Optimal Ate Pairing on Elliptic Curves with Embedding Degree $9, 15$ and $27^\star$

Emmanuel Fouotsa[1] and Nadia El Mrabet[2] and Aminatou Pecha[2,3]

(1) LMNO,Université de Caen Basse Normandie, 14032 CAEN Cedex, France.
(1) Higher Teacher Training College, University of Bamenda, Cameroon
emmanuel.fouotsa@unicaen.fr
(2) LIASD − Université Paris 8 -France - elmrabet@ai.univ-paris8.fr
(2) SAS - CMP Gardanne - France - nadia.el-mrabet@emse.fr
(3) Institut Supérieur du Sahel, Université de Maroua
P.O. Box 46 Maroua, Cameroun
aminap2001@yahoo.fr

Abstract. Since the advent of pairing based cryptography, much attention has been given to efficient computation of pairings on elliptic curves with even embedding degrees. The few works that exist in the case of odd embedding degrees require some improvements. This paper considers the computation of optimal ate pairings on elliptic curves of embedding degrees $k = 9, 15$ and 27 which have twists of order three. Mainly, we provide a detailed arithmetic and cost estimation of operations in the tower field of the corresponding extension fields. A good selection of parameters at the 128, 192 and 256-bits security level enables us to improve the theoretical cost for the Miller step and the final exponentiation using the lattice-based method comparatively to the previous few works that exist in these cases. In particular for $k = 15$ we obtain an improvement up to 25% in the computation of the final exponentiation.

Keywords: Elliptic Curves, Optimal Pairings , Miller's algorithm , Extension fields arithmetic , Final exponentiation

1 Introduction

Pairings are bilinear maps defined on the group of rational points of elliptic or hyper elliptic curves [35]. They enable to realise many cryptographic protocols such as the Identity-Based cryptosystem [7], Identity-Based Encryption [9], the Identity-Based undeniable signature [27], short signatures [8] or Broadcast encryption [16]. A survey of some applications of pairings can be found in [13], [6, Chapter X]. These many applications justify the research on efficient computation of pairings. Generally, if E is an ordinary elliptic curve defined over a finite field $\mathbb{F}_q$ and r a large prime divisor of the order of the group $E(\mathbb{F}_q)$, the embedding degree of E with respect to r and q is the smallest integer k such that $r \mid q^k - 1$. The Tate pairing and its variants are the most used in cryptography. They map two linearly independent points of order r-subgroups of $E(\mathbb{F}_{q^k})$ to the group of $r-$th roots of unity in the finite fields $\mathbb{F}_{q^k}$. The computation of Tate pairings and its variants consists of an application of the Miller algorithm [31] and a final exponentiation. Efficient computation of pairings requires construction of pairing-friendly elliptic curves over $\mathbb{F}_q$ with prescribed embedding degree k (see for example [5] or [14]) and efficient

* This work was supported by French projects ANR SIMPATIC (ANR-12-INSE-0014) and LIRIMA-MACISA. The third author acknowledges support from The Simons Foundation through Pole of Research in Mathematics with applications to Information Security, Sub-Saharan Africa

arithmetic in the towering fields associated to $\mathbb{F}_{q^k}$ (see [24], [17], [22], [11]). Much works have been done for decreasing the Miller loop leading to the concept of pairing lattices [19], or the optimal pairing described by Vercauteren which can be computed with the smallest number of iterations in the Miller algorithm [34]. Due to these progress, the final exponentiation step has became a serious task. In this work, we concentrate on elliptic curves with embedding degree $9, 15$ and 27 at the $128, 192$ and 256-bit security level respectively according to recommendations in Table 1 [14]. These curves admit twists of degree three which enable computation to be done

Security level	Bit length of r	Bit length of q^k	k $\rho \approx 1$	k $\rho \approx 2$
80	160	$960 - 1280$	$6 - 8$	$3 - 4$
128	256	$3000 - 5000$	$12 - 20$	$6 - 10$
192	384	$8000 - 10000$	$20 - 26$	$10 - 13$
256	512	$14000 - 18000$	$28 - 36$	$14 - 18$

