9, I_9	36m	25s	63m+12s+i
$\mathbb{F}_{p^{27}}$:	M_{27}, S_{27}, I_{27}	216m	125s	387m+62s+i
$\mathbb{F}_{p^{81}}$:	M_{81}, S_{81}, I_{81}	1296m	725s	2331m+312s+i

In the table above, we find a relationship between the operation cost and embedding degree 3^j as describe below

The cost of multiplication in elliptic curve with embedding degree 3^j is:

$$M_{3^j} = 6^j m$$

The cost of squaring in elliptic curve with embedding degree 3^j is:

$$S_{3^j} = 5^j s$$

The cost of inversion in elliptic curve with embedding degree 3^j is:

$$I_{3^j} = \sum_1^j 9.6^{j-1} m + \sum_1^j 2.5^{j-1} s + i$$

Proof 2 *By recurrence relation we will prove the above formulas.*

i- for j=1 we have $M_3 = 6m$, $S_3 = 5s$ and $I_3 = 9m + 2s + i$, and that is correct.

ii- Let for j=n $M_{3^n} = 6^n m$, $S_{3^n} = 5^n s$ and $I_{3^n} = \sum_1^n 9.6^{n-1} m + \sum_1^n 2.5^{n-1} s + i$ are correct.

iii- We will prove the same for j=n+1 are also correct, We have

$$M_{3^{n+1}} = M_{3^n.3} = (M_{3^n})_{\mathbb{F}_3} = 6^n M_3 = 6^n.6m = 6^{n+1}m.$$

$$S_{3^{n+1}} = S_{3^n.3} = (S_{3^n})_{\mathbb{F}_3} = 5^n S_3 = 5^n.5s = 5^{n+1}s.$$

$$I_{3^{n+1}} = I_{3^n.3} = (I_{3^n})_{\mathbb{F}_3} = \sum_1^n 9.6^{n-1} M_3 + \sum_1^n 2.5^{n-1} S_3 + I_3$$

$$= \sum_1^n 9.6^{n-1}.6m + \sum_1^n 2.5^{n-1}.5s + 9m + 2s + i$$

$$= \sum_2^{n+1} 9.6^{n-1} m + \sum_2^{n+1} 2.5^{n-1} s + 9m + 2s + i$$

$$= \sum_1^{n+1} 9.6^{n-1} m + \sum_1^{n+1} 2.5^{n-1} s + i$$

5 Conclusion

In this paper, we present efficient methods for building towers of finite field extensions of the form $2^i.3^j < 100$ for use in cryptography. We do the constructions of those elliptic curve for embedding degree of the form $2^i < 100$ and $3^j < 100$. To accomplish this, we employ the tower building technique and examine the use of degree 2 and 3 twists to perform operations in $\mathbb{F}_{p^4}$, $\mathbb{F}_{p^8}$, $\mathbb{F}_{p^9}$, $\mathbb{F}_{p^{16}}$, $\mathbb{F}_{p^{27}}$, $\mathbb{F}_{p^{32}}$, $\mathbb{F}_{p^{64}}$ and $\mathbb{F}_{p^{81}}$. By analyzing these twists, we are able to calculate the cost of multiplication, squaring, and inversion in these finite fields, leading to better performance in cryptographic applications.

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) gcc:6285

[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, No 3, June 2011.

[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]. Ezekiel J. Kachisa, Edward F. Schaefer, and Michael Scott. Constructing Brezing-Weng pairing-friendly elliptic curves using elements in the cyclotomic field. In Galbraith and Paterson [29], pages 126-135.
[18]. Augusto Jun Devegili1, Colm Eigeartaigh, Michael Scott, and Ricardo Dahab, Multiplication and Squaring on Pairing-Friendly Fields, 2006.
[19]. ISMAIL ASSOUJAA, SIHAM EZZOUAK, HAKIMA MOUANIS. Compression Point in Field of Characteristic 3. Springer, I4CS 2022, CCIS 1747, pp. 104â€“111, 2022 https://doi.org/10.1007/978-3-031-23201-5_7.
[20]. 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.
[21]. 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
[22]. 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), 103â€“118.
[23]. 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.
[24]. 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.