sciendo

TATRA MOUNTAINS
Mathematical Publications

DOI: 10.2478/tmmp-2023-0008
Tatra Mt. Math. Publ. **83** (2023), 103–118

TOWER BUILDING TECHNIQUE ON ELLIPTIC CURVE WITH EMBEDDING DEGREE 18

Ismail Assoujaa—Siham Ezzouak—Hakima Mouanis

University Sidi Mohammed Ben Abdellah, Fez, MOROCCO

ABSTRACT. Pairing based cryptography is one of the best security solution that devote a lot of attention. So, to make pairing practical, secure and computationally efficient, we choose to work with extension finite field of the form $\mathbb{F}_{p^k}$ with $k \geq 12$. In this paper, we focus on the case of curves with embedding degree 18. We use the tower building technique, and study the case of degree 2 or 3 twist to carry out most arithmetics operations in $\mathbb{F}_{p^2}$, $\mathbb{F}_{p^3}$, $\mathbb{F}_{p^6}$, $\mathbb{F}_{p^9}$ and $\mathbb{F}_{p^{18}}$, thus we speed up the computation in optimal ate pairing.

1. Introduction

After the discovering of pairing-based cryptography, developers and researchers have been studying and improving 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 appeared like tate pairing, ate pairing and a lot more. The benefice of Elliptic curve cryptosystems which was discovered by Neal Koblitz [1] and Victor Miller [2] are to reduce the key sizes of the keys utilize in public key cryptography. Some works like presented in [3] interested in signature numeric. The authors in [4] show that we can use the final exponentiation in pairings as one of the countermeasures against fault attacks. In [5–7,13] Nadia El and others show a study case of working with elliptic curve with embedding degree 5, 9, 15 and 27. Also in [9–12] researchers show the case of working with curve with embedding degree 18. In [8] they give a study of security level of optimal ate pairing.

2020 Mathematics Subject Classification: 11T71, 14G50.
Keywords: optimal ate pairing, Miller algorithm, embedding degree 18, twist curve.

In the present article, we seek to obtain efficient ways to pairing computation for curves of embedding degree 18. We will see how to improve arithmetic operation in curves with embedding degree 18 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 $\mathbb{F}_{p^6}$, and when we use a degree 3 twists, we can handle most operations in $\mathbb{F}_{p^3}$ and $\mathbb{F}_{p^6}$ or $\mathbb{F}_{p^9}$ 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 $\mathbb{F}_{p^6}$, $\mathbb{F}_{p^9}$ and $\mathbb{F}_{p^{18}}$

In this paper, we will investigate and examine what will happens in case of optimal ate pairing with embedding degree 18.

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 tower building technique used in this work. Section 4 will presents the optimal ate pairing used in our work. Finally, Section 5 we will calculate the operation cost in this tower fields 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 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;
- $\mathbb{G}_1 \subset \big(E(\mathbb{F}_p)\big)$: additive group of cardinal $n \in \mathbb{N}^*$;
- $\mathbb{G}_2 \subset \big(E(\mathbb{F}_{p^k})\big)$: additive group of cardinal $n \in \mathbb{N}^*$;
- $\mathbb{G}_3 \subset \mathbb{F}_{p^k}^* \subset \mu_n$: cyclic multiplicative group of cardinal $n \in \mathbb{N}^*$;
- $E[r]$ or $E(\mathbb{F}_p)[r]$: The subgroup of $E(\mathbb{F}_p)$ with order r;
- $\mu_n = \{u \in \bar{\mathbb{F}_p} | u^n = 1\}$;
- 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_6, S_6, I_6: multiplication, squaring, inversion in field $\mathbb{F}_{p^6}$;
- M_9, S_9, I_9: multiplication, squaring, inversion in field $\mathbb{F}_{p^9}$;
- M_{18}, S_{18}, I_{18}: multiplication, squaring, inversion in field $\mathbb{F}_{p^{18}}$;
- π_p: Frobenius map in field $\mathbb{F}_p$;
- ϕ: Frobenius map in $E(\mathbb{F}_p)$.