Table 1. Bit sizes of curves parameters and corresponding embedding degrees to obtain commonly desired levels of security.

in subfields and also lead to the denominator elimination technique. To our knowledge just few works ([26], [32] and [36]) exist in these cases and much attention have been given only to elliptic curves with even embedding degree (see for example [1],[15]). Also, another motivation to our work is the recent results on the resolution of discrete logarithm problem [23]. Indeed according to the first analysis of this article, as for instance in [18], the security level for elliptic curve with friable embedding degree should be taken greater than those presented in Table 1. The main consequence is that elliptic curves with embedding degree 12 or 18 may not be the one assuring a nice ratio between the security level and the arithmetic. Elliptic curves with odd embedding degree could become interesting and more efficient than elliptic curve with even embedding degree. As for now, we do not know how the attack of [23] will increase the size of fields and will modify the choice of good parameters for pairing computation, we still consider the Table 1 in order to make our comparison. So we proposed a detailed arithmetic in the towering fields associated to the fields $\mathbb{F}_{q^9}, \mathbb{F}_{q^{15}}$ and $\mathbb{F}_{q^{27}}$. The lattice-based method explained by Fuentes et *al.*[15] is applied to compute the final exponentiation in the cases $k = 9, 15$. We also find a simple expression and explicit cost evaluation for the optimal pairing in the cases $k = 9$ and $k = 15$ comparatively to the work in [32]. The results obtained are an improvement with respect to previous works [26], [32] and [36] respectively for $k = 9, 15$ and 27. Precisely, our contributions (see Table 3 for comparison) in this work are:

1. Determination of an explicit cost of the computation of the optimal pairing for elliptic curves stated above. This includes a good selection of parameters for a shorter Miller loop and an efficient exponentiation. In particular, we saved one inversion in $\mathbb{F}_{p^{27}}$ for the computation of the Miller loop in the case $k = 27$.
2. Details on the arithmetic in the tower fields of $\mathbb{F}_{q^9}, \mathbb{F}_{q^{15}}$ and $\mathbb{F}_{q^{27}}$. Especially, we give the cost of the computation of Frobenius maps and Inversions in the cyclotomic subgroups of $\mathbb{F}^{\star}_{q^9}, \mathbb{F}^{\star}_{q^{15}}$ and $\mathbb{F}^{\star}_{q^{27}}$, (see Appendices A, B and C).

3. Improvement of the costs of the final exponentiation by saving $24M_9 + 5S_9, 26M_{15} + 173S_{15}$ and $20M_{27}$ operations for elliptic curves of embedding degrees $9, 15$ and 27 respectively, comparatively to previous works in these cases.

The rest of this paper is organised as follows: In Section 2 we briefly present the Tate and ate pairings together with the Miller algorithm for their efficient computation, we also recall the concept of optimal ate pairing and the lattice-based method for computing the final exponentiation. Sections 4, 5 and 6 present arithmetic in sub fields, and cost estimation of the Miller step and the final exponentiation when considering the embedding degrees $k = 9, 15$ and 27 respectively. Each of these sections includes a comparative analysis with previous work. Section 7 presents a general comparison of the results obtained in this work and the previous results in the literature. We conclude the work in Section 8 in which we suggest as future work the search for parameters to have *subgroup secure* ordinary curves [3] and to ensure protection against *small-subgroup attacks*[29].

Notations

The following notations are used in this work.
M_k, S_k, I_k : Cost of multiplication, squaring and inversion in the field $\mathbb{F}_{q^k}$, for any integer k.
m_c, s_c, i_c : Cost of multiplication, squaring and inversion in the field $\mathbb{F}_q$ where the bit length of q is c.

