Tower building technique on elliptic curve with embedding degree 72

ISMAIL ASSOUJAA[1], SIHAM EZZOUAK[2] AND HAKIMA MOUANIS[3]
Departement of Mathematics (LASMA laboratory)
University Sidi Mohammed Ben Abdellah
Fez city
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 72. We use the tower building technique, and study the case when using a degree 2 or 3 twist to carry out most operations in $\mathbb{F}_{p^4}$, $\mathbb{F}_{p^6}$, $\mathbb{F}_{p^8}$, $\mathbb{F}_{p^9}$, $\mathbb{F}_{p^{12}}$, $\mathbb{F}_{p^{18}}$, $\mathbb{F}_{p^{24}}$, $\mathbb{F}_{p^{36}}$ and $\mathbb{F}_{p^{72}}$.

Key-Words: Optimal ate pairing, Miller Algorithm, Embedding degree 72, Twist curve

Received: May 12, 2022. Revised: October 26, 2022. Accepted: November 28, 2022. Published: December 31, 2022.

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 [6],[7],[8], [15] Nadia El and others show a study case of working with elliptic curve with embedding degree 5,9,15 and 27. Also in [10],[11],[12],[13] and [14] researchers show the case of working with curve with some embedding degree. In [9] they give a study of security level of optimal ate pairing, and other useful work (see [5]) .

In the present article, we seek to obtain efficient ways to pairing computation for curves of embedding degree 72. We will see how to improve arithmetic operation in curves with embedding degree 72 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 $\mathbb{F}_{p^2}$ and $\mathbb{F}_{p^4}$ or $\mathbb{F}_{p^6}$ and $\mathbb{F}_{p^{12}}$, and when we use a degree 3 twists, we can handle most operations in $\mathbb{F}_{p^3}$ and $\mathbb{F}_{p^6}$ or $\mathbb{F}_{p^6}$ or $\mathbb{F}_{p^9}$ and $\mathbb{F}_{p^{18}}$ instead. By making use of an tower building technique, we also improve the arithmetic of $\mathbb{F}_{p^9}$ and $\mathbb{F}_{p^6}$ in order to get better results. Finally we will compare these cases to know which one is the optimal arithmetic path on $\mathbb{F}_{p^2}$, $\mathbb{F}_{p^3}$, $\mathbb{F}_{p^4}$, $\mathbb{F}_{p^6}$, $\mathbb{F}_{p^8}$, $\mathbb{F}_{p^9}$, $\mathbb{F}_{p^{12}}$, $\mathbb{F}_{p^{18}}$, $\mathbb{F}_{p^{24}}$, $\mathbb{F}_{p^{36}}$ and $\mathbb{F}_{p^{72}}$

In this paper, we will investigate and examine what will happens in case of optimal ate pairing with embedding degree 72.

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 new techniques of tower building the elliptic curve of embedding degree 72. Section 4 will presents the optimal ate pairing used in our work. Finally, Section 5 we will calculate the operation cost in this tower

elds for each possible case and 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_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_8, S_8, I_8: multiplication, squaring, inversion in field $\mathbb{F}_{p^8}$.
- 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_{24}, S_{24}, I_{24}: multiplication, squaring, inversion in field $\mathbb{F}_{p^{24}}$.
- M_{36}, S_{36}, I_{36}: multiplication, squaring, inversion in field $\mathbb{F}_{p^{36}}$
- M_{72}, S_{72}, I_{72}: multiplication, squaring, inversion in field $\mathbb{F}_{p^{72}}$.

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 ([20]).
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 ([20]).

2.1 Pairing definition and proprieties:

Definition 2.1. *[18], 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:*

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

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

$$\begin{aligned} e(S_1 + S_2, T) &= e(S_1, T)e(S_2, T) \\ e(S, T_1 + T_2) &= e(S, T_1)e(S, T_2) \end{aligned}$$

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

$$\begin{aligned} \pi_p : \mathbb{F}_{p^m} &\rightarrow \mathbb{F}_{p^m} \\ a &\mapsto a^p \end{aligned}$$

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

$$\begin{aligned} \phi : E(\mathbb{F}_q) &\rightarrow E(\mathbb{F}_q) \\ P(x, y) &\mapsto (x^q, y^q). \\ P_\infty &\mapsto P_\infty. \end{aligned}$$

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

$\phi(Q) = [p]Q$.
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 [16]:
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 72:
As describe in ([9]-pp31), let k be a positive integer with $k < 1000$ and $3 \mid k$. Let $l = lcm(8, k)$, in our case ok $k = 72$, we found that $l = 72$

$$\begin{cases} q(x) = \frac{1}{8}(2(x^{\frac{l}{k}}+1)^2 + (1-x^{\frac{l}{k}})^2(x^{\frac{5l}{24}} + x^{\frac{l}{8}} - x^{\frac{l}{24}})^2) \\ = \frac{1}{8}(2(x^4+1)^2 + (1-x^4)^2(x^{15}+x^9-x^3)^2). \\ r(x) = \Phi_l(x) = \Phi_{72}(x) = x^{24} - x^{12} + 1. \\ t(x) = x^{l/k} + 1 = x^4 + 1. \end{cases}$$

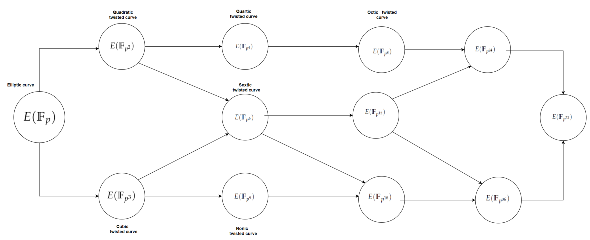
We can see that
$q(x) + 1 - t(x) = (x^{24} - x^{12} + 1)(x^{14} - 2x^{10} + 2x^8 + x^6 - 4x^4 + 2)/8$
hence $r(x)$ really divides $q(x) + 1 - t(x)$.
Twists of curves:
Let E be an elliptic curve of j-invariant 0, defined over $\mathbb{F}_p$. We have :