2.1. Pairing definition and proprieties

Definition 2.1 ([16]). Let $(\mathbb{G}_1, +)$, $(\mathbb{G}_2, +)$ and $(\mathbb{G}_3, \cdot)$ be 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

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

defined by:

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

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:

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

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

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

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

$$\phi(P) = P \quad \text{and} \quad \phi(Q) = [p]Q\,.$$

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 $E(\mathbb{F}_p)$.

$$f_{t-1,Q} = (t-1)(Q) - ([t-1]Q) - (t-2)(P_\infty).$$

2.2. 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 the ability 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.

3. Tower building technique for elliptic curve with embedding degree 18

3.1. KSS-18 Curves

The equation of KSS-18 curve over $\mathbb{F}_{p^{18}}$ is given by,([17]-pp. 9)

$$(E) : y^2 = x^3 + b, \quad \text{with} \quad b \in \mathbb{F}_p\,.$$

Their polynomials $p(x)$, $r(x)$ and $t(x)$ are parametrized by x such that:

$$\begin{cases} p(x) = (x^8+5x^7+7x^6+37x^5+188x^4+259x^3+343x^2+1763x+2401)/21, \\ r(x) = x^6+37x^3+343, \\ t(x) = (x^4+16x+7)/7. \end{cases}$$

When $x \equiv 14 \mod 42$. The exponent $d = \Phi_k(p)/r$ is a degree-42 polynomial in the variable x and the ρ value is $\rho = \log_2 p/\log_2 r \approx 1.33\ldots$

TABLE 1. Twists of curves.

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

3.2. Twists of curves:

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

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 $\mathbb{F}_{p^3}$.

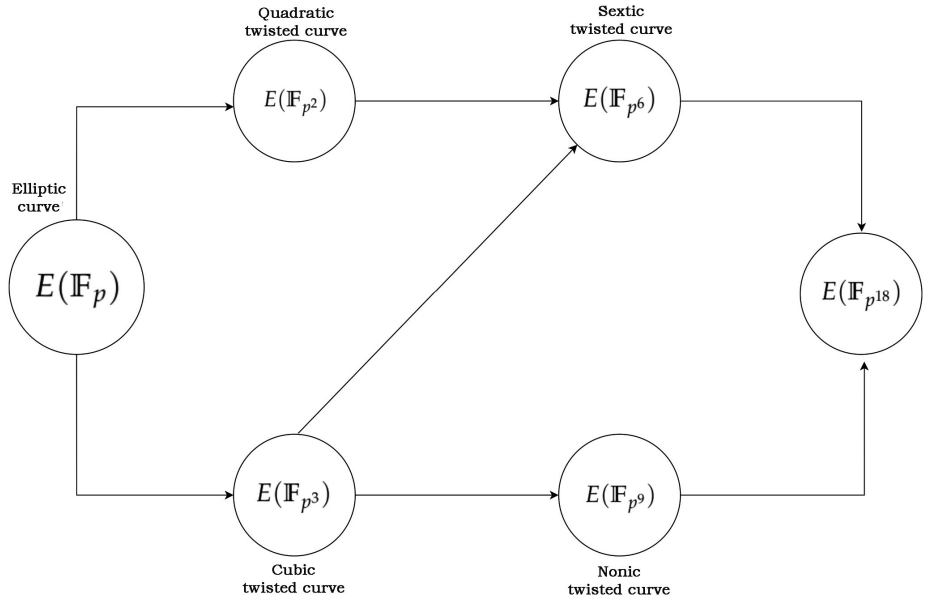

FIGURE 1. Tower building of elliptic curve with embedding degree 18.

In the figure above, we can see that to build the elliptic curve $E(\mathbb{F}_{p^{18}})$, we have three possible paths:

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

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

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

Each points P, Q, R in $E(\mathbb{F}_p)$ can be written in $E(\mathbb{F}_{p^{18}})$ linked to the path chosen (see [9], pp. 4). Each rational point P''', Q''', $R''' \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{18}})$ has a special vector representation with 18 elements in $\mathbb{F}_p$ for each x''' and y''' coordinates. Figure 2 below shows the structure of the coefficients of $P''' \in E(\mathbb{F}_{p^{18}})$ and its cubic twisted isomorphic rational point $P'' \in E(\mathbb{F}_{p^6})$, which also has a cubic twisted isomorphic rational point $P' \in E(\mathbb{F}_{p^2})$, that lead to a quadratic twisted isomorphic rational point $P \in E(\mathbb{F}_p)$.

