Tower Building Technique on Elliptic Curve with Embedding Degree 36

[1]ISMAIL ASSOUJAA, [2]SIHAM EZZOUAK, [3]HAKIMA MOUANIS
Departement of Mathematics (LASMA laboratory)
University Sidi Mohammed Ben Abdellah
Fez city, MOROCCO

Abstract: Recent progress on pairing based cryptography was the use of extension of finite fields of the form $\mathbb{F}_{p^k}$, and it was a lot secure and efficient when $k \geq 12$. In this paper, we will use the tower building technique to study the case of k=36 to improve arithmetic operation. We will use a degree 2 or 3 twist to carry out most operations in $\mathbb{F}_{p^2}$, $\mathbb{F}_{p^3}$, $\mathbb{F}_{p^4}$, $\mathbb{F}_{p^6}$, $\mathbb{F}_{p^9}$, $\mathbb{F}_{p^{12}}$, $\mathbb{F}_{p^{18}}$ and $\mathbb{F}_{p^{36}}$, many paths will be found. Finally we will take the optimal case to improve the computation in optimal ate pairing

Key-Words: Optimal ate pairing, Miller Algorithm, Embedding degree 36, Twist curve

Received: December 22, 2021. Revised: October 22, 2022. Accepted: November 29, 2022. Published: December 27, 2022.

1. Introduction

After the discovering of pairing-based cryptography, developers and researchers have been studying 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 benefit of Elliptic curve cryptosystems which was discovered by Neal Koblitz [1] and Victor Miller [2] is to reduce the key sizes of the keys used in public key cryptography. Some works are 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 a curve with embedding degree 18. In [8] they give a study of the security level of optimal ate pairing.

In the present article, we seek to obtain efficient ways to pairing computation for curves of embedding degree 36. We will see how to improve arithmetic operation in curves with embedding degree 36 by using the tower building technique. We will give all the cases studies that build these curves of embedding degree 36, we will also studies the cases when using a degree 2 or 3 twists, to handle most operations in $\mathbb{F}_{p^2}$, $\mathbb{F}_{p^3}$, $\mathbb{F}_{p^4}$, $\mathbb{F}_{p^6}$, $\mathbb{F}_{p^9}$, $\mathbb{F}_{p^{12}}$, $\mathbb{F}_{p^{18}}$ and $\mathbb{F}_{p^{36}}$. By making use of this tower building technique, we can also improve the arithmetic of $\mathbb{F}_{p^6}$, $\mathbb{F}_{p^{12}}$, $\mathbb{F}_{p^{18}}$ and $\mathbb{F}_{p^{36}}$ in order to get better results. Finally we will compare these cases to know which one is the optimal arithmetic path on $\mathbb{F}_{p^2}$, $\mathbb{F}_{p^3}$, $\mathbb{F}_{p^4}$, $\mathbb{F}_{p^6}$, $\mathbb{F}_{p^9}$, $\mathbb{F}_{p^{12}}$, $\mathbb{F}_{p^{18}}$ and $\mathbb{F}_{p^{36}}$.

In this paper, we will investigate and examine what will happen in case of optimal ate pairing with embedding degree 36.

The paper is organized as follows: section 2, we recall some background on the main pairing properties also ate pairing, and Miller Algorithm. Section 3, presents our new techniques of tower building the elliptic curve of embedding degree 36. Section 4, will present the results of our work with comparison between these methods. 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 a, $b \in \mathbb{F}_p$ with p prime number. The symbol a_{opt} will denote the optimal ate pairing. We shall use, without explicit mention, the following

- p: a prime number.
- $q = p^k$: a power of a prime number.
- $\mathbb{G}_1 \subset (E(\mathbb{F}_p))$: additive group of cardinal $n \in \mathbb{N}^*$.
- $\mathbb{G}_2 \subset (E(\mathbb{F}_{p^k}))$: additive group of cardinal $n \in \mathbb{N}^*$.
- $\mathbb{G}_3 \subset \mathbb{F}^*_{p^k} \subset \mu_n$: cyclic multiplicative group of cardinal $n \in \mathbb{N}^*$.

- $\mu_n = \{u \in \bar{\mathbb{F}}_p | u^n = 1\}$.
- P_∞ : the point at infinity of the elliptic curve.
- k : the embedding degree: the smallest integer such that r divides $p^k - 1$.
- $f_{s,P}$: 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_4, S_4, I_4: multiplication, squaring, inversion in field $\mathbb{F}_{p^4}$
- 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_{12}, S_{12}, I_{12}: multiplication, squaring, inversion in field $\mathbb{F}_{p^{12}}$.
- M_{18}, S_{18}, I_{18}: multiplication, squaring, inversion in field $\mathbb{F}_{p^{18}}$.
- M_{36}, S_{36}, I_{36}: multiplication, squaring, inversion in field $\mathbb{F}_{p^{36}}$.

Arithmetic operation cost:

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]).
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]).

2.1 Pairing definition and proprieties:

Definition 2.1. *[16], Let* $(\mathbb{G}_1, +)$, $(\mathbb{G}_2, +)$ *and* $(\mathbb{G}_3, .)$ *three finite abelian groups of the same order r. A pairing is a function:*

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_3$$
$$(P, Q) \mapsto e(P, Q)$$

with the following properties:
1- Bilinear: for all $S, S_1, S_2 \in \mathbb{G}_1$ *and for all* $T, T_1, T_2 \in \mathbb{G}_2$

$$e(S_1 + S_2, T) = e(S_1, T)e(S_2, T)$$
$$e(S, T_1 + T_2) = e(S, T_1)e(S, T_2)$$

2- Non-degenerate: $\forall P \in \mathbb{G}_1$, *there is a* $Q \in \mathbb{G}_2$ *such that* $e(P, Q) \neq 1$ *and* $\forall Q \in \mathbb{G}_2$, *there is a* $P \in \mathbb{G}_1$ *such that* $e(P, Q) \neq 1$.
(*) if $e(S, T) = 1$ *for all* $T \in \mathbb{G}_2$, *then* $T = P_\infty$.