2 Background and previous works

2.1 Pairings and the Miller Algorithm

Let E be an elliptic curve defined over $\mathbb{F}_q$, a finite field of characteristic $p > 3$. Let r be a large prime factor of the group order of the elliptic curve. Let $m \in \mathbb{Z}$, $P \in E(\mathbb{F}_q)[r]$ and $f_{m,P}$ a function with divisor Div $(f_{m,P}) = m(P) - ([m]P) - (m-1)(\mathcal{O})$ where $\mathcal{O}$ denotes the identity element of the group of points of the elliptic curve. Consider two points $P \in E(\mathbb{F}_q)[r]$ and $Q \in E(\mathbb{F}_{q^k})[r]$ of order r and μ_r the group of r-th roots of unity in $\mathbb{F}^*_{q^k}$. The reduced Tate pairing e_r is a bilinear and non degenerate map defined as

$$e_r : E(\mathbb{F}_q)[r] \times E(\mathbb{F}_{q^k})[r] \to \mu_r, (P, Q) \mapsto f_{r,P}(Q)^{\frac{q^k-1}{r}}$$

To define a variant of the Tate pairing called ate pairing [20], denote $[i] : P \longmapsto [i]P$ the endomorphism defined on $E(\mathbb{F}_q)$ which consists to add P to itself i times. Let $\pi_q : E\left(\overline{\mathbb{F}_q}\right) \to E\left(\overline{\mathbb{F}_q}\right), (x, y) \mapsto (x^q, y^q)$ be the Frobenius endomorphism on the curve where $\overline{\mathbb{F}_q}$ is the algebraic closure of the finite field $\mathbb{F}_q$. The relation between the trace t of the Frobenius endomorphism and the group order is given by [35, Theorem 4.3]: $\sharp E(\mathbb{F}_q) = q + 1 - t$ and π_q has exactly two eigenvalues 1 and q. This enables to consider $P \in \mathbb{G}_1 = E\left(\overline{\mathbb{F}_q}\right)[r] \cap \operatorname{Ker}(\pi_q - [1]) = E(\mathbb{F}_q)[r]$ and $Q \in \mathbb{G}_2 = E\left(\overline{\mathbb{F}_q}\right)[r] \cap \operatorname{Ker}(\pi_q - [q])$. The ate pairing is defined as follows:

$$e_A : \mathbb{G}_2 \times \mathbb{G}_1 \to \mu_r, (Q, P) \mapsto f_{t-1,Q}(P)^{\frac{q^k-1}{r}}.$$

In all variants of pairings, one needs a function $f_{m,U}(V)$ which is efficiently computed thanks to the Miller algorithm [31]. Indeed denote $h_{R,S}$ a rational function with divisor $\mathrm{Div}(h_{R,S}) =$

$(R)+(S)-(S+R)-(\mathcal{O})$ where R and S are two arbitrary points on the elliptic curve. In the case of elliptic curves in Weierstrass form, $h_{R,S} = \frac{\ell_{R,S}}{v_{R+S}}$ where $\ell_{R,S}$ is the straight line containing R and S and v_{R+S} is the corresponding vertical line passing through $R+S$. Miller uses the *double-and-add* method as the addition chains for m (see [2, Chapter 9] for more details on addition chains) to compute $f := f_{m,U}(V)$. Write $m = m_n 2^n + ... + m_1 2 + m_0 > 0$ with $m_i \in \{-1, 0, 1\}$, the (modified) Miller algorithm that computes efficiently the pairing $f_{m,U}(V)^{(q^k-1)/r}$ of two points U and V is given as follows:

1: Set $f \leftarrow 1$ and $R \leftarrow U$
2: **For** $i = n-1$ **down to** 0 **do**
3: $\quad f \leftarrow f^2 \cdot h_{R,R}(V)$, $\quad R \leftarrow 2R$ $\quad$ Doubling step
5: $\quad$ **if** $m_i = 1$ **then**
6: $\quad f \leftarrow f \cdot h_{R,U}(V)$ $\quad R \leftarrow R + U$, **end if** $\quad$ Addition step
7: $\quad$ **if** $m_i = -1$ **then**
8: $\quad f \leftarrow f / h_{R,U}(V)$ $\quad R \leftarrow R - U$, **end for** $\quad$ Addition step
10: **return** $e = f^{\frac{q^k-1}{r}}$ $\quad$ Final exponentiation

The use of twists enable to efficiently do some computations during the execution of this algorithm as we explain in the next section.