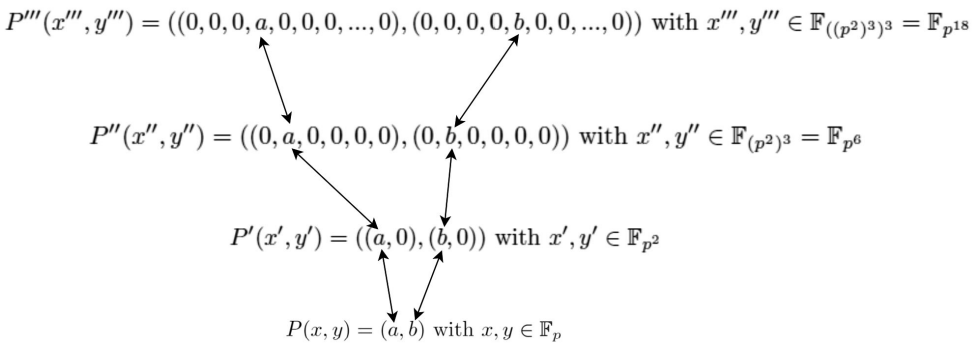

FIGURE 2. Easily mapping and remapping between P, P', P'' and P'''.

The same for other paths

$$\begin{aligned}
Q'''(x''', y''') &= \big((0,\ldots,0,a,0,0,0),(0,0,0,0,0,0,0,0,b,0,\ldots,0)\big) \\
&\quad \text{with } x''', y''' \in \mathbb{F}_{((p^3)^3)^2} = \mathbb{F}_{p^{18}}, \\
Q''(x'', y'') &= \big((0,0,0,0,0,0,0,a,0),(0,0,0,0,b,0,0,0,0)\big) \\
&\quad \text{with } x'', y'' \in \mathbb{F}_{(p^3)^3} = \mathbb{F}_{p^9}, \\
Q'(x', y') &= \big((0,0,a),(0,b,0)\big) \\
&\quad \text{with } x', y' \in \mathbb{F}_{p^3}, \\
Q(x, y) &= (a, b) \\
&\quad \text{with } x, y \in \mathbb{F}_p.
\end{aligned}$$

$$\begin{aligned}
R'''(x''', y''') &= \big((0,\ldots,0,a,0,0,0),(0,0,0,0,0,0,0,0,b,0,\ldots,0)\big) \\
&\quad \text{with } x''', y''' \in \mathbb{F}_{((p^3)^2)^3} = \mathbb{F}_{p^{18}}, \\
R''(x'', y'') &= \big((0,0,0,0,a,0),(0,0,b,0,0,0)\big) \\
&\quad \text{with } x'', y'' \in \mathbb{F}_{(p^3)^2} = \mathbb{F}_{p^6}, \\
R'(x', y') &= \big((0,0,a),(0,b,0)\big) \\
&\quad \text{with } x', y' \in \mathbb{F}_{p^3}, \\
R(x, y) &= (a, b) \\
&\quad \text{with } x, y \in \mathbb{F}_p.
\end{aligned}$$

4. Optimal ate pairing on elliptic curves with embedding degree 18

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 18)**.**
The Optimal ate pairing on elliptic curves with embedding degree 18 is define for

$$P \in \mathbb{G}_1 \quad \text{and} \quad Q \in \mathbb{G}_2.$$

We note it a_{opt}, such that:

$$a_{\text{opt}} : \mathbb{G}_2 \times \mathbb{G}_1 \longrightarrow \mathbb{G}_3$$
$$(Q, P) \mapsto a_{\text{opt}}(Q, P) = f_{x,Q}(P)^{\frac{p^{18}-1}{r}}$$

For optimal ate pairing with embedding degree 18 ([19], pp. 30), we have

$$(Q, P) \mapsto \left(f_{x,Q} \cdot f_{3,Q}^{p} \cdot l_{x[Q],[3p]Q}(P)\right)^{\frac{p^{18}-1}{r}}$$