2.2 Frobenius Map

.
For any element $a \in \mathbb{F}_{p^m}$, let us consider the following map

$$\pi_p : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$$
$$a \mapsto a^p$$

Defined by:

$$\begin{aligned}\pi_p(a) &= (a_1 w + a_2 w^p + a_3 w^{p^2} + ... + a_m w^{p^{m-1}})^p \\ &= a_1 w^p + a_2 w^{p^2} + a_3 w^{p^3} + ... + a_m w^{p^m} \\ &= a_m w + a_1 w^p + a_2 w^{p^2} + ... + a_{m-1} w^{p^{m-1}}\end{aligned}$$

Note that the order of $\mathbb{F}^*_{p^m}$ is given by $p^m - 1$, that is, $w^{p^m} = w$ is satisfied.
The map π_p is specially called the Frobenius map.
The Frobenius map for a rational point in $E(\mathbb{F}_q)$ is given by:
For any rational point $P = (x, y)$, Frobenius map ϕ is given by

$$\phi : E(\mathbb{F}_q) \to E(\mathbb{F}_q)$$
$$P(x, y) \mapsto (x^q, y^q).$$
$$P_\infty \mapsto P_\infty.$$

Definition 2.2. *(Ate pairing):*
The Ate pairing is define by

$$\mathbb{G}_1 = E[r] \cap ker(\phi - [1]) \text{ and } \mathbb{G}_2 = E[r] \cap ker(\phi - [p]),$$

where ϕ *denotes the Frobenius map over* $E(\mathbb{F}_p)$.
Let $P \in \mathbb{G}_1$, *and* $Q \in \mathbb{G}_2$ *satisfy:* $\phi(P) = P$

and $\phi(Q) = [p]Q$, *with [p]Q be the scalar multiplication for the rational point Q with scalar p as:* $[p]Q = \sum_{i=0}^{p-1} Q$, $0 \le p < r$, *(if p=r then* $[r]Q = P_\infty$ *) .*

We note the ate pairing with $a(Q,P)$, *such that:*

$$a : \mathbb{G}_2 \times \mathbb{G}_1 \longrightarrow \mathbb{F}_{p^k}^* / (\mathbb{F}_{p^k}^*)^r$$
$$(Q,P) \mapsto a(Q,P) = f_{t-1,Q}(P)^{\frac{p^k-1}{r}},$$

where $f_{t-1,Q}$ *is the rational function associated to the point Q and integer* $t-1$, *with t is the Frobenius trace of* $E(\mathbb{F}_p)$. $f_{t-1,Q} = (t-1)(Q) - ([t-1]Q) - (t-2)(P_\infty)$

2.3 Pairing-friendly elliptic curves

.
We will use the definition of pairing-friendly curves that is taken from [14]:
The construction of such curves depends on our being able to find integers x, y satisfying an equation of the form $Dy^2 = 4q(x) - t(x)^2$

- $q(x)$ and $t(x)$ are polynomials
- The parameter D is the Complex-multiplication discriminant fixed positive integer

Elliptic Curves with Embedding Degree 36:
We can take:

$$\begin{cases} q(x) = \frac{1}{28749}(x^{14} - 4x^{13} + 7x^{12} \\ +683x^8 - 2510x^7 + 4781x^6 \\ +117649x^2 - 386569x + 823543) \\ r(x) = x^{12} + 683x^6 + 117649 \\ t(x) = \frac{1}{259}(259 + 757x + 2x^7). \end{cases}$$

We can see that $q(x) = \frac{1}{28749}(x^{12} + 683x^6 + 117649)(x^2 - 4x + 7) + \frac{1}{28749}(84027x + 222x^7) = \frac{1}{28749}(x^{12} + 683x^6 + 117649)(x^2 - 4x + 7) + \frac{1}{259}(757x + 2x^7)$
so $q(x) + 1 - t(x) = \frac{1}{28749}(x^{12} + 683x^6 + 117649)(x^2 - 4x + 7) = \frac{1}{28749} r(x)(x^2 - 4x + 7)$
hence $r(x)$ really divides $q(x) + 1 - t(x)$.

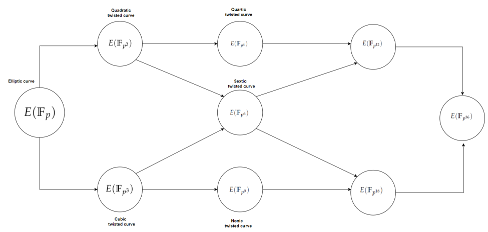
Twists of curves:
Let E be an elliptic curve of j-invariant 0, defined over $\mathbb{F}_p$. We have :

k	equation	isomorphism
k=d	$y^2 = x^3 + b$	$\psi_d : E'(\mathbb{F}_p) \to E(\mathbb{F}_{p^d})$ with $\psi_d(x,y) = (xv^{2/d}, yv^{3/d})$.
k=2	$y^2 = x^3 + av^{-2}x + bv^{-3}$	$\psi_2 : E'(\mathbb{F}_p) \to E(\mathbb{F}_{p^2})$ with $\psi_2(x,y) = (xv, yv^{3/2})$.
k=3	$E' : y^2 = x^3 + bv^{-2}$	$\psi_3 : E'(\mathbb{F}_p) \to E(\mathbb{F}_{p^3})$ with $\psi_3(x,y) = (xv^{2/3}, yv)$.
k=4	$E' : y^2 = x^3 + av^{-1}x$	$\psi_4 : E'(\mathbb{F}_p) \to E(\mathbb{F}_{p^4})$ with $\psi_4(x,y) = (xv^{1/2}, yv^{3/4})$.
k=6	$E' : y^2 = x^3 + bv^{-1}$	$\psi_6 : E'(\mathbb{F}_p) \to E(\mathbb{F}_{p^6})$ with $\psi_6(x,y) = (xv^{1/3}, yv^{1/2})$.
k=9	$E' : y^2 = x^3 + bj$	$\psi_9 : E'(\mathbb{F}_p) \to E(\mathbb{F}_{p^9})$ with $\psi_9(x,y) = (xv^{2/9}, yv^{1/3})$.
k=12	$E' : y^2 = x^3 + c$	$\psi_{12} : E'(\mathbb{F}_p) \to E(\mathbb{F}_{p^{12}})$ with $\psi_{12}(x,y) = (xv^{1/6}, yv^{1/4})$.
k=18	$E' : y^2 = x^3 + bi$	$\psi_{18} : E'(\mathbb{F}_p) \to E(\mathbb{F}_{p^{18}})$ with $\psi_{18}(x,y) = (xv^{1/9}, yv^{1/6})$.
k=36	$E' : y^2 = x^3 + d$	$\psi_{36} : E'(\mathbb{F}_p) \to E(\mathbb{F}_{p^{36}})$ with $\psi_{36}(x,y) = (xv^{1/18}, yv^{1/12})$.