k	equation	isomorphism
k=d	$y^2 = x^3 + b$	$\psi_d : E'(\mathbb{F}_p) \to E(\mathbb{F}_{p^d})$ $\psi_d(x, y) = (xv^{2/d}, yv^{3/d})$.
k=2	$y^2 = x^3 + av^{-2}x + bv^{-3}$	$\psi_2 : E'(\mathbb{F}_p) \to E(\mathbb{F}_{p^2})$ $\psi_2(x, y) = (xv, yv^{3/2})$.
k=3	$E' : y^2 = x^3 + bv^{-2}$	$\psi_3 : E'(\mathbb{F}_p) \to E(\mathbb{F}_{p^3})$ $\psi_3(x, y) = (xv^{2/3}, yv)$.
k=4	$E' : y^2 = x^3 + av^{-1}x$	$\psi_4 : E'(\mathbb{F}_p) \to E(\mathbb{F}_{p^4})$ $\psi_4(x, y) = (xv^{1/2}, yv^{3/4})$.
k=6	$E' : y^2 = x^3 + bv^{-1}$	$\psi_6 : E'(\mathbb{F}_p) \to E(\mathbb{F}_{p^6})$ $\psi_6(x, y) = (xv^{1/3}, yv^{1/2})$.
k=8	$E' : y^2 = x^3 + bv^{-3/4}$	$\psi_8 : E'(\mathbb{F}_p) \to E(\mathbb{F}_{p^8})$ $\psi_8(x, y) = (xv^{2/d}, yv^{3/d})$.
k=9	$E' : y^2 = x^3 + bv^{-2/3}$	$\psi_9 : E'(\mathbb{F}_p) \to E(\mathbb{F}_{p^9})$ $\psi_9(x, y) = (xv^{2/9}, yv^{1/3})$.
k=12	$E' : y^2 = x^3 + bv^{-1/2}$	$\psi_{12} : E'(\mathbb{F}_p) \to E(\mathbb{F}_{p^{12}})$ $\psi_{12}(x, y) = (xv^{1/6}, yv^{1/4})$.
k=18	$E' : y^2 = x^3 + bv^{-1/3}$	$\psi_{18} : E'(\mathbb{F}_p) \to E(\mathbb{F}_{p^{18}})$ $\psi_{18}(x, y) = (xv^{1/9}, yv^{1/6})$.
k=24	$E' : y^2 = x^3 + bv^{-1/4}$	$\psi_{24} : E'(\mathbb{F}_p) \to E(\mathbb{F}_{p^{24}})$ $\psi_{24}(x, y) = (xv^{1/12}, yv^{1/8})$.
k=36	$E' : y^2 = x^3 + bv^{-1/6}$	$\psi_{36} : E'(\mathbb{F}_p) \to E(\mathbb{F}_{p^{36}})$ $\psi_{36}(x, y) = (xv^{1/18}, yv^{1/12})$.
k=72	$E' : y^2 = x^3 + bv^{-1/12}$	$\psi_{72} : E'(\mathbb{F}_p) \to E(\mathbb{F}_{p^{72}})$ $\psi_{72}(x, y) = (xv^{1/36}, yv^{1/24})$.

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 Elliptic Curve with Embedding Degree 72

The figure below show all path possible for building an elliptic curve with embedding degree 72

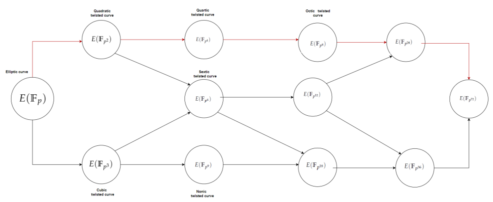


There is eight path possible to building this curve

$E(\mathbb{F}_p) \to E(\mathbb{F}_{p^2}) \to E(\mathbb{F}_{p^4}) \to E(\mathbb{F}_{p^8}) \to E(\mathbb{F}_{p^{24}}) \to E(\mathbb{F}_{p^{72}})$
$E(\mathbb{F}_p) \to E(\mathbb{F}_{p^2}) \to E(\mathbb{F}_{p^6}) \to E(\mathbb{F}_{p^{12}}) \to E(\mathbb{F}_{p^{24}}) \to E(\mathbb{F}_{p^{72}})$
$E(\mathbb{F}_p) \to E(\mathbb{F}_{p^2}) \to E(\mathbb{F}_{p^6}) \to E(\mathbb{F}_{p^{18}}) \to E(\mathbb{F}_{p^{36}}) \to E(\mathbb{F}_{p^{72}})$
$E(\mathbb{F}_p) \to E(\mathbb{F}_{p^2}) \to E(\mathbb{F}_{p^6}) \to E(\mathbb{F}_{p^{12}}) \to E(\mathbb{F}_{p^{36}}) \to E(\mathbb{F}_{p^{72}})$
$E(\mathbb{F}_p) \to E(\mathbb{F}_{p^3}) \to E(\mathbb{F}_{p^6}) \to E(\mathbb{F}_{p^{12}}) \to E(\mathbb{F}_{p^{24}}) \to E(\mathbb{F}_{p^{72}})$
$E(\mathbb{F}_p) \to E(\mathbb{F}_{p^3}) \to E(\mathbb{F}_{p^6}) \to E(\mathbb{F}_{p^{12}}) \to E(\mathbb{F}_{p^{36}}) \to E(\mathbb{F}_{p^{72}})$
$E(\mathbb{F}_p) \to E(\mathbb{F}_{p^3}) \to E(\mathbb{F}_{p^6}) \to E(\mathbb{F}_{p^{18}}) \to E(\mathbb{F}_{p^{36}}) \to E(\mathbb{F}_{p^{72}})$
$E(\mathbb{F}_p) \to E(\mathbb{F}_{p^3}) \to E(\mathbb{F}_{p^9}) \to E(\mathbb{F}_{p^{18}}) \to E(\mathbb{F}_{p^{36}}) \to E(\mathbb{F}_{p^{72}})$

Exploring the first path

$E(\mathbb{F}_p) \to E(\mathbb{F}_{p^2}) \to E(\mathbb{F}_{p^4}) \to E(\mathbb{F}_{p^8}) \to E(\mathbb{F}_{p^{24}}) \to E(\mathbb{F}_{p^{72}})$



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 $v^2 = 2^{1/2}$

$\mathbb{F}_{p^8} = \mathbb{F}_{p^4}[t]/(t^3-v),$ with t a non-square and $t^2 = 2^{1/4}$

$\mathbb{F}_{p^{24}} = \mathbb{F}_{p^8}[w]/(w^3-t),$ with w a non-cube and $w^3 = 2^{1/8}$

$\mathbb{F}_{p^{72}} = \mathbb{F}_{p^{24}}[w]/(w^3-t),$ with w a non-cube and $w^3 = 2^{\frac{1}{24}}$

Each rational point $P^5 \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{72}})$ has a special vector representation with 72 elements in $\mathbb{F}_p$ for each x^5 and y^5 coordinates. The construction below show that point $P^5 \in E(\mathbb{F}_{p^{72}})$ and its cubic twisted isomorphic rational point $P^4 \in E(\mathbb{F}_{p^{24}})$, which also has a cubic twisted isomorphic rational point $P''' \in E(\mathbb{F}_{p^8})$, that lead to a three quadratic twisted isomorphic rational point $P'' \in E(\mathbb{F}_{p^4})$, $P' \in E(\mathbb{F}_{p^2})$ and $P \in E(\mathbb{F}_p)$.

$$\begin{aligned}
P^5(x^5,y^5) &= ((a,0,...,0),(0,...,0,b)) \ / \ x^5,y^5 \in \mathbb{F}_{p^{72}}\\
P^4(x^4,y^4) &= ((a,0,...,0),(0,...,0,b)) \ / \ x^4,y^4 \in \mathbb{F}_{p^{24}}\\
P'''(x''',y''') &= ((a,0,...,0),(0,...,0,b)) \ / \ x''',y''' \in \mathbb{F}_{p^8}\\
P''(x'',y'') &= ((a,0,0,0),(0,0,0,b)) \text{ with } x'',y'' \in \mathbb{F}_{p^4}\\
P'(x',y') &= ((a,0),(0,b)) \text{ with } x',y' \in \mathbb{F}_{p^2}\\
P(x,y) &= (a,b) \text{ with } x,y \in \mathbb{F}_p
\end{aligned}$$