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

Algorithm 1 Optimal ate pairing with embedding degree 18

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

$f \leftarrow 1$, $T \leftarrow Q$
for $i = l_{\log_2(l)-1}$ down to 0 do
$f \leftarrow f^2 \cdot\ l_{T,T}(P), T \leftarrow [2]T$
if $l_i = 1$ then
$f \leftarrow f \cdot\ l_{T,Q}(P), T \leftarrow T + Q$
end
end
$f_1 \leftarrow f^p$
$f \leftarrow f \cdot\ f_1$
$Q_1 \leftarrow x[Q]$, $Q_2 \leftarrow [3p]Q$
$f \leftarrow f \cdot\ l_{Q_1,Q_2}(P)$
$f \leftarrow f^{\frac{p^{18}-1}{r}}$
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 $\frac{p^{18}-1}{r}$. *The efficient computation of final exponentiation take a lot of attention. Because this exponentiation can be divide into two parts as follow:*

$$\frac{p^{18}-1}{r} = \left(\frac{p^{18}-1}{\phi_k(p)}\right) \cdot \left(\frac{\phi_k(p)}{r}\right).$$

Remark 1. We can take

$$A = \frac{p^{18}-1}{\phi_k(p)} \quad \text{and} \quad d = \frac{\phi_k(p)}{r},$$

so that

$$f^{\frac{p^{18}-1}{r}} = \left(f^A\right)^d.$$

The goal of this final exponentiation is to raise the function $f \in \mathbb{F}_{p^k}$ in the miller loop result, to the $\left(\frac{p^{18}-1}{r}\right)^{th}$ power. As we see above, this can be broken into two part,

$$\frac{p^{18}-1}{r} = \left(\frac{p^{18}-1}{\phi_k(p)}\right) \cdot \left(\frac{\phi_k(p)}{r}\right).$$

Computing $f^A = f^{\frac{p^{18}-1}{\phi_k(p)}}$ is considered easy, consting only a few multiplications and inversions, 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

$$p^{18}-1 = \left(p^9-1\right)\left(p^9+1\right) \quad \text{or} \quad p^{18}-1 = \left(p^6-1\right)\left(p^{12}+p^6+1\right).$$

So

$$\frac{p^{18}-1}{r} = (p^6-1)\left(\frac{p^{12}+p^6+1}{r}\right) \quad \text{or} \quad \frac{p^{18}-1}{r} = (p^9-1)\left(\frac{p^9+1}{r}\right).$$

Curve	Final exponentiation	Easy part	Hard part
KSS-18	$\frac{p^{18}-1}{r}$	p^6-1	$\frac{p^{12}+p^6+1}{r}$
KSS-18	$\frac{p^{18}-1}{r}$	p^9-1	$\frac{p^9+1}{r}$

The exponentiation $f^{\frac{p^{18}-1}{r}}$ can be computed using the following multiplication-powering-inversion chain:

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

The cost to calculate $f^{\frac{p^{36}-1}{r}}$ is $5(p-1)M_k + 2I_k + 2M_k$ or:

- $$f \to f^p \to \left((f^p)^p\right)^p = f^{p^3} \to \left(f^{p^3}\right)^{p^3} = f^{p^6} \to (f^{p^6})^{p^6} = f^{p^{12}},$$
$$f \to \frac{f^{p^6}}{f} = f^{p^6-1},$$
$$f \to f^{p^{12}} \cdot f^{p^6} \cdot f = f^{p^{12}+p^6+1},$$
$$f \to f^{p^6-1} \cdot f^{p^{12}+p^6+1} = f^{p^{18}-1} \to f^{\frac{p^{18}-1}{r}}.$$

The cost for computing $f^{\frac{p^{36}-1}{r}}$ is $5(p-1)M_k + 2I_k + 3M_k$. So with working with the first case is a slight better than second case, so the cost of miller algorithm in this case is

$$\frac{l}{2}(6M_K + 3S_k + 2I_k) + 5(p-1)M_k + 6M_k + S_k + 3I_k\,.$$

5. Operation cost in the tower fields of $\mathbb{F}_{p^{18}}$

5.1. Arithmetic in the Tower Fields of $\mathbb{F}_{p^{18}}$

The main building block of pairing computation is extension-field arithmetic. Hence, its efficient implementation is crucial. A popular choice consists of implementing the extension field through a tower of extensions, with appropriate choices of irreducible polynomials in all possible cases:

In the table below we considers $3|(p-1)$ and β is a quadratic and cubic non residue in $\mathbb{F}_p$.