with $a, b \in \mathbb{F}_p$, $j \in \mathbb{F}_{p^3}$ and basis element j is the cubic non residue in $\mathbb{F}_{p^3}$, $i \in \mathbb{F}_{p^3}$ and basis element j is the quadratic and cubic non residue in $\mathbb{F}_{p^3}$.

3. Tower Building Technique for Elliptic Curve with Embedding Degree 36

The figure below show all path possible for building an elliptic curve with embedding degree 36



There is six path possible to building this curve

$$E(\mathbb{F}_p) \longrightarrow E(\mathbb{F}_{p^2}) \longrightarrow E(\mathbb{F}_{p^4}) \longrightarrow E(\mathbb{F}_{p^{12}}) \longrightarrow E(\mathbb{F}_{p^{36}})$$

$$E(\mathbb{F}_p) \longrightarrow E(\mathbb{F}_{p^2}) \longrightarrow E(\mathbb{F}_{p^6}) \longrightarrow E(\mathbb{F}_{p^{12}}) \longrightarrow E(\mathbb{F}_{p^{36}})$$

$$E(\mathbb{F}_p) \longrightarrow E(\mathbb{F}_{p^2}) \longrightarrow E(\mathbb{F}_{p^6}) \longrightarrow E(\mathbb{F}_{p^{18}}) \longrightarrow E(\mathbb{F}_{p^{36}})$$

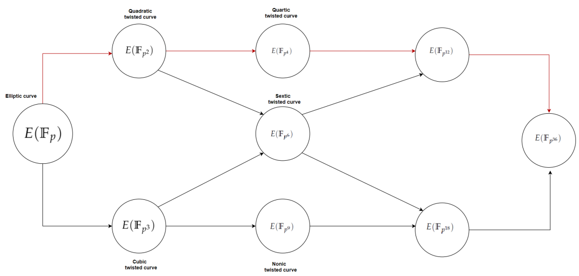
$$E(\mathbb{F}_p) \longrightarrow E(\mathbb{F}_{p^3}) \longrightarrow E(\mathbb{F}_{p^6}) \longrightarrow E(\mathbb{F}_{p^{12}}) \longrightarrow E(\mathbb{F}_{p^{36}})$$

$$E(\mathbb{F}_p) \longrightarrow E(\mathbb{F}_{p^3}) \longrightarrow E(\mathbb{F}_{p^6}) \longrightarrow E(\mathbb{F}_{p^{18}}) \longrightarrow E(\mathbb{F}_{p^{36}})$$

$$E(\mathbb{F}_p) \longrightarrow E(\mathbb{F}_{p^3}) \longrightarrow E(\mathbb{F}_{p^9}) \longrightarrow E(\mathbb{F}_{p^{18}}) \longrightarrow E(\mathbb{F}_{p^{36}})$$

Exploring the first path

$E(\mathbb{F}_p) \longrightarrow E(\mathbb{F}_{p^2}) \longrightarrow E(\mathbb{F}_{p^4}) \longrightarrow E(\mathbb{F}_{p^{12}}) \longrightarrow E(\mathbb{F}_{p^{36}})$



In everything that follow, we considers $3|(p-1)$ and β is a quadratic and cubic non residue in $\mathbb{F}_p$. The appropriate choices of irreducible polynomial defined by:

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

$\mathbb{F}_{p^4} = \mathbb{F}_{p^2}[v]/(v^2-u)$, with v a non-square and $v^2 = 2^{\frac{1}{2}}$

$\mathbb{F}_{p^{12}} = \mathbb{F}_{p^4}[t]/(t^3-v)$, with t a non-cube and $t^3 = 2^{\frac{1}{4}}$

$\mathbb{F}_{p^{36}} = \mathbb{F}_{p^{12}}[w]/(w^3-t)$, with w a non-cube and $w^3 = 2^{\frac{1}{12}}$

Each point P in $E(\mathbb{F}_p)$ can be written in $E(\mathbb{F}_{p^{36}})$ linked to the path choosed (see [9]-pp4). Each rational point $P^4 \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{36}})$ has a special vector representation with 36 elements in $\mathbb{F}_p$ for each x^4 and y^4 coordinates. The structure of the coefficients of $P^4 \in E(\mathbb{F}_{p^{36}})$ and its cubic twisted isomorphic rational point $P''' \in E(\mathbb{F}_{p^{12}})$, which also has a cubic twisted isomorphic rational point $P'' \in E(\mathbb{F}_{p^4})$, that lead to a quadratic twisted isomorphic rational point $P' \in E(\mathbb{F}_{p^2})$, with other quadratic twisted isomorphic rational point $P \in E(\mathbb{F}_p)$.

$$\begin{aligned}
P^4(x^4,y^4) &= ((a,0,...,0),(0,...,0,b)) \,/\, x^4,y^4 \in \mathbb{F}_{p^{36}}\\
P'''(x''',y''') &= ((a,0,...,0),(0,...,0,b)) \,/\, x''',y''' \in \mathbb{F}_{p^{12}}\\
P''(x'',y'') &= ((a,0,0,0),(0,0,0,b)) \text{ with } x'',y'' \in \mathbb{F}_{p^4}\\
P'(x',y') &= ((a,0),(0,b)) \text{ with } x',y' \in \mathbb{F}_{p^2}\\
P(x,y) &= (a,b) \text{ with } x,y \in \mathbb{F}_p
\end{aligned}$$