2.2 Use of Twists

Twists of elliptic curves enable to efficiently compute pairings. Indeed, in the Miller algorithm the doubling of point (lines 3) and the addition of points (lines 6 and 8) are done in the extension fields $\mathbb{F}_{q^k}$ in the case of ate pairing. The use of twists enables to perform these operations rather in a sub field of $\mathbb{F}_{q^k}$ and also leads to the denominator elimination. More precisely, a twist of an elliptic curve E defined over a finite field $\mathbb{F}_q$ is an elliptic curve E' defined over $\mathbb{F}_q$ which is isomorphic to E over an algebraic closure of $\mathbb{F}_q$. The smallest integer d such that E and E' are isomorphic over $\mathbb{F}_{q^d}$ is called the degree of the twist. Elliptic curves of embedding degree $k = 9, 15$ and $k = 27$ admit twists of order three. Explicit constructions of such curves can be found in [30], [12] and [4] . The general equation of these curves is given by $E : y^2 = x^3 + b$. The equation defining the twist E' has the form $y^2 = x^3 + b\omega^6$ where $\{1, \omega, \omega^2\}$ is the basis of the $\mathbb{F}_{q^{k/3}}$-vector space $\mathbb{F}_{q^k}$ and the isomorphism between E' and E is $\psi : E' \longrightarrow E; (x', y') \longmapsto (x'/\omega^2, y'/\omega^3)$. Using this isomorphism, points Q in $\mathbb{G}_2$ can be instead taken as $(x\omega^2, y\omega^3) \in \mathbb{G}'_2 \subset \psi^{-1}(E(\mathbb{F}_{q^{k/3}}))$ where $x, y \in \mathbb{F}_{q^{k/3}}$. More details on twists can be found in [10].

2.3 Optimal Pairings

The reduction of Miller's loop length is an important way to improve the computation of pairings. The latest work is a generalized method to find the shortest loop, which leads to the concept of optimal pairing due to Vercauteren [34]. Let $\lambda = mr$ be a multiple of r such that $r \nmid m$ and write $\lambda = \sum_{i=0}^{l} c_i q^i = h(q)$, $(h(z) \in \mathbb{Z}[z])$. Recall that $h_{R,S}$ is the Miller function defined in section

2.1. For $i = 0, \cdots l$ set $s_i = \sum_{j=i}^{l} c_j q^j$; then the map

$$\begin{array}{rcl} e_o : \mathbb{G}_2 \times \mathbb{G}_1 & \rightarrow & \mu_r \\ (Q, P) & \longmapsto & \left(\prod_{i=0}^{l} f_{c_i,Q}^{q^i}(P) \cdot \prod_{i=0}^{l-1} h_{[s_{i+1}]Q,[c_i q^i]Q}(P) \right)^{\frac{q^k-1}{r}} \end{array} \tag{1}$$

defines a bilinear pairing and non degenerate if
$mkq^k \neq ((q^k - 1)/r) \cdot \sum_{i=0}^{l} i c_i q^{i-1} \bmod r$.
The coefficients $c_i : i = 0, \cdots, l$ can be obtained from the short vectors obtained from the lattice

$$L = \begin{pmatrix} r & 0 & 0 & \cdots & 0 \\ -q & 1 & 0 & \cdots & 0 \\ -q^2 & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ -q^{\phi(k)-1} & 0 & 0 & \cdots & 1 \end{pmatrix} \tag{2}$$