$k = 2$	$\mathbb{F}_{p^2} = \mathbb{F}_p[u]/(u^2 - \beta)$, with β a non-square and $u^2 = 2$
$k = 6$	$\mathbb{F}_{p^6} = \mathbb{F}_{p^2}[v]/(v^3 - u)$, with u a non-cube and $v^3 = 2^{1/2}$
$k = 18$	So $\mathbb{F}_{p^{18}} = \mathbb{F}_{p^6}[t]/(t^3 - v)$ with v a non-cube and $t^3 = 2^{1/6}$.
$k = 3$	$\mathbb{F}_{p^3} = \mathbb{F}_p[u]/(u^3 - \beta)$, with (p-1) is divisble by 3 and β is quadratic and cubic non residue in $\mathbb{F}_p$, and $u^3 = 2$
$k = 6$	$\mathbb{F}_{p^6} = \mathbb{F}_{p^3}[v]/(v^2 - u)$, with u a non-square and $v^2 = 2^{1/3}$
$k = 18$	So $\mathbb{F}_{p^{18}} = \mathbb{F}_{p^6}[t]/(t^3 - v)$ with v a non-cube and $t^3 = 2^{1/6}$.
$k = 3$	$\mathbb{F}_{p^3} = \mathbb{F}_p[u]/(u^3 - \beta)$, with (p-1) is divisble by 3 and β is quadratic and cubic non residue in $\mathbb{F}_p$, and $u^3 = 2$
$k = 92$	$\mathbb{F}_{p^9} = \mathbb{F}_{p^3}[v]/(v^3 - u)$, with u a non-cube and $v^3 = 2^{1/3}$
$k = 18$	So $\mathbb{F}_{p^{18}} = \mathbb{F}_{p^9}[t]/(t^2 - v)$ with v a non-square and $t^2 = 2^{1/9}$.

5.2. Cost of operations

To calculate the cost of multiplication, squaring and inversion in the fields $\mathbb{F}_{p^6}$, $\mathbb{F}_{p^9}$ and $\mathbb{F}_{p^{18}}$, we will compute each operation depend on each chosen case. We already know that the cost of multiplication, squaring and inversion in the quadratic field $\mathbb{F}_{p^2}$ are $3m$, $2m$, $4m+i$, respectively ([18]).
Also, the cost of multiplication, squaring and inversion in the cubic twisted field $\mathbb{F}_{p^3}$ are $6m$, $5s$, $9m+2s+i$, respectively [18]).

First case:

$$\mathbb{F}_{p^2} \to \mathbb{F}_{p^6} \to \mathbb{F}_{p^{18}}.$$

- $M_2 = 3m$.
- $M_6 = (M_2)_{\mathbb{F}_{p^3}} = (3m)_{\mathbb{F}_{p^3}} = 3M_3 = 3 \times 6m = 18m$.
- $M_{18} = (M_6)_{\mathbb{F}_{p^3}} = (18m)_{\mathbb{F}_{p^3}} = 18M_3 = 18 \times 6m = 108m$
- $S_2 = 2m$.
- $S_6 = (S_2)_{\mathbb{F}_{p^3}} = (2m)_{\mathbb{F}_{p^3}} = 2M_3 = 2 \times 6 = 12m$.
- $S_{18} = (S_6)_{\mathbb{F}_{p^3}} = (12m)_{\mathbb{F}_{p^3}} = 12M_3 = 12 \times 6 = 72m$.
- $I_2 = 4m + i$.
- $I_6 = (I_2)_{\mathbb{F}_{p^3}} = (4m+i)_{\mathbb{F}_{p^3}} = 4M_3 + I_3 = 4 \times 6m + 9m + 2s + i = 33m + 2s + i$.
- $I_{18} = (I_6)_{\mathbb{F}_{p^3}} = (33m+2s+i)_{\mathbb{F}_{p^3}} = 33M_3 + 2S_3 + I_3 = 33 \times 6m + 2 \times 5s + 9m + 2s + i = 207m + 12s + i$.