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

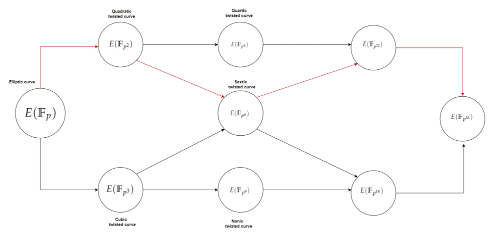
$$\begin{aligned}
M_{36} &= (M_{12})_{\mathbb{F}_{p^3}} = ((M_4)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = (((M_2)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}}\\
&= (((3m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = ((3M_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}}\\
&= ((9m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = (9M_3)_{\mathbb{F}_{p^3}} = (54m)_{\mathbb{F}_{p^3}}\\
&= 54M_3 = 324m,
\end{aligned}$$

$$\begin{aligned}
S_{36} &= (S_{12})_{\mathbb{F}_{p^3}} = ((S_4)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = (((S_2)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}}\\
&= (((2m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = ((2M_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}}\\
&= ((6m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = (6M_3)_{\mathbb{F}_{p^3}} = (36m)_{\mathbb{F}_{p^3}}\\
&= 36M_3 = 216m,
\end{aligned}$$

$$\begin{aligned}
I_{36} &= (I_{12})_{\mathbb{F}_{p^3}} = ((I_4)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = (((I_2)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}}\\
&= (((4m+i)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = ((4M_2+I_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}}\\
&= ((16m+i)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = (16M_3+I_3)_{\mathbb{F}_{p^3}}\\
&= (105m+2s+i)_{\mathbb{F}_{p^3}} = 105M_3+2S_3+I_3\\
&= 639m+12s+i,
\end{aligned}$$

Exploring the second path

$E(\mathbb{F}_p) \longrightarrow E(\mathbb{F}_{p^2}) \longrightarrow E(\mathbb{F}_{p^6}) \longrightarrow E(\mathbb{F}_{p^{12}}) \longrightarrow E(\mathbb{F}_{p^{36}})$



The appropriate choices of irreducible polynomial defined by:

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

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

$\mathbb{F}_{p^{12}} = \mathbb{F}_{p^6}[t]/(t^2-v)$, with t a non-square and $t^2 = 2^{1/6}$

$\mathbb{F}_{p^{36}} = \mathbb{F}_{p^{12}}[w]/(w^3-t)$, / w a non-cube and $w^3 = 2^{1/12}$

Each rational point $P^4 \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{36}})$ has a special vector representation with 36 elements in $\mathbb{F}_p$ for each x^4 and y^4 coordinates. The structure of the coefficients of $P^4 \in E(\mathbb{F}_{p^{36}})$ and its cubic twisted isomorphic rational point $P''' \in E(\mathbb{F}_{p^{12}})$, which also has a quadratic twisted isomorphic rational point $P'' \in E(\mathbb{F}_{p^6})$, that lead to a cubic twisted isomorphic rational point $P' \in E(\mathbb{F}_{p^2})$, with other quadratic twisted isomorphic rational point $P \in E(\mathbb{F}_p)$.

$$\begin{aligned}
P^4(x^4,y^4) &= ((a,0,...,0),(0,...,0,b)) \,/\, x^4,y^4 \in \mathbb{F}_{p^{36}}\\
P'''(x''',y''') &= ((a,0,...,0),(0,...,0,b)) \,/\, x''',y''' \in \mathbb{F}_{p^{12}}\\
P''(x'',y'') &= ((a,0,...,0),(0,...,0,b)) \text{ with } x'',y'' \in \mathbb{F}_{p^6}\\
P'(x',y') &= ((a,0),(0,b)) \text{ with } x',y' \in \mathbb{F}_{p^2}\\
P(x,y) &= (a,b) \text{ with } x,y \in \mathbb{F}_p
\end{aligned}$$

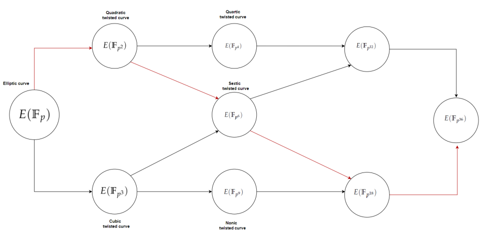
The cost of multiplication, squaring and inversion in in the 36^{th} twisted field $\mathbb{F}_{p^{36}}$ are:

$$\begin{aligned} M_{36} &= (M_{12})_{\mathbb{F}_{p^3}} = (M_6)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = ((M_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\ &= ((3m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = ((3M_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\ &= ((18m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = (18M_2)_{\mathbb{F}_{p^3}} = (54m)_{\mathbb{F}_{p^3}} \\ &= 54M_3 = 324m, \end{aligned}$$

$$\begin{aligned} S_{36} &= (S_{12})_{\mathbb{F}_{p^3}} = (S_6)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = ((S_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\ &= ((2m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = ((2M_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\ &= ((12m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = (12M_2)_{\mathbb{F}_{p^3}} = (36m)_{\mathbb{F}_{p^3}} \\ &= 36M_3 = 216m, \end{aligned}$$

$$\begin{aligned} I_{36} &= (I_{12})_{\mathbb{F}_{p^3}} = (I_6)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = ((I_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\ &= ((4m+i)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\ &= ((4M_3+I_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = ((33m+2s+i)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\ &= (33M_2+2S_2+I_2)_{\mathbb{F}_{p^3}} = (107m+i)_{\mathbb{F}_{p^3}} \\ &= 107M_3+I_3 = 651m+2s+i, \end{aligned}$$

Exploring the third path
$E(\mathbb{F}_p) \longrightarrow E(\mathbb{F}_{p^2}) \longrightarrow E(\mathbb{F}_{p^6}) \longrightarrow E(\mathbb{F}_{p^{18}}) \longrightarrow E(\mathbb{F}_{p^{36}})$



The appropriate choices of irreducible polynomial defined by:

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

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

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

$\mathbb{F}_{p^{36}} = \mathbb{F}_{p^{12}}[w]/(w^2-t),$ / w a non-square and $w^2 = 2^{1/18}$