The cost of multiplication, squaring and inversion in in the 72^{th} twisted field $\mathbb{F}_{p^{72}}$ are:

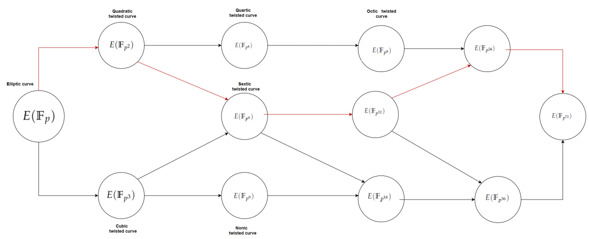
$$\begin{aligned}
M_{72} &= (M_{24})_{\mathbb{F}_{p^3}} = ((M_8)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = (((M_4)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}}\\
&= ((((M_2)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = ((((3m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}}\\
&= (((3M_2)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = (((9m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}}\\
&= ((9M_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = ((27m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = (27M_3)_{\mathbb{F}_{p^3}}\\
&= (162m)_{\mathbb{F}_{p^3}} = 162M_3 = 972m.
\end{aligned}$$

$$\begin{aligned}
S_{72} &= (S_{24})_{\mathbb{F}_{p^3}} = ((S_8)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = (((S_4)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}}\\
&= ((((S_2)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = ((((2m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}}\\
&= (((2M_2)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = (((6m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}}\\
&= ((6M_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = ((18m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = (18M_3)_{\mathbb{F}_{p^3}}\\
&= (108m)_{\mathbb{F}_{p^3}} = 108M_3 = 648m.
\end{aligned}$$

$$\begin{aligned}
I_{72} &= (I_{24})_{\mathbb{F}_{p^3}} = ((I_8)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = (((I_4)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}}\\
&= ((((I_2)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = ((((4m+i)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}}\\
&= (((4M_2+I_2)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = (((16m+i)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}}\\
&= ((16M_2+I_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}} = ((52m+i)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}}\\
&= (52M_3+I_3)_{\mathbb{F}_{p^3}} = (321m+2s+i)_{\mathbb{F}_{p^3}}\\
&= 321M_3+2S_3+I_3 = 1935m+12s+i.
\end{aligned}$$

Exploring the second path

$E(\mathbb{F}_p) \to E(\mathbb{F}_{p^2}) \to E(\mathbb{F}_{p^6}) \to E(\mathbb{F}_{p^{12}}) \to E(\mathbb{F}_{p^{24}}) \to E(\mathbb{F}_{p^{72}})$



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 $v^3 = 2^{1/2}$

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

$\mathbb{F}_{p^{24}} = \mathbb{F}_{p^{12}}[w]/(w^2-t),$ / w a non-square and $w^2 = 2^{1/12}$

$\mathbb{F}_{p^{72}} = \mathbb{F}_{p^{24}}[w]/(w^3-t),$ with w a non-cube and $w^3 = 2^{\frac{1}{24}}$

Each rational point $P^5 \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{72}})$ has a special vector representation with 72 elements in $\mathbb{F}_p$ for each x^5 and y^5 coordinates. The construction below show that point $P^5 \in E(\mathbb{F}_{p^{72}})$ and its cubic twisted isomorphic rational point $P^4 \in E(\mathbb{F}_{p^{24}})$, which also has a quadratic twisted isomorphic rational point $P''' \in E(\mathbb{F}_{p^{12}})$, that lead to a more quadratic twisted isomorphic rational point $P'' \in E(\mathbb{F}_{p^6})$ and its cubic twisted isomorphic rational point $P' \in E(\mathbb{F}_{p^2})$ and $P \in E(\mathbb{F}_p)$.

$$\begin{aligned}
P^5(x^5, y^5) &= ((a, 0, ..., 0), (0, ..., 0, b)) \ / \ x^5, y^5 \in \mathbb{F}_{p^{72}} \\
P^4(x^4, y^4) &= ((a, 0, ..., 0), (0, ..., 0, b)) \ / \ x^4, y^4 \in \mathbb{F}_{p^{24}} \\
P'''(x''', y''') &= ((a, 0, ..., 0), (0, ..., 0, b)) \ / \ x''', y''' \in \mathbb{F}_{p^{12}} \\
P''(x'', y'') &= ((a, 0, ..., 0), (0, ..., 0, b)) \ / \ x'', y'' \in \mathbb{F}_{p^6} \\
P'(x', y') &= ((a, 0), (0, b)) \text{ with } x', y' \in \mathbb{F}_{p^2} \\
P(x, y) &= (a, b) \text{ with } x, y \in \mathbb{F}_p
\end{aligned}$$

The cost of multiplication, squaring and inversion in in the 72^{th} twisted field $\mathbb{F}_{p^{72}}$ are:

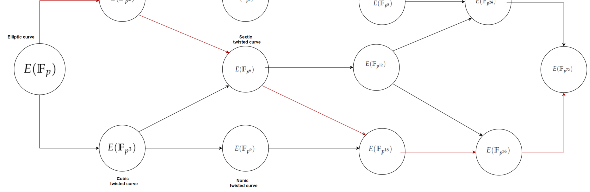
$$\begin{aligned}
M_{72} &= (M_{24})_{\mathbb{F}_{p^3}} = (M_{12})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = ((M_6)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\
&= (((M_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = (((3m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\
&= (((3M_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = (((18m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\
&= ((18M_2)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = ((54m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = (54M_2)_{\mathbb{F}_{p^3}} \\
&= (162m)_{\mathbb{F}_{p^3}} = 162M_3 = 972m.
\end{aligned}$$

$$\begin{aligned}
S_{72} &= (S_{24})_{\mathbb{F}_{p^3}} = (S_{12})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = ((S_6)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\
&= (((S_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = (((2m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\
&= (((2M_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = (((12m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\
&= ((12M_2)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = ((36m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = (36M_2)_{\mathbb{F}_{p^3}} \\
&= (108m)_{\mathbb{F}_{p^3}} = 108M_3 = 648m.
\end{aligned}$$

$$\begin{aligned}
I_{72} &= (I_{24})_{\mathbb{F}_{p^3}} = (I_{12})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = ((I_6)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\
&= (((I_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = (((4m+i)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\
&= (((4M_3+I_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = (((33m+2s+i)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\
&= ((33M_2+2S_2+I_2)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = ((107m+i)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\
&= (107M_2+I_2)_{\mathbb{F}_{p^3}} = (325m+i)_{\mathbb{F}_{p^3}} \\
&= 325M_3 + I_3 = 1959m + 2s + i.
\end{aligned}$$

Exploring the third path

$E(\mathbb{F}_p) \to E(\mathbb{F}_{p^2}) \to E(\mathbb{F}_{p^6}) \to E(\mathbb{F}_{p^{18}}) \to E(\mathbb{F}_{p^{36}}) \to E(\mathbb{F}_{p^{72}})$