Second case:

$$\mathbb{F}_{p^3} \to \mathbb{F}_{p^6} \to \mathbb{F}_{p^{18}}.$$

- $M_3 = 6m$.
- $M_6 = (M_3)_{\mathbb{F}_{p^2}} = (6m)_{\mathbb{F}_{p^2}} = 6M_2 = 6 \times 3m = 18m$.
- $M_{18} = (M_6)_{\mathbb{F}_{p^3}} = (18m)_{\mathbb{F}_{p^3}} = 18M_3 = 18 \times 6m = 108m$.
- $S_3 = 5s$.
- $S_6 = (S_3)_{\mathbb{F}_{p^2}} = (5s)_{\mathbb{F}_{p^2}} = 5S_2 = 5 \times 2m = 10m$.
- $S_{18} = (S_6)_{\mathbb{F}_{p^3}} = (10m)_{\mathbb{F}_{p^3}} = 10M_3 = 10 \times 6m = 60m$.
- $I_3 = 9m + 2s + i$.
- $I_6 = (I_3)_{\mathbb{F}_{p^2}} = (9m+2s+i)_{\mathbb{F}_{p^2}} = 9M_2 + 2S_2 + I_2 = 9 \times 3m + 2 \times 2m + 4m + i = 35m + i$.
- $I_{18} = (I_6)_{\mathbb{F}_{p^3}} = (35m+i)_{\mathbb{F}_{p^3}} = 35M_3 + I_3 = 219m + 2s + i$.

Third case:

$$\mathbb{F}_{p^3} \to \mathbb{F}_{p^9} \to \mathbb{F}_{p^{18}}.$$

- $M_3 = 6m$.
- $M_9 = (M_3)_{\mathbb{F}_{p^3}} = (6m)_{\mathbb{F}_{p^3}} = 6M_3 = 6 \times 6m = 36m$.
- $M_{18} = (M_9)_{\mathbb{F}_{p^2}} = (36m)_{\mathbb{F}_{p^2}} = 36M_2 = 36 \times 3m = 108m$
- $S_3 = 5s$.
- $S_9 = (S_3)_{\mathbb{F}_{p^3}} = (5s)_{\mathbb{F}_{p^3}} = 5S_3 = 5 \times 5s = 25s$.
- $S_{18} = (S_9)_{\mathbb{F}_{p^2}} = (25s)_{\mathbb{F}_{p^2}} = 25S_2 = 25 \times 2m = 50m$.
- $I_3 = 9m + 2s + i$.
- $I_9 = (I_3)_{\mathbb{F}_{p^2}} = (9m + 2s + i)_{\mathbb{F}_{p^3}} = 9M_3 + 2S_3 + I_3 = 9 \times 6m + 2 \times 5s + 9m + 2s + i = 63m + 12s + i$.
- $I_{18} = (I_9)_{\mathbb{F}_{p^2}} = (63m + 12s + i)_{\mathbb{F}_{p^2}} = 63M_2 + 12S_2 + I_2 = 217m + i$.

TABLE 2. Cost of operations in each tower fields

Path	Field	Operation	Cost
Path1	$\mathbb{F}_{p^2}$:	M_2, S_2, I_2	$3m, 2m, 4m + i$
	$\mathbb{F}_{p^6}$:	M_6, S_6, I_6	$18m, 12m, 33m + 2s + i$
	$\mathbb{F}_{p^{18}}$:	M_{18}, S_{18}, I_{18}	$108m, 72m, 207m + 12s + i$
Path2	$\mathbb{F}_{p^3}$:	M_3, S_3, I_3	$6m, 5s, 9m + 2s + i$
	$\mathbb{F}_{p^6}$:	M_6, S_6, I_6	$18m, 10m, 35m + i$
	$\mathbb{F}_{p^{18}}$:	M_{18}, S_{18}, I_{18}	$108m, 60m, 219m + 2s + i$
Path3	$\mathbb{F}_{p^3}$:	M_3, S_3, I_3	$6m, 5s, 9m + 2s + i$
	$\mathbb{F}_{p^9}$:	M_9, S_9, I_9	$36m, 25s, 63m + 12s + i$
	$\mathbb{F}_{p^{18}}$:	M_{18}, S_{18}, I_{18}	$108m$, $50m$, $217m + i$