Each rational point $P^4 \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{36}})$ has a special vector representation with 36 elements in $\mathbb{F}_p$ for each x^4 and y^4 coordinates. The structure of the coefficients of $P^4 \in E(\mathbb{F}_{p^{36}})$ and its quadratic twisted isomorphic rational point $P''' \in E(\mathbb{F}_{p^{18}})$, which also has a cubic twisted isomorphic rational point $P'' \in E(\mathbb{F}_{p^6})$, that lead to a cubic twisted isomorphic rational point $P' \in E(\mathbb{F}_{p^2})$, with other quadratic twisted isomorphic rational point $P \in E(\mathbb{F}_p)$.

$$\begin{aligned} P^4(x^4,y^4) &= ((a,0,...,0),(0,...,0,b)) \text{ with } x^4,y^4 \in \mathbb{F}_{p^{36}} \\ P'''(x''',y''') &= ((a,0,...,0),(0,...,0,b)) \ / \ x''',y''' \in \mathbb{F}_{p^{18}} \\ P''(x'',y'') &= ((a,0,...,0),(0,...,0,b)) \text{ with } x'',y'' \in \mathbb{F}_{p^6} \\ P'(x',y') &= ((a,0),(0,b)) \text{ with } x',y' \in \mathbb{F}_{p^2} \\ P(x,y) &= (a,b) \text{ with } x,y \in \mathbb{F}_p \end{aligned}$$

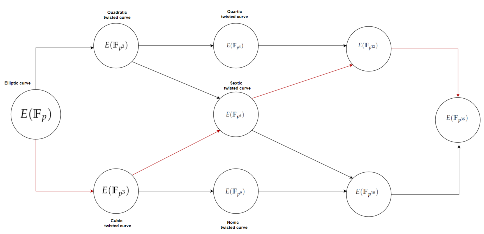
The cost of multiplication, squaring and inversion in in the 36^{th} twisted field $\mathbb{F}_{p^{36}}$ are:

$$\begin{aligned} M_{36} &= (M_{18})_{\mathbb{F}_{p^2}} = (M_6)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = ((M_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\ &= ((3m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = ((3M_3)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\ &= ((18m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = (18M_3)_{\mathbb{F}_{p^2}} = (108m)_{\mathbb{F}_{p^2}} \\ &= 108M_2 = 324m, \end{aligned}$$

$$\begin{aligned} S_{36} &= (S_{18})_{\mathbb{F}_{p^2}} = (S_6)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = ((S_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\ &= ((2m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = ((2M_3)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\ &= ((12m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = (12M_3)_{\mathbb{F}_{p^2}} = (72m)_{\mathbb{F}_{p^2}} \\ &= 72M_2 = 216m, \end{aligned}$$

$$\begin{aligned} I_{36} &= (I_{18})_{\mathbb{F}_{p^2}} = (I_6)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = ((I_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\ &= ((4m+i)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\ &= ((4M_3+I_3)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = ((33m+2s+i)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\ &= (33M_3+2S_3+I_3)_{\mathbb{F}_{p^2}} = (215m+2s+i)_{\mathbb{F}_{p^2}} \\ &= 207M_2+12S_2+I_2 = 649m+i, \end{aligned}$$

Exploring the forth path
$E(\mathbb{F}_p) \longrightarrow E(\mathbb{F}_{p^3}) \longrightarrow E(\mathbb{F}_{p^6}) \longrightarrow E(\mathbb{F}_{p^{12}}) \longrightarrow E(\mathbb{F}_{p^{36}})$



The appropriate choices of irreducible polynomial defined by:

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

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

$$\mathbb{F}_{p^{12}} = \mathbb{F}_{p^6}[t]/(t^2 - v), \text{ with } t \text{ a non-square and } t^2 = 2^{1/6}$$

$$\mathbb{F}_{p^{36}} = \mathbb{F}_{p^{12}}[w]/(w^3 - t), \ / \ w \text{ a non-cube and } w^3 = 2^{1/12}$$

Each rational point $P^4 \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{36}})$ has a special vector representation with 36 elements in $\mathbb{F}_p$ for each x^4 and y^4 coordinates. The structure of the coefficients of $P^4 \in E(\mathbb{F}_{p^{36}})$ and its cubic twisted isomorphic rational point $P''' \in E(\mathbb{F}_{p^{12}})$, which also has a quadratic twisted isomorphic rational point $P'' \in E(\mathbb{F}_{p^6})$, that lead to a quadratic twisted isomorphic rational point $P' \in E(\mathbb{F}_{p^3})$, with other cubic twisted isomorphic rational point $P \in E(\mathbb{F}_p)$.

$$\begin{aligned} P^4(x^4, y^4) &= ((a, 0, ..., 0), (0, ..., 0, b)) \ / \ x^4, y^4 \in \mathbb{F}_{p^{36}} \\ P'''(x''', y''') &= ((a, 0, ..., 0), (0, ..., 0, b)) \ / \ x''', y''' \in \mathbb{F}_{p^{12}} \\ P''(x'', y'') &= ((a, 0, ..., 0), (0, ..., 0, b)) \ / \ x'', y'' \in \mathbb{F}_{p^6} \\ P'(x', y') &= ((a, 0, 0), (0, 0, b)) \text{ with } x', y' \in \mathbb{F}_{p^3} \\ P(x, y) &= (a, b) \text{ with } x, y \in \mathbb{F}_p \end{aligned}$$