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 $t^3 = 2^{1/6}$

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

$\mathbb{F}_{p^{72}} = \mathbb{F}_{p^{36}}[w]/(w^2 - t)$, / w a non-square and $w^2 = 2^{1/36}$

Each rational point $P^5 \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{72}})$ has a special vector representation with 72 elements in $\mathbb{F}_p$ for each x^5 and y^5 coordinates. The construction below show that point $P^5 \in E(\mathbb{F}_{p^{72}})$ and its quadratic twisted isomorphic rational point $P^4 \in E(\mathbb{F}_{p^{36}})$, which also has a quadratic twisted isomorphic rational point $P''' \in E(\mathbb{F}_{p^{18}})$, that lead to a more cubic twisted isomorphic rational point $P'' \in E(\mathbb{F}_{p^6})$ and its cubic twisted isomorphic rational point $P' \in E(\mathbb{F}_{p^2})$ and $P \in E(\mathbb{F}_p)$.

$$\begin{aligned}
P^5(x^5, y^5) &= ((a, 0, ..., 0), (0, ..., 0, b)) \ / \ x^5, y^5 \in \mathbb{F}_{p^{72}} \\
P^4(x^4, y^4) &= ((a, 0, ..., 0), (0, ..., 0, b)) \ / \ x^4, y^4 \in \mathbb{F}_{p^{36}} \\
P'''(x''', y''') &= ((a, 0, ..., 0), (0, ..., 0, b)) \ / \ x''', y''' \in \mathbb{F}_{p^{18}} \\
P''(x'', y'') &= ((a, 0, ..., 0), (0, ..., 0, b)) \ / \ x'', y'' \in \mathbb{F}_{p^6} \\
P'(x', y') &= ((a, 0), (0, b)) \text{ with } x', y' \in \mathbb{F}_{p^2} \\
P(x, y) &= (a, b) \text{ with } x, y \in \mathbb{F}_p
\end{aligned}$$

The cost of multiplication, squaring and inversion in in the 72^{th} twisted field $\mathbb{F}_{p^{72}}$ are:

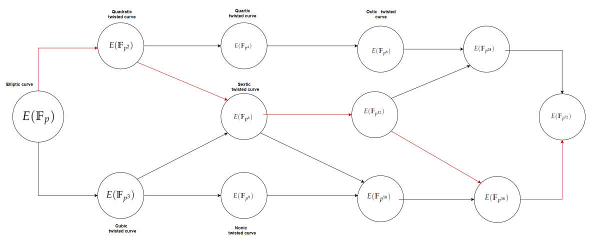
$$\begin{aligned}
M_{72} &= (M_{36})_{\mathbb{F}_{p^2}} = (M_{18})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = ((M_6)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\
&= (((M_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = (((3m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\
&= (((3M_3)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = (((18m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\
&= ((18M_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = ((108m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = (108M_2)_{\mathbb{F}_{p^2}} \\
&= (324m)_{\mathbb{F}_{p^2}} = 324M_2 = 972m.
\end{aligned}$$

$$\begin{aligned}
S_{72} &= (S_{36})_{\mathbb{F}_{p^2}} = (S_{18})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = ((S_6)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\
&= (((S_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = (((2m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\
&= (((2M_3)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = (((12m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\
&= ((12M_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = ((72m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = (72M_2)_{\mathbb{F}_{p^2}} \\
&= (216m)_{\mathbb{F}_{p^2}} = 216M_2 = 648m.
\end{aligned}$$

$$\begin{aligned} I_{72} &= (I_{36})_{\mathbb{F}_{p^2}} = ((I_{18})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = (((I_6)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\ &= ((((I_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = ((((4m+i)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\ &= (((4M_3+I_3)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\ &= (((33m+2s+i)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\ &= ((33M_3+2S_3+I_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\ &= ((207m+12s+i)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\ &= (207M_2+12S_2+I_2)_{\mathbb{F}_{p^2}} = (649m+i)_{\mathbb{F}_{p^2}} \\ &= 649M_2+I_2 = 1951m+i. \end{aligned}$$

Exploring the forth path

$E(\mathbb{F}_p) \to E(\mathbb{F}_{p^2}) \to E(\mathbb{F}_{p^6}) \to E(\mathbb{F}_{p^{12}}) \to E(\mathbb{F}_{p^{36}}) \to E(\mathbb{F}_{p^{72}})$



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 $t^2 = 2^{1/6}$

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

$\mathbb{F}_{p^{72}} = \mathbb{F}_{p^{36}}[z]/(z^2-w)$, / z a non-square and $z^2 = 2^{1/36}$

Each rational point $P^5 \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{72}})$ has a special vector representation with 72 elements in $\mathbb{F}_p$ for each x^5 and y^5 coordinates. The construction below show that point $P^5 \in E(\mathbb{F}_{p^{72}})$ and its quadratic twisted isomorphic rational point $P^4 \in E(\mathbb{F}_{p^{36}})$, which also has a cubic twisted isomorphic rational point $P''' \in E(\mathbb{F}_{p^{12}})$, that lead to a more quadratic twisted isomorphic rational point $P'' \in E(\mathbb{F}_{p^6})$ and its cubic twisted isomorphic rational point $P' \in E(\mathbb{F}_{p^2})$ and $P \in E(\mathbb{F}_p)$.

$$\begin{aligned} P^5(x^5,y^5) &= ((a,0,...,0),(0,...,0,b)) \ / \ x^5, y^5 \in \mathbb{F}_{p^{72}} \\ P^4(x^4,y^4) &= ((a,0,...,0),(0,...,0,b)) \ / \ x^4, y^4 \in \mathbb{F}_{p^{36}} \\ P'''(x''',y''') &= ((a,0,...,0),(0,...,0,b)) \ / \ x''', y''' \in \mathbb{F}_{p^{12}} \\ P''(x'',y'') &= ((a,0,...,0),(0,...,0,b)) \ / \ x'', y'' \in \mathbb{F}_{p^6} \\ P'(x',y') &= ((a,0),(0,b)) \text{ with } x', y' \in \mathbb{F}_{p^2} \\ P(x,y) &= (a,b) \text{ with } x, y \in \mathbb{F}_p \end{aligned}$$

The cost of multiplication, squaring and inversion in in the 72^{th} twisted field $\mathbb{F}_{p^{72}}$ are:

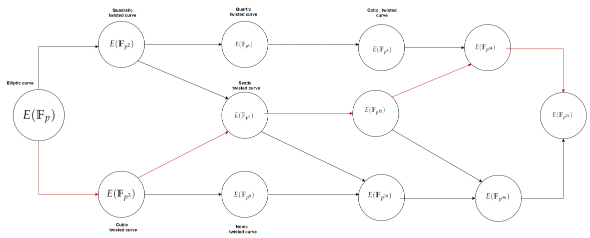
$$\begin{aligned} M_{72} &= (M_{36})_{\mathbb{F}_{p^2}} = ((M_{12})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = (((M_6)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\ &= ((((M_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = ((((3m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\ &= (((3M_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = (((18m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\ &= ((18M_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = ((54m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = (54M_3)_{\mathbb{F}_{p^2}} \\ &= (324m)_{\mathbb{F}_{p^2}} = 324M_2 = 972m. \end{aligned}$$

$$\begin{aligned} S_{72} &= (S_{36})_{\mathbb{F}_{p^2}} = ((S_{12})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = (((S_6)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\ &= ((((S_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = ((((2m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\ &= (((2M_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = (((12m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\ &= ((12M_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = ((36m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = (36M_3)_{\mathbb{F}_{p^2}} \\ &= (216m)_{\mathbb{F}_{p^2}} = 216M_2 = 648m. \end{aligned}$$

$$\begin{aligned} I_{72} &= (I_{36})_{\mathbb{F}_{p^2}} = ((I_{12})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = (((I_6)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\ &= ((((I_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = ((((4m+i)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\ &= (((4M_3+I_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\ &= (((33m+2s+i)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\ &= ((33M_2+2S_2+I_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\ &= ((107m+i)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = (107M_3+I_3)_{\mathbb{F}_{p^2}} \\ &= (651m+2s+i)_{\mathbb{F}_{p^2}} = 651M_2+2S_2+I_2 \\ &= 1961m+i. \end{aligned}$$

Exploring the fifth path

$E(\mathbb{F}_p) \to E(\mathbb{F}_{p^3}) \to E(\mathbb{F}_{p^6}) \to E(\mathbb{F}_{p^{12}}) \to E(\mathbb{F}_{p^{24}}) \to E(\mathbb{F}_{p^{72}})$



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 $v^2 = 2^{1/3}$

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

$\mathbb{F}_{p^{24}} = \mathbb{F}_{p^{12}}[w]/(w^2-t)$, / w a non-square and $w^2 = 2^{1/12}$

$\mathbb{F}_{p^{72}} = \mathbb{F}_{p^{24}}[z]/(z^3 - w),$ / w a non-cube and $z^3 = 2^{1/24}$

Each rational point $P^5 \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{72}})$ has a special vector representation with 72 elements in $\mathbb{F}_p$ for each x^5 and y^5 coordinates. The construction below show that point $P^5 \in E(\mathbb{F}_{p^{72}})$ and its cubic twisted isomorphic rational point $P^4 \in E(\mathbb{F}_{p^{24}})$, which also has a quadratic twisted isomorphic rational point $P''' \in E(\mathbb{F}_{p^{12}})$, that lead to a more quadratic twisted isomorphic rational point $P'' \in E(\mathbb{F}_{p^6})$ and its cubic twisted isomorphic rational point $P' \in E(\mathbb{F}_{p^3})$ and $P \in E(\mathbb{F}_p)$.

$$\begin{aligned}
P^5(x^5, y^5) &= ((a, 0, ..., 0), (0, ..., 0, b)) \text{ / } x^5, y^5 \in \mathbb{F}_{p^{72}} \\
P^4(x^4, y^4) &= ((a, 0, ..., 0), (0, ..., 0, b)) \text{ / } x^4, y^4 \in \mathbb{F}_{p^{24}} \\
P'''(x''', y''') &= ((a, 0, ..., 0), (0, ..., 0, b)) \text{ / } x''', y''' \in \mathbb{F}_{p^{12}} \\
P''(x'', y'') &= ((a, 0, ..., 0), (0, ..., 0, b)) \text{ / } x'', y'' \in \mathbb{F}_{p^6} \\
P'(x', y') &= ((a, 0, 0), (0, 0, b)) \text{ with } x', y' \in \mathbb{F}_{p^3} \\
P(x, y) &= (a, b) \text{ with } x, y \in \mathbb{F}_p
\end{aligned}$$

The cost of multiplication, squaring and inversion in in the 72^{th} twisted field $\mathbb{F}_{p^{72}}$ are:

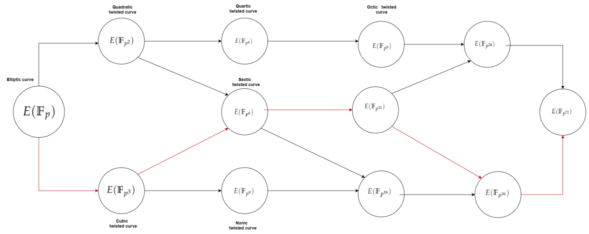
$$\begin{aligned}
M_{72} &= (M_{24})_{\mathbb{F}_{p^3}} = (M_{12})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = ((M_6)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\
&= (((M_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = (((6m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\
&= (((6M_2)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = (((18m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\
&= ((18M_2)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = ((54m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = (54M_2)_{\mathbb{F}_{p^3}} \\
&= (162m)_{\mathbb{F}_{p^3}} = 162M_3 = 972m.
\end{aligned}$$

$$\begin{aligned}
S_{72} &= (S_{24})_{\mathbb{F}_{p^3}} = (S_{12})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = ((S_6)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\
&= (((S_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = (((5s)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\
&= (((5S_2)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = (((10m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\
&= ((10M_2)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = ((30m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = (30M_2)_{\mathbb{F}_{p^3}} \\
&= (90m)_{\mathbb{F}_{p^3}} = 90M_3 = 540m.
\end{aligned}$$

$$\begin{aligned}
I_{72} &= (I_{24})_{\mathbb{F}_{p^3}} = (I_{12})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = ((I_6)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\
&= (((I_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\
&= (((9m + 2s + i)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\
&= (((9M_2 + 2S_2 + I_2)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\
&= (((35m + i)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\
&= ((35M_2 + I_2)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} = ((109m + i)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}} \\
&= (109M_2 + I_2)_{\mathbb{F}_{p^3}} = (331m + i)_{\mathbb{F}_{p^3}} \\
&= 331M_3 + I_3 = 1997m + 2s + i.
\end{aligned}$$

Exploring the sixth path

$$E(\mathbb{F}_p) \to E(\mathbb{F}_{p^3}) \to E(\mathbb{F}_{p^6}) \to E(\mathbb{F}_{p^{12}}) \to E(\mathbb{F}_{p^{36}}) \to E(\mathbb{F}_{p^{72}})$$



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 $v^2 = 2^{1/3}$

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

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

$\mathbb{F}_{p^{72}} = \mathbb{F}_{p^{36}}[z]/(z^2 - w),$ / z a non-square and $z^2 = 2^{1/36}$

Each rational point $P^5 \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{72}})$ has a special vector representation with 72 elements in $\mathbb{F}_p$ for each x^5 and y^5 coordinates. The construction below show that point $P^5 \in E(\mathbb{F}_{p^{72}})$ and its quadratic twisted isomorphic rational point $P^4 \in E(\mathbb{F}_{p^{36}})$, which also has a cubic twisted isomorphic rational point $P''' \in E(\mathbb{F}_{p^{12}})$, that lead to a more quadratic twisted isomorphic rational point $P'' \in E(\mathbb{F}_{p^6})$ and its cubic twisted isomorphic rational point $P' \in E(\mathbb{F}_{p^3})$ and $P \in E(\mathbb{F}_p)$.