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

On path 1:

$$\frac{l}{2}(6M_{18}+3S_{18}+2I_{18})+5(p-1)M_{18}+6M_{18}+S_{18}+3I_{18}$$
$$=(688,6l+540p+949,8)m.$$

On path 3:

$$\frac{l}{2}(6M_{18}+3S_{18}+2I_{18})+5(p-1)M_{18}+6M_{18}+S_{18}+3I_{18}$$
$$=(656l+540p+929)m.$$

So we found that the optimal path to do this calculation is when we chose the third path, so the best path for tower building the elliptic curve of embedding degree 18 is:

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

Security

We shall suppose that $\mathbb{F}_q$ is a prime power field, and we set $q = p^{18}$, in order for a pairing-based cryptosystem to be secure, the field $\mathbb{F}_{p^{18}}$ must be large enough so that discrete logs cannot feasibly be found using the best available algorithms (the number field and function field sieves). In order to determine the advantage of the proposal, we applied the proposed mapping technique from rational point $Q \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{18}})$ to its isomorphic point

$$Q' \in \mathbb{G}'_2 \subset E'(\mathbb{F}_{p^2}) \quad \text{or} \quad Q' \in \mathbb{G}'_2 \subset E'(\mathbb{F}_{p^3}).$$

The resulted points are re-mapped to $\mathbb{G}_2$ in $\mathbb{F}_{p^{18}}$. Scott et al. [15] has proposed the size of characteristics p to be 508 to 512-bit with order r of 376 to 384-bit for 192-bit security level.

This table below shows the minimum size of p and r to have $\rho \backsimeq \frac{4}{3}$, and so we yield the security level required.

Curve	Pairing	k	$\mathbb{G}_2$	Bits	Towering	$\log_2 p$	$\log_2 r$	ρ
KSS-192	a_{opt}	18	$\mathbb{F}_{p^2}$	512	1-2-6-18	508	376	$\backsimeq \frac{4}{3}$
KSS-192	a_{opt}	18	$\mathbb{F}_{p^3}$	512	1-3-6-18	508	376	$\backsimeq \frac{4}{3}$
KSS-192	a_{opt}	18	$\mathbb{F}_{p^3}$	512	1-3-9-18	511	378	$\backsimeq \frac{4}{3}$

Conclusion

In this paper, we give some methods for tower building of extension of finite field of embedding degree 18. We prove that there is two efficients constructions

of these extensions of degree 18. We prove that by using a degree 2 or 3 twist, we handle to perform most of the operations in $\mathbb{F}_{p^2}$ or $\mathbb{F}_{p^3}$ or in $\mathbb{F}_{p^6}$ or $\mathbb{F}_{p^9}$, $\mathbb{F}_{p^{18}}$. By using this tower building technique, we also improve the arithmetic of $\mathbb{F}_{p^6}$, $\mathbb{F}_{p^9}$ and $\mathbb{F}_{p^{18}}$ in order to speed up multiplication, squaring and inversion, and found the optimal path for tower building this field with the minimal cost.

REFERENCES

[1] MILLER, V. S.: *Use of elliptic curves in cryptography*, In: Advances in Cryptology—CRYPTO '85 (Santa Barbara, Calif., 1985), *Lecture Notes in Comput. Sci. Vol. 218*, Springer, Berlin, 1986. pp. 417–426.

[2] KOBLITZ, N.: *Elliptic curve cryptosystems*, Math. Comp. **48** (1987), no. 177, 203–209.

[3] RIVEST, R. L.—SHAMIR, A.—ADLEMAN, L. M.: *A method for obtaining digital signatures and public-key cryptosystems*, Comm. ACM, **21** (1978), no. 2, 120–126.

[4] WHELAN, C.—SCOTT, M.: *The Importance of the Final Exponentiation in Pairings When Considering Fault Attacks*. In: (T. Takagi, T.Okamoto, E. Okamoto, eds.) Pairing 2007. *Lecture Notes in Comput. Sci. Vol. 4575*, 2007, pp. 225–246.

[5] EL MRABET, N.—GUILLERMIN, N.—IONICA, S.: *A study of pairing computation for curves with embedding degree 15*, DBLP Vol. 2009.

[6] EL MRABET, N.—MARC JOYE, M.: *Guide to Pairing-Based Cryptography*. Cryptography and Network Security, Chapman and Hall/CRC Press, 2017.