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

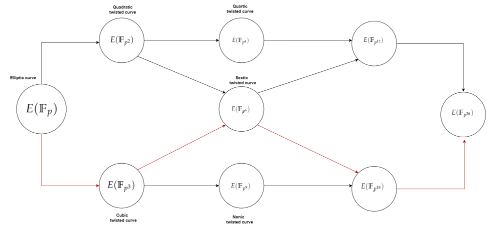
$$\begin{aligned} M_{36} &= (M_{12})_{\mathbb{F}_{p^3}} = (M_6)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = ((M_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\ &= ((6m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = ((6M_2)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\ &= ((18m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = (18M_2)_{\mathbb{F}_{p^3}} = (54m)_{\mathbb{F}_{p^3}} \\ &= 54M_3 = 324m, \end{aligned}$$

$$\begin{aligned} S_{36} &= (S_{12})_{\mathbb{F}_{p^3}} = (S_6)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = ((S_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\ &= ((5s)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = ((5S_2)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\ &= ((10m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = (10M_2)_{\mathbb{F}_{p^3}} = (30m)_{\mathbb{F}_{p^3}} \\ &= 30M_3 = 180m, \end{aligned}$$

$$\begin{aligned} I_{36} &= (I_{12})_{\mathbb{F}_{p^3}} = (I_6)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = ((I_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\ &= ((9m + 2s + +i)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\ &= ((9M_2 + 2S_2 + I_2)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = ((35m + i)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\ &= (35M_2 + I_2)_{\mathbb{F}_{p^3}} = (109m + i)_{\mathbb{F}_{p^3}} \\ &= 109M_3 + I_3 = 663m + 2s + i, \end{aligned}$$

Exploring the fifth path

$$E(\mathbb{F}_p) \longrightarrow E(\mathbb{F}_{p^3}) \longrightarrow E(\mathbb{F}_{p^6}) \longrightarrow E(\mathbb{F}_{p^{18}}) \longrightarrow E(\mathbb{F}_{p^{36}})$$



The appropriate choices of irreducible polynomial defined by:

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

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

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

$$\mathbb{F}_{p^{36}} = \mathbb{F}_{p^{18}}[w]/(w^2 - t), \ / \ w \text{ a non-square and } w^2 = 2^{1/18}$$

Each rational point $P^4 \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{36}})$ has a special vector representation with 36 elements in $\mathbb{F}_p$ for each x^4 and y^4 coordinates. The structure of the coefficients of $P^4 \in E(\mathbb{F}_{p^{36}})$ and its quadratic twisted isomorphic rational point $P''' \in E(\mathbb{F}_{p^{18}})$, which also has a cubic twisted isomorphic rational point $P'' \in E(\mathbb{F}_{p^6})$, that lead to a quadratic twisted isomorphic rational point $P' \in E(\mathbb{F}_{p^3})$, with other cubic twisted isomorphic rational point $P \in E(\mathbb{F}_p)$.

$$\begin{aligned} P^4(x^4, y^4) &= ((a, 0, ..., 0), (0, ..., 0, b)) \ / \ x^4, y^4 \in \mathbb{F}_{p^{36}} \\ P'''(x''', y''') &= ((a, 0, ..., 0), (0, ..., 0, b)) \ / \ x''', y''' \in \mathbb{F}_{p^{18}} \\ P''(x'', y'') &= ((a, 0, ..., 0), (0, ..., 0, b)) \ / \ x'', y'' \in \mathbb{F}_{p^6} \\ P'(x', y') &= ((a, 0, 0), (0, 0, b)) \text{ with } x', y' \in \mathbb{F}_{p^3} \\ P(x, y) &= (a, b) \text{ with } x, y \in \mathbb{F}_p \end{aligned}$$

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

$$\begin{aligned} M_{36} &= (M_{18})_{\mathbb{F}_{p^2}} = (M_6)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = ((M_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\ &= ((6m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = ((6M_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\ &= ((18m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = (18M_3)_{\mathbb{F}_{p^2}} = (108m)_{\mathbb{F}_{p^2}} \\ &= 54M_3 = 324m, \end{aligned}$$

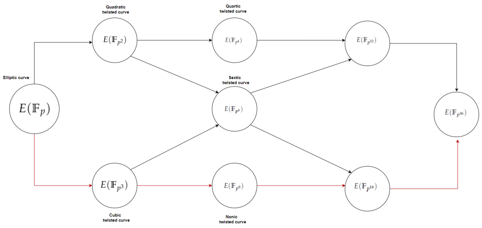
$$\begin{aligned} S_{36} &= (S_{18})_{\mathbb{F}_{p^2}} = (S_6)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = ((S_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\ &= ((5s)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = ((5S_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\ &= ((10m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = (10M_3)_{\mathbb{F}_{p^2}} = (60m)_{\mathbb{F}_{p^2}} \\ &= 60M_2 = 180m, \end{aligned}$$

DOI: 10.37394/23205.2022.21.39

$$
\begin{aligned}
I_{36} &= (I_{18})_{\mathbb{F}_{p^2}} = (I_6)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = ((I_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\
&= ((9m + 2s + i)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\
&= ((9M_2 + 2S_2 + I_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = ((35m + i)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\
&= (35M_3 + I_3)_{\mathbb{F}_{p^2}} = (219m + 2s + i)_{\mathbb{F}_{p^2}} \\
&= 219M_2 + 2S_2 + I_2 = 665m + i,
\end{aligned}
$$

Exploring the sixth path

$E(\mathbb{F}_p) \longrightarrow E(\mathbb{F}_{p^3}) \longrightarrow E(\mathbb{F}_{p^9}) \longrightarrow E(\mathbb{F}_{p^{18}}) \longrightarrow E(\mathbb{F}_{p^{36}})$



The appropriate choices of irreducible polynomial defined by:

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

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

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

$\mathbb{F}_{p^{36}} = \mathbb{F}_{p^{18}}[w]/(w^2 - t)$, / w a non-square and $w^2 = 2^{\frac{1}{18}}$

Each rational point $P^4 \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{36}})$ has a special vector representation with 36 elements in $\mathbb{F}_p$ for each x^4 and y^4 coordinates. The structure of the coefficients of $P^4 \in E(\mathbb{F}_{p^{36}})$ and its quadratic twisted isomorphic rational point $P''' \in E(\mathbb{F}_{p^{18}})$, which also has a quadratic twisted isomorphic rational point $P'' \in E(\mathbb{F}_{p^9})$, that lead to a cubic twisted isomorphic rational point $P' \in E(\mathbb{F}_{p^3})$, with other cubic twisted isomorphic rational point $P \in E(\mathbb{F}_p)$.