2.4 Final Exponentiation and the lattice-based Method for its Computation

The result of the Miller loop step is raised to the power $\frac{p^k-1}{r}$, where we assume that q is now a prime denoted p for simplicity. This step is called the final exponentiation(line 10 in Miller's algorithm). The efficient computation of final exponentiation has became a serious task. Observe that this exponent can be divided into two parts as follows:

$$\frac{p^k - 1}{r} = \left[\frac{p^k - 1}{\phi_k(p)}\right] \cdot \left[\frac{\phi_k(p)}{r}\right]$$

where $\phi_k(x)$ is the k-th cyclotomic polynomial. The final exponentiation is therefore computed as $f^{\frac{p^k-1}{r}} = \left[f^{\frac{p^k-1}{\phi_k(p)}}\right]^{\frac{\phi_k(p)}{r}}$. The computation of the first part $A = f^{\frac{p^k-1}{\phi_k(p)}}$ is generally inexpensive as it consists of few multiplications, inversion and p-th powering in $\mathbb{F}_{p^k}$. The second part $A^{\frac{\phi_k(p)}{r}}$ is considered more difficult and is called the hard part. An efficient method to compute the hard part is described by Scott *et al.* [33]. They suggested to write $d = \frac{\phi_k(p)}{r}$ in base p as $d = d_0 + d_1 p + ... + d_{\phi(k)-1} p^{\phi(k)-1}$ and find a short vectorial addition chains to compute A^d much more efficiently than the naive method. In [15], based on the fact that a fixed power of a pairing is still a pairing, Fuentes *et al.*[15] suggested to apply Scott *et al.*'s method with a power of any multiple d' of d with r not dividing d'. This could lead to efficient exponentiation than computing directly A^d. Their idea of finding the polynomial $d'(x)$ is to apply the LLL-algorithm to the matrix formed by $\mathbb{Q}$-linear combinations of the elements $d(x), xd(x), ..., x^{degr-1}d(x)$. They successfully applied the method in the case of elliptic curves of embedding degrees $8, 12$ and 18 [15]. In Sections 4 and 5 we apply this method to improve the computation of the final exponentiation for elliptic curves of embedding degree $k = 9$ and 15. A clever method was used by Zhang *et al.* [36] to compute the final exponentiation in the case $k = 27$.

3 Arithmetic in the Tower Fields of $\mathbb{F}_{p^9}$, $\mathbb{F}_{p^{27}}$ and $\mathbb{F}_{p^{15}}$

A pairing is computed as an element of the extension field $\mathbb{F}_{p^k}$. But its efficient computation depends on the arithmetic of sub fields of $\mathbb{F}_{p^k}$ which is generally organised as tower of sub fields extensions. In this section we recall the tower extension of finite fields $\mathbb{F}_{p^9}, \mathbb{F}_{p^{27}}$ and $\mathbb{F}_{p^{15}}$. We also give explicit cost of the arithmetic operations.
For extension fields arithmetic in $\mathbb{F}_{p^9}, \mathbb{F}_{p^{27}}$ we consider $p \equiv 1 \bmod 3$ motivated by the work of Baretto et *al.*[4] on the construction of elliptic curves of embedding degree 9 and 27. This implies that $\mathbb{F}_{p^{27}}$ can be represented as $\mathbb{F}_p[X]/(X^k - \alpha)$, for $k = 3^i, i = 2, 3$ where α is a cubic non residue modulo p. Since $p \equiv 1 \bmod 3$ and as Euler's conjecture says that 2 is a cube mod p if and only if $3 \mid p$, we always have $X^3 - 2$ irreducible over $\mathbb{F}_p$. Therefore cubic extensions will be constructed using the polynomials $X^3 - \alpha_i$ where $\alpha_i = 2^{1/3^i}$. A tower extension for $\mathbb{F}_{p^{27}}$ together with the one for $\mathbb{F}_{p^9}$ are then given by:

$$\mathbb{F}_{p^3} = \mathbb{F}_p[u] \text{ with } u^3 = 2$$

$$\mathbb{F}_{p^9} = \mathbb{F}_{p^3}[v] \text{ with } v^3 = 2^{1/3}$$

$$\mathbb{F}_{p^{27}} = \mathbb{F}_{p^9}[w] \text{ with } w^3 = 2^{1/9}$$

The costs of the computation of the Frobenius maps and cyclotomic inversions are given in Lemma 1 for the extension $\mathbb{F}_{p^9}$. The proof of this Lemma is given in Appendix A.