[7] FOUOTSA, E.—EL MRABET, N.—PECHA, A.: *Optimal Ate pairing on elliptic curves with embedding degree 9; 15 and 27*, J. Groups Complex. Cryptol. **12** (2020), no. 1, Paper no. 3, 25 p.

[8] MBIANG, N. B.—DE FREITAS ARANHA, D.—FOUOTSA, E.: *Computing the optimal ate pairing over elliptic curves with embedding degrees 54 and 48 at the 256-bit security level*, Int. J. Appl. Cryptography, **4**, (2020) no. 1, 45–59.

[9] KHANDAKER, M. A.-A—PARK, T.—NOGAMI, Y.—KIM, H.: *A Comparative sdudy of Twist property in KSS curves of embedding degree 16 and 18 from the implementation perspective*, J. Inf. Commun. Convergence Engnr. **15** (2017), no. (2), 97–103.

[10] KHANDAKER, M. A.-A—NOGAMI, Y.: *Isomorphic mapping for ate-based pairing over KSS curve of embedding degree 18*. In: Fourth International Symposium on Computing and Networking (CANDAR). IEEE, 2016, pp. 629–634, DOI: 10.1109/CANDAR.2016.0113.

[11] AFREEN, R.—MEHROTRA, S. C.: *A review on elliptic curve cryptography for embedded systems*, Int. J. Comput. Sci. & Information Technology (IJCSIT), **3**, (2011) no. 3, arXiv preprint arXiv:1107.3631.

[12] KHANDAKER, M. A.-A—NOGAMI, Y.: *A consideration of towering scheme for efficient arithmetic operation over extension field of degree 18*. In: 19th International Conference on Computer and Information Technology, (ICCIT), Dhaka, Bangladesh, December 18–20, 2016, North South University, Dhaka, Bangladesh, 2016, pp. 276–281, DOI: 10.1109/ICCITECHN.2016.7860209.

[13] EL MRABET, N.—GUILLEVIC, A.—IONICA, S.: *Efficient multiplication in finite field extensions of degree 5*, In: Progress in Cryptology—AFRICACRYPT 2011, *Lecture Notes in Comput. Sci., Vol. 6737*, Springer, Heidelberg, 2011, pp. 188–205. DBLP 10.1007/978-3-642-21969-6-12

[14] SCOTT, M.—GUILLEVIC, A.: *A new family of pairing-friendly elliptic curves*, In: 7th International Workshop, WAIFI 2018, Bergen, Norway, June 14–16, 2018. Revised selected papers. (Lilya Budaghyan, ed. et al.) *Arithmetic of finite fields. Lect. Notes Comput. Sci. Vol. 11321*, Cham: Springer, 2018, pp. 43–57.

[15] SCOTT, M.: *On the efficient implementation of pairing-based protocols*, In: *Cryptography and Coding*, Springer-Verlag, Berlin, 2011. pp. 296–308,

[16] SILVERMAN, J. H.: *The Arithmetic of Elliptic Curves*. 2nd ed. Graduate Texts in Mathematics Vol. 106, Springer, New York, 2009.

[17] KACHISA, E. J.—SCHAEFER, E. F. —SCOTT, M.: *Constructing Brezing-Weng pairing-friendly elliptic curves using elements in the cyclotomic field*. In: Pairing-Based Cryptography–Pairing 2008: Second International Conference, Egham, UK, September 1–3, 2008. Proceedings 2. Springer-Verlag Berlin Heidelberg. pp. 126–135.

[18] DEVEGILI, A. J.—Ó'HÉIGEARTAIGH, C.—SCOTT, M.—DAHAB, R.: *Multiplication and squaring on pairing-friendly fields*, ePrint, 471, 2006.

[19] BARBULESCU, R.—DUQUESNE, S.: *Updating key size estimations for pairings*, J. Cryptol. **32** (2019), 1298–1336.

Received November 2, 2022

FSDM
LASMA Department
Faculty of science
University Sidi Mohammed Ben Abdellah
Fez, MOROCCO

E-mail: ismail.assoujja@usmba.ac.ma
siham.ezzouak@usmba.ac.ma
hmouanis@yahoo.fr