$$\begin{aligned}
P^5(x^5, y^5) &= ((a, 0, ..., 0), (0, ..., 0, b)) \text{ / } x^5, y^5 \in \mathbb{F}_{p^{72}} \\
P^4(x^4, y^4) &= ((a, 0, ..., 0), (0, ..., 0, b)) \text{ / } x^4, y^4 \in \mathbb{F}_{p^{36}} \\
P'''(x''', y''') &= ((a, 0, ..., 0), (0, ..., 0, b)) \text{ / } x''', y''' \in \mathbb{F}_{p^{12}} \\
P''(x'', y'') &= ((a, 0, ..., 0), (0, ..., 0, b)) \text{ / } x'', y'' \in \mathbb{F}_{p^6} \\
P'(x', y') &= ((a, 0, 0), (0, 0, b)) \text{ with } x', y' \in \mathbb{F}_{p^3} \\
P(x, y) &= (a, b) \text{ with } x, y \in \mathbb{F}_p
\end{aligned}$$

The cost of multiplication, squaring and inversion in in the 72^{th} twisted field $\mathbb{F}_{p^{72}}$ are:

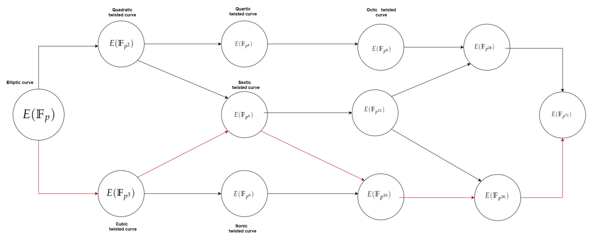
$$\begin{aligned}
M_{72} &= (M_{36})_{\mathbb{F}_{p^2}} = (M_{12})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = ((M_6)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\
&= (((M_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = (((6m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\
&= (((6M_2)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = (((18m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\
&= ((18M_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = ((54m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = (54M_3)_{\mathbb{F}_{p^2}} \\
&= (324m)_{\mathbb{F}_{p^2}} = 324M_2 = 972m.
\end{aligned}$$

$$\begin{aligned} S_{72} &= (S_{36})_{\mathbb{F}_{p^2}} = (S_{12})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = ((S_6)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\ &= (((S_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = (((5s)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\ &= (((5S_2)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = (((10m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\ &= ((10M_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = ((30m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = (30M_3)_{\mathbb{F}_{p^2}} \\ &= (180m)_{\mathbb{F}_{p^2}} = 180M_2 = 540m. \end{aligned}$$

$$\begin{aligned} I_{72} &= (I_{36})_{\mathbb{F}_{p^2}} = (I_{12})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = ((I_6)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\ &= (((I_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\ &= (((9m+2s+i)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\ &= (((9M_2+2S_2+I_2)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\ &= (((35m+i)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\ &= ((35M_2+I_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = ((109m+i)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} \\ &= (109M_3+I_3)_{\mathbb{F}_{p^2}} = (663m+2s+i)_{\mathbb{F}_{p^2}} \\ &= 663M_2+2S_2+I_2 = 1997m+i. \end{aligned}$$

Exploring the seventh path

$E(\mathbb{F}_p) \to E(\mathbb{F}_{p^3}) \to E(\mathbb{F}_{p^6}) \to E(\mathbb{F}_{p^{18}}) \to E(\mathbb{F}_{p^{36}}) \to E(\mathbb{F}_{p^{72}})$



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 $v^2 = 2^{1/3}$

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

$\mathbb{F}_{p^{36}} = \mathbb{F}_{p^{18}}[w]/(w^2-t)$, / w a non-square and $w^3 = 2^{1/18}$

$\mathbb{F}_{p^{72}} = \mathbb{F}_{p^{36}}[z]/(z^2-w)$, / z a non-square and $z^2 = 2^{1/36}$

Each rational point $P^5 \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{72}})$ has a special vector representation with 72 elements in $\mathbb{F}_p$ for each x^5 and y^5 coordinates. The construction below show that point $P^5 \in E(\mathbb{F}_{p^{72}})$ and its quadratic twisted isomorphic rational point $P^4 \in E(\mathbb{F}_{p^{36}})$, which also has a quadratic twisted isomorphic rational point $P''' \in E(\mathbb{F}_{p^{18}})$, that lead to a more cubic twisted isomorphic rational point $P'' \in E(\mathbb{F}_{p^6})$ and its cubic twisted isomorphic rational point $P' \in E(\mathbb{F}_{p^3})$ and $P \in E(\mathbb{F}_p)$.

$$\begin{aligned} P^5(x^5,y^5) &= ((a,0,...,0),(0,...,0,b)) \;/\; x^5,y^5 \in \mathbb{F}_{p^{72}} \\ P^4(x^4,y^4) &= ((a,0,...,0),(0,...,0,b)) \;/\; x^4,y^4 \in \mathbb{F}_{p^{36}} \\ P'''(x''',y''') &= ((a,0,...,0),(0,...,0,b)) \;/\; x''',y''' \in \mathbb{F}_{p^{18}} \\ P''(x'',y'') &= ((a,0,...,0),(0,...,0,b)) \;/\; x'',y'' \in \mathbb{F}_{p^6} \\ P'(x',y') &= ((a,0,0),(0,0,b)) \text{ with } x',y' \in \mathbb{F}_{p^3} \\ P(x,y) &= (a,b) \text{ with } x,y \in \mathbb{F}_p \end{aligned}$$

The cost of multiplication, squaring and inversion in in the 72^{th} twisted field $\mathbb{F}_{p^{72}}$ are:

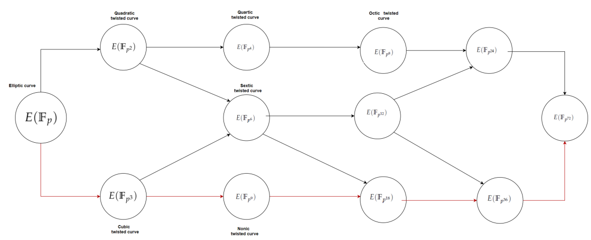
$$\begin{aligned} M_{72} &= (M_{36})_{\mathbb{F}_{p^2}} = (M_{18})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = ((M_6)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\ &= (((M_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = (((6m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\ &= (((6M_2)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}} = (((18m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\ &= ((18M_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = ((108m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = (108M_2)_{\mathbb{F}_{p^2}} \\ &= (324m)_{\mathbb{F}_{p^2}} = 324M_2 = 972m. \end{aligned}$$

$$\begin{aligned} S_{72} &= (S_{36})_{\mathbb{F}_{p^2}} = (S_{18})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = ((S_6)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\ &= (((S_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = (((5s)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\ &= (((5S_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = (((10m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\ &= ((10M_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = ((60m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = (60M_2)_{\mathbb{F}_{p^2}} \\ &= (180m)_{\mathbb{F}_{p^2}} = 180M_2 = 540m. \end{aligned}$$

$$\begin{aligned} I_{72} &= (I_{36})_{\mathbb{F}_{p^2}} = (I_{18})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = ((I_6)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\ &= (((I_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\ &= (((9m+2s+i)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\ &= (((9M_2+2S_2+I_2)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\ &= (((35m+i)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\ &= ((35M_3+I_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = ((219m+2s+i)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\ &= (219M_2+2S_2+I_2)_{\mathbb{F}_{p^2}} = (665m+i)_{\mathbb{F}_{p^2}} \\ &= 665M_2+I_2 = 1999m+i. \end{aligned}$$