$$
\begin{aligned}
P^4(x^4, y^4) &= ((a, 0, ..., 0), (0, ..., 0, b)) \text{ with } x^4, y^4 \in \mathbb{F}_{p^{36}} \\
P'''(x''', y''') &= ((a, 0, ..., 0), (0, ..., 0, b)) \text{ with } x''', y''' \in \mathbb{F}_{p^{18}} \\
P''(x'', y'') &= ((a, 0, ..., 0), (0, ..., 0, b)) \text{ with } x'', y'' \in \mathbb{F}_{p^9} \\
P'(x', y') &= ((a, 0, 0), (0, 0, b)) \text{ with } x', y' \in \mathbb{F}_{p^3} \\
P(x, y) &= (a, b) \text{ with } x, y \in \mathbb{F}_p
\end{aligned}
$$

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

$$
\begin{aligned}
M_{36} &= (M_{18})_{\mathbb{F}_{p^2}} = (M_9)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = ((M_3)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\
&= ((6m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = ((6M_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\
&= ((36m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = (36M_2)_{\mathbb{F}_{p^2}} = (108m)_{\mathbb{F}_{p^2}} \\
&= 108M_2 = 324m,
\end{aligned}
$$

$$
\begin{aligned}
S_{36} &= (S_{18})_{\mathbb{F}_{p^2}} = (S_9)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = ((S_3)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\
&= ((5s)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = ((5S_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\
&= ((25s)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = (25S_2)_{\mathbb{F}_{p^2}} = (50m)_{\mathbb{F}_{p^2}} \\
&= 50M_2 = 150m,
\end{aligned}
$$

$$
\begin{aligned}
I_{36} &= (I_{18})_{\mathbb{F}_{p^2}} = (I_9)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = ((I_3)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\
&= ((9m + 2s + i)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\
&= ((9M_3 + 2S_3 + I_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\
&= ((63m + 12s + i)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\
&= (63M_2 + 12S_2 + I_2)_{\mathbb{F}_{p^2}} = (217m + i)_{\mathbb{F}_{p^2}} \\
&= 217M_2 + I_2 = 655m + i,
\end{aligned}
$$

4. Main Theorem

Let E be an elliptic curve defined over $\mathbb{F}_p$ with $p > 3$ according to the following short Weierstrass equation: $E : y^2 = x^3 + ax + b$.

Definition 4.1. *(Optimal ate pairing on elliptic curves with embedding degree 36):*
The Optimal ate pairing on elliptic curves with embedding degree 36 is define for $P \in \mathbb{G}_1$, and $Q \in \mathbb{G}_2$. We note it a_{opt}, such that:

$$
\begin{aligned}
a_{opt} &: \mathbb{G}_2 \times \mathbb{G}_1 \longrightarrow \mathbb{G}_3 \\
&(Q, P) \mapsto a_{opt}(Q, P) = f_{x,Q}(P)^{\frac{p^{36}-1}{r}}
\end{aligned}
$$

For optimal ate pairing with embedding degree 36 we have:

$$
(Q, P) \mapsto (f_{x,Q}.f^p_{3,Q}.l_{x[Q],[3p]Q}(P))^{\frac{p^{36}-1}{r}}
$$

with $l_{A,B}$ denotes the line through points A and B,

Algorithm 1 Optimal ate pairing with embedding degree 36

Input: $P \in \mathbb{G}_1, Q \in \mathbb{G}'_2$
Output: $a_{opt}(Q, P)$

1: $f \leftarrow 1, T \leftarrow Q$
2: for $i = l_{log_2(l)-1}$ downto 0 do
3: $f \leftarrow f^2.l_{T,T}(P), T \leftarrow [2]T$
4: if $l_i = 1$ then
5: $f \leftarrow f.l_{T,Q}(P), T \leftarrow T + Q$
6: end
7: end
8: $f_1 \leftarrow f^p$
9: $f \leftarrow f.f_1$
10: $Q_1 \leftarrow x[Q], Q_2 \leftarrow [3p]Q$
11: $f \leftarrow f.l_{Q_1,Q_2}(P)$
12: $f \leftarrow f^{\frac{p^{36}-1}{r}}$
13: return f

The cost of line 3 is $3M_k + 2S_k + I_k$
The cost of line 5 is $3M_k + S_k + I_k$

Lemma 4.1. .
In miller algorithm we have that the final exponentiation is $\frac{p^{36}-1}{r}$. The efficient computation of final exponentiation take a lot of attention. Because this exponentiation can be divide into two parts as follow:

$$\frac{p^{36}-1}{r} = (\frac{p^{36}-1}{\phi_k(p)}).(\frac{\phi_k(p)}{r})$$

We can take $A = \frac{p^{36}-1}{\phi_k(p)}$ and $d = \frac{\phi_k(p)}{r}$, so that $f^{\frac{p^{18}-1}{r}} = (f^A)^d$.
The goal of this final exponentiation is to raise the function $f \in \mathbb{F}_{p^k}$ in the miller loop result, to the $\frac{p^{36}-1}{r}$ -th power. As we see above, this can be broken into two part, $\frac{p^{36}-1}{r} = (\frac{p^{36}-1}{\phi_k(p)}).(\frac{\phi_k(p)}{r})$. Computing $f^A = f^{\frac{p^{36}-1}{\phi_k(p)}}$ is considered easy, consting only a few multiplication and inversion, and inexpensive p-th powering in $\mathbb{F}_{p^k}$. But the calculation of the power $d = \frac{\phi_k(p)}{r}$ is a more hard to do.
We can see that: $p^{36} - 1 = (p^{18} - 1)(p^{18} + 1)$ or $p^{36} - 1 = (p^{12} - 1)(p^{24} + p^{12} + 1)$

Curve	*Final exponentiation*	*Easy part*	*Hard part*
KSS-36	$\frac{p^{36}-1}{r}$	$p^{12} - 1$	$\frac{p^{24}+p^{12}+1}{r}$
KSS-36	$\frac{p^{36}-1}{r}$	$p^{18} - 1$	$\frac{p^{18}+1}{r}$

The exponentiation $f^{\frac{p^{36}-1}{r}}$ can be computed using the following multiplication-powering-inversion chain:

- $f \to f^p \to ((f^p)^p)^p = f^{p^3} \to ((f^{p^3})^{p^3})^{p^3}$
$$= f^{p^9} \to (f^{p^9})^{p^9} = f^{p^{18}}$$
$$f \to \frac{f^{p^{18}}}{f} = f^{p^{18}-1}$$
$$f \to f^{p^{18}}.f = f^{p^{18}+1}$$
$$f \to f^{p^{18}-1}.f^{p^{18}+1} = f^{p^{36}-1} \to f^{\frac{p^{36}-1}{r}}$$

The cost to calculate $f^{\frac{p^{36}-1}{r}}$ is

$$6(p-1)M_k + 2I_k + 2M_k$$

- *or* $f \to f^p \to ((f^p)^p)^p = f^{p^3} \to (f^{p^3})^{p^3}$
$$= f^{p^6} \to (f^{p^6})^{p^6} = f^{p^{12}}$$
$$f \to (f^{p^{12}})^{p^{12}} \to f^{p^{24}}$$
$$f \to \frac{f^{p^{12}}}{f} = f^{p^{12}-1}$$
$$f \to f^{p^{24}}.f^{p^{12}}.f = f^{p^{24}+p^{12}+1}$$
$$f \to f^{p^{12}-1}.f^{p^{24}+p^{12}+1} = f^{p^{36}-1} \to f^{\frac{p^{36}-1}{r}}$$

The cost to calculate $f^{\frac{p^{36}-1}{r}}$ is

$$6(p-1)M_k + 2I_k + 3M_k$$

So with working with the first case is a slight better than second case, so the cost of miller algorithm in this case is

$$\frac{l}{2}(6M_K+3S_k+2I_k)+6(p-1)M_k+6M_k+S_k+3I_k$$

Comparison

Here we shall give cost of operations (Multiplication, squaring and inversion) of the tower field that we use in every path possible

Table 1: Cost of operations in first path

Field	O	Cost
$\mathbb{F}_{p^4}$:	M_4	9m
	S_4	6m
	I_4	16m+i
$\mathbb{F}_{p^{12}}$:	M_{12}	54m
	S_{12}	36m
	I_{12}	105m+2s+i
$\mathbb{F}_{p^{36}}$:	M_{36}	324m
	S_{36}	216m
	I_{36}	639m+12s+i

Table 2: Cost of operations in second path

Field	O	Cost
$\mathbb{F}_{p^6}$:	M_6	18m
	S_6	12m
	I_6	33m+2s+i
$\mathbb{F}_{p^{12}}$:	M_{12}	54m
	S_{12}	36m
	I_{12}	107m+i
$\mathbb{F}_{p^{36}}$:	M_{36}	324m
	S_{36}	216m
	I_{36}	651m+2s+i

Table 3: Cost of operations in third path

Field	O	Cost
$\mathbb{F}_{p^6}$:	M_6	18m
	S_6	12m
	I_6	33m+2s+i
$\mathbb{F}_{p^{18}}$:	M_{18}	108m
	S_{18}	72m
	I_{18}	207m+12s+i
$\mathbb{F}_{p^{36}}$:	M_{36}	324m
	S_{36}	216m
	I_{36}	649m+i

Table 4: Cost of operations in fourth path

Field	O	Cost
$\mathbb{F}_{p^6}$:	M_6	18m
	S_6	10m
	I_6	35m+i
$\mathbb{F}_{p^{12}}$:	M_{12}	54m
	S_{12}	30m
	I_{12}	109m+i
$\mathbb{F}_{p^{36}}$:	M_{36}	324m
	S_{36}	180m
	I_{36}	663m+2s+i

Table 5: Cost of operations in fifth path

Field	O	Cost
$\mathbb{F}_{p^6}$:	M_6	18m
	S_6	10m
	I_6	35m+i
$\mathbb{F}_{p^{18}}$:	M_{18}	108m
	S_{18}	60m
	I_{18}	219m+2s+i
$\mathbb{F}_{p^{36}}$:	M_{36}	324m
	S_{36}	180m
	I_{36}	665m+i

Table 6: Cost of operations in sixth path

Field	O	Cost
$\mathbb{F}_{p^9}$:	M_9	36m
	S_9	25s
	I_9	73m+12s+i
$\mathbb{F}_{p^{18}}$:	M_{18}	108m
	S_{18}	50m
	I_{18}	217m+i
$\mathbb{F}_{p^{36}}$:	M_{36}	324m
	S_{36}	150m
	I_{36}	655m+i

In the tables above give the overall cost of operations in each the tower fields.
We found that the cost of multiplication is the same for any path chosen, however the cost of squaring and inversion change on the path, so we can see that the minimal cost for squaring is 150m (path 6) and inversion is 639m+12s+i (path 1), so to find the better path we shall calculate the cost of miller algorithm taking $S = 0.8M$ and $I = 40M$ in path 1 and 6, we have:
On path 1: (1964,6l+1944p+2308,8)m.
On path 6: (1892l+1944p+2235).
So we found that the optimal path to do this calculation is when we chose the sixth path, so the best path for tower building the elliptic curve of embedding degree 36 is:

$$\mathbb{F}_p \longrightarrow \mathbb{F}_{p^3} \longrightarrow \mathbb{F}_{p^9} \longrightarrow \mathbb{F}_{p^{18}} \longrightarrow \mathbb{F}_{p^{36}}$$

5. Conclusion

In this paper, we give some methods for tower building of extension of finite field of embedding degree 36. We show that there is three efficients constructions of these extensions of degree 36. We show that by using a degree 2 or 3 twist we handle to perform most of the operations in $\mathbb{F}_p$ or $\mathbb{F}_{p^9}$ or in $\mathbb{F}_p$ or $\mathbb{F}_{p^6}$. By using this tower building technique, we also improve the arithmetic of $\mathbb{F}_{p^6}$ and $\mathbb{F}_{p^9}$ in order to get better results of calculate the cost of their multiplication, squaring and inversion, and found the optimal path for tower building this field with the minimal cost.

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.