Exploring the eighth path

$E(\mathbb{F}_p) \to E(\mathbb{F}_{p^3}) \to E(\mathbb{F}_{p^9}) \to E(\mathbb{F}_{p^{18}}) \to E(\mathbb{F}_{p^{36}}) \to E(\mathbb{F}_{p^{72}})$



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 $w^2 = 2^{1/18}$

$\mathbb{F}_{p^{72}} = \mathbb{F}_{p^{36}}[z]/(z^2-w)$, / z a non-square and $z^2 = 2^{1/36}$

Each rational point $P^5 \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{72}})$ has a special vector representation with 72 elements in $\mathbb{F}_p$ for each x^5 and y^5 coordinates. The construction below show that point $P^5 \in E(\mathbb{F}_{p^{72}})$ and its quadratic twisted isomorphic rational point $P^4 \in E(\mathbb{F}_{p^{36}})$, which also has a quadratic twisted isomorphic rational point $P''' \in E(\mathbb{F}_{p^{18}})$, that lead to a more quadratic twisted isomorphic rational point $P'' \in E(\mathbb{F}_{p^9})$ and its cubic twisted isomorphic rational point $P' \in E(\mathbb{F}_{p^3})$ and $P \in E(\mathbb{F}_p)$.

$$
\begin{aligned}
P^5(x^5, y^5) &= ((a, 0, ..., 0), (0, ..., 0, b)) \ / \ x^5, y^5 \in \mathbb{F}_{p^{72}} \\
P^4(x^4, y^4) &= ((a, 0, ..., 0), (0, ..., 0, b)) \ / \ x^4, y^4 \in \mathbb{F}_{p^{36}} \\
P'''(x''', y''') &= ((a, 0, ..., 0), (0, ..., 0, b)) \ / \ x''', y''' \in \mathbb{F}_{p^{18}} \\
P''(x'', y'') &= ((a, 0, ..., 0), (0, ..., 0, b)) \ / \ x'', y'' \in \mathbb{F}_{p^9} \\
P'(x', y') &= ((a, 0, 0), (0, 0, b)) \text{ with } x', y' \in \mathbb{F}_{p^3} \\
P(x, y) &= (a, b) \text{ with } x, y \in \mathbb{F}_p
\end{aligned}
$$

The cost of multiplication, squaring and inversion in in the 72^{th} twisted field $\mathbb{F}_{p^{72}}$ are:

$$
\begin{aligned}
M_{72} &= (M_{36})_{\mathbb{F}_{p^2}} = ((M_{18})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = (((M_9)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\
&= (((M_3)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = (((6m)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\
&= (((6M_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = (((36m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\
&= ((36M_2)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = ((108m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = (108M_2)_{\mathbb{F}_{p^2}} \\
&= (324m)_{\mathbb{F}_{p^2}} = 324M_2 = 972m.
\end{aligned}
$$

$$
\begin{aligned}
S_{72} &= (S_{36})_{\mathbb{F}_{p^2}} = ((S_{18})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = (((S_9)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\
&= (((S_3)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = (((5s)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\
&= (((5S_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = (((25s)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\
&= ((25S_2)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = ((50m)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = (50M_2)_{\mathbb{F}_{p^2}} \\
&= (150m)_{\mathbb{F}_{p^2}} = 150M_2 = 450m.
\end{aligned}
$$

$$
\begin{aligned}
I_{72} &= (I_{36})_{\mathbb{F}_{p^2}} = ((I_{18})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} = (((I_9)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\
&= (((I_3)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\
&= (((9m + 2s + i)_{\mathbb{F}_{p^3}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\
&= (((9M_3 + 2S_3 + I_3)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\
&= (((63m + 12s + i)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\
&= ((63M_2 + 12S_2 + I_2)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\
&= ((217m + i)_{\mathbb{F}_{p^2}})_{\mathbb{F}_{p^2}} \\
&= (217M_2 + I_2)_{\mathbb{F}_{p^2}} = (655m + i)_{\mathbb{F}_{p^2}} \\
&= 655M_2 + I_2 = 1969m + i.
\end{aligned}
$$

4. Optimal Ate Pairing on Elliptic Curve with Embedding Degree 72

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 72):*
The Optimal ate pairing on elliptic curves with embedding degree 72 is define for $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$. We note it a_{opt}, such that:

$$
\begin{aligned}
a_{opt} : \mathbb{G}_2 \times \mathbb{G}_1 &\longrightarrow \mathbb{G}_3 \\
(Q, P) &\mapsto a_{opt}(Q, P) = f_{x,Q}(P)^{\frac{p^{72}-1}{r}}
\end{aligned}
$$

For optimal ate pairing with embedding degree 72 ([21]-pp30), we have:

$$(Q, P) \mapsto (f_{x,Q} . f_{3,Q}^p . l_{x[Q],[3p]Q}(P))^{\frac{p^{72}-1}{r}}$$

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

Algorithm 1 Optimal ate pairing with embedding degree 72

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: $f \leftarrow f^{\frac{p^{72}-1}{r}}$
13: return f

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

Proposition 4.1. .
In miller algorithm we have that the final exponentiation is $\frac{p^{72}-1}{r}$. The efficient computation of final exponentiation take a lot of attention. Because this exponentiation can be divide into two parts as follow: $\frac{p^{72}-1}{r} = (\frac{p^{72}-1}{\phi_k(p)}).(\frac{\phi_k(p)}{r})$

Remark 4.1. *We can take $A = \frac{p^{72}-1}{\phi_k(p)}$ and $d = \frac{\phi_k(p)}{r}$, so that $f^{\frac{p^{72}-1}{r}} = (f^A)^d$.*

The goal of this final exponentiation is to raise the function $f \in \mathbb{F}_{p^k}$ in the miller loop result, to the $\frac{p^{72}-1}{r}$ -th power. As we see above, this can be broken into two part, $\frac{p^{72}-1}{r} = (\frac{p^{72}-1}{\phi_k(p)}).(\frac{\phi_k(p)}{r})$. Computing $f^A = f^{\frac{p^{72}-1}{\phi_k(p)}}$ 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: $p^{72} - 1 = (p^{36} - 1)(p^{36} + 1)$ or $p^{72} - 1 = (p^{24} - 1)(p^{48} + p^{24} + 1)$

Curve	Final exponentiation	Easy part	Hard part
KSS-72	$\frac{p^{72}-1}{r}$	$p^{24} - 1$	$\frac{p^{48}+p^{24}+1}{r}$
KSS-72	$\frac{p^{72}-1}{r}$	$p^{36} - 1$	$\frac{p^{36}+1}{r}$

The exponentiation $f^{\frac{p^{72}-1}{r}}$ can be computed using the following multiplication-powering-inversion chain:

- $f \to f^p \to ((f^p)^p)^p = f^{p^3} \to ((f^{p^3})^{p^3})^{p^3}$
$= f^{p^9} \to (f^{p^9})^{p^9} = f^{p^{18}} = (f^{p^{18}})^{p^{18}} = f^{p^{36}}$
$$f \to \frac{f^{p^{36}}}{f} = f^{p^{36}-1}$$
$$f \to f^{p^{36}}.f = f^{p^{36}+1}$$
$$f \to f^{p^{36}-1}.f^{p^{36}+1} = f^{p^{72}-1} \to f^{\frac{p^{72}-1}{r}}$$

The cost to calculate $f^{\frac{p^{72}-1}{r}}$ is

$$7(p-1)M_k + 2I_k + 2M_k$$

- or $f \to f^p \to ((f^p)^p)^p = f^{p^3} \to (f^{p^3})^{p^3}$
$= f^{p^6} \to (f^{p^6})^{p^6} = f^{p^{12}} = (f^{p^{12}})^{p^{12}} = f^{p^{24}}$
$$f \to (f^{p^{24}})^{p^{24}} \to f^{p^{48}}$$
$$f \to \frac{f^{p^{24}}}{f} = f^{p^{24}-1}$$
$$f \to f^{p^{48}}.f^{p^{24}}.f = f^{p^{48}+p^{24}+1}$$
$$f \to f^{p^{24}-1}.f^{p^{48}+p^{24}+1} = f^{p^{72}-1} \to f^{\frac{p^{72}-1}{r}}$$

The cost for computing $f^{\frac{p^{72}-1}{r}}$ is

$$7(p-1)M_k + 2I_k + 3M_k$$

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

$$\frac{l}{2}(6M_K + 3S_k + 2I_k) + 7(p-1)M_k + 6M_k + S_k + 3I_k$$

5. Comparison

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
$\mathbb{F}_{p^8}$:	M_8	27m
	S_8	18m
	I_8	52m+i
$\mathbb{F}_{p^{24}}$:	M_{24}	162m
	S_{24}	108m
	I_{24}	321m+2s+i
$\mathbb{F}_{p^{72}}$:	M_{72}	972m
	S_{72}	648m
	I_{72}	1935m+12s+i

Table 2: Cost of operations in second path

Field	O	Cost
$\mathbb{F}_{p^6}$:	M_6	18m
	S_6	2m
	I_6	33m+2s+i
$\mathbb{F}_{p^{12}}$:	M_{12}	54m
	S_{12}	12m
	I_{12}	107m+i
$\mathbb{F}_{p^{24}}$:	M_{24}	162m
	S_{24}	36m
	I_{24}	325m+2s+i
$\mathbb{F}_{p^{72}}$:	M_{72}	972m
	S_{72}	648m
	I_{72}	1943m+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}	36m
	I_{18}	207m+12s+i
$\mathbb{F}_{p^{36}}$:	M_{36}	324m
	S_{36}	108m
	I_{36}	649m+i
$\mathbb{F}_{p^{72}}$:	M_{72}	972m
	S_{72}	648m
	I_{72}	1951m+i

Table 4: Cost of operations in forth 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}	661m++2si
$\mathbb{F}_{p^{72}}$:	M_{72}	972m
	S_{72}	648m
	I_{72}	1961m+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
$\mathbb{F}_{p^{12}}$:	M_{12}	54m
	S_{12}	30m
	I_{12}	109m+i
$\mathbb{F}_{p^{24}}$:	M_{24}	162m
	S_{24}	90m
	I_{24}	331m+i
$\mathbb{F}_{p^{72}}$:	M_{72}	972m
	S_{72}	540m
	I_{72}	1997m+2s+i

Table 6: Cost of operations in sixth 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
$\mathbb{F}_{p^{72}}$:	M_{72}	972m
	S_{72}	540m
	I_{72}	1997m+i

Table 7: Cost of operations in seventh 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
$\mathbb{F}_{p^{72}}$:	M_{72}	972m
	S_{72}	540m
	I_{72}	1999m+i

Table 8: Cost of operations in eighth path

Field	O	Cost
$\mathbb{F}_{p^9}$:	M_9	36m
	S_9	25s
	I_9	63m+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
$\mathbb{F}_{p^{72}}$:	M_{72}	972m
	S_{72}	450m
	I_{72}	1969m+i

In the tables above, we give the overall cost of operations in each the tower fields. We found that the cost of multiplication is the same whatever the path, however the cost of squaring and inversion change on the path, so we can see that the minimal cost for squaring is 450m (path 8) and inversion is 1935m+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 3, we have:
On path 1:

$$\frac{l}{2}(6M_{72}+3S_{72}+2I_{72})+7(p-1)M_{72}+6M_{72}+S_{72}+3I_{72} = (5872.6l + 6804p + 5629, 8)m.$$

On path 8:

$$\frac{l}{2}(6M_{72} + 3S_{72} + 2I_{72}) + 7(p - 1)M_{72} + 6M_{72} + S_{72} + 3I_{72} = (5600l + 6804p + 5505)m.$$

So we found that the optimal path to do this calculation is when we chose the eighth path, so the best path for tower building the elliptic curve of embedding degree 72 is:

$$E(\mathbb{F}_p) \to E(\mathbb{F}_{p^3}) \to E(\mathbb{F}_{p^9}) \to E(\mathbb{F}_{p^{18}}) \to E(\mathbb{F}_{p^{36}}) \to E(\mathbb{F}_{p^{72}})$$

6. Conclusion

In this paper, we give some methods for tower building of extension of finite field of embedding degree 72. We show that there are two efficients constructions of these extensions of degree 72. We show that by using a degree 2 or 3 twist we handle to perform most of the operations in $\mathbb{F}_{p^4}$, $\mathbb{F}_{p^6}$, $\mathbb{F}_{p^8}$, $\mathbb{F}_{p^9}$, $\mathbb{F}_{p^{12}}$, $\mathbb{F}_{p^{18}}$, $\mathbb{F}_{p^{24}}$, $\mathbb{F}_{p^{36}}$ and $\mathbb{F}_{p^{72}}$. By using this tower building technique, we also improve the arithmetic of $\mathbb{F}_{p^{72}}$ in order to speed up miller algorithm by reducing the cost of 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 public-key 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] ISMAIL ASSOUJAA, SIHAM EZZOUAK, HAKIMA MOUANIS. Compression Point in Field of Characteristic 3. Springer, I4CS 2022, CCIS 1747, pp. 104–111, 2022. https://doi.org/10.1007/978-3-031-23201-5_7.

[6] Nadia El Mrabet, Nicolas Guillermin, and Sorina Ionica. A study of pairing computation for curves with embedding degree 15. DBLP volume 2009.

[7] Nadia El Mrabet and Marc Joye. GUIDE TO PAIRING-BASED CRYPTOGRAPHY. Chapman and Hall/CRC CRYPTOGRAPHY AND NETWORK SECURITY, 2018.

[8] 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

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

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

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

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

[19] 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.

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

[21] Razvan Barbulescu, Sylvain Duquesne, Updating Key Size Estimations for Pairings, J Cryptol. 2019.