Lemma 1 *In the finite field* $\mathbb{F}_{p^9}$,

1. *The computation of the* $p^3; p^6$*-Frobenius maps costs* $6m_{343} + 6a_{343}$
2. *The computation of the* $p; p^2; p^4; p^5; p^7; p^8$*-Frobenius maps costs* $8m_{343} + 6a_{343}$
3. *The inverse of an element* α *of the* $G_{\phi_3(p^3)}$*-order cyclotomic subgroup is computed as* $\alpha^{-1} = \alpha^{p^3} \cdot \alpha^{p^6}$ *and the cost is* $36s_{343} + 84a_{343}$

Similarly, in the finite field $\mathbb{F}_{p^{27}}$ the Lemma 2 gives the costs of the computation of the Frobenius maps and cyclotomic inversions. The proof of this Lemma is given in Appendix B.

Lemma 2 *In the finite field* $\mathbb{F}_{p^{27}}$,

1. *The computation of the* $p^3; p^6; p^9$*-Frobenius maps costs* $18m_{514} + 18a_{514}$
2. *The computation of the* $p; p^2; p^4; p^5; p^7; p^8$*-Frobenius maps costs* $26m_{514} + 18a_{514}$
3. *The inverse of an element* α *of the* $G_{\phi_3(p^9)}$*-order cyclotomic subgroup is computed as* $\alpha^{-1} = \alpha^{p^9} \cdot \alpha^{p^{18}}$ *and the cost is* $216s_{514} + 759a_{514}$

In the case of $\mathbb{F}_{p^{15}}$, we consider pairing friendly curves over $\mathbb{F}_p$ where $p \equiv 1 \bmod 5$ [12]. According to [28, Theorem 3.75] the polynomial $X^5 - \alpha$ is irreducible over $\mathbb{F}_p[X]$ if and only if α is neither a cubic root nor a fifth root in $\mathbb{F}_p$. A tower extension for $\mathbb{F}_{p^{15}}$ can be constructed as follows:

$$\mathbb{F}_{p^5} = \mathbb{F}_p[u] \text{ with } u^5 = 2$$

$$\mathbb{F}_{p^{15}} = \mathbb{F}_{p^5}[v] \text{ with } v^3 = u. \textit{ where } u \in \mathbb{F}_{p^5}$$

Our main contribution in this section is the computation of Frobenius maps and the inversions in the $\phi_n(.)$-order cyclotomic subgroup of $\mathbb{F}^{\star}_{p^k}$. The costs of the computation of the Frobenius maps and cyclotomic inversions are given in Lemma 3.

Lemma 3 *In the finite field* $\mathbb{F}_{p^{15}}$*,*

1. *The computation of the* $p^5; p^{10}$*-Frobenius maps costs* $10m_{575} + 12a_{575}$
2. *The computation of the* $p; p^2; p^3; p^4; p^6; p^7; p^8; p^9$*-Frobenius maps costs* $14m_{575} + 12a_{575}$
3. *The inverse of an element* α *of the* $G_{\phi_3(p^5)}$*-order cyclotomic subgroup is computed as* $\alpha^{-1} = \alpha^{p^5} \cdot \alpha^{p^{10}}$ *and the cost is* $54s_{575} + 837a_{575}$

Proof. The proof is given in Appendix C.

In Table 3 we summarise the overall cost of operations in the tower fields described above. The costs for squaring, multiplication and inversion are from [26], [32] and [36] respectively for $k = 9, 15$ and 27. Explicit details of the cost of Frobenius maps and inversions in the cyclotomic subgroup are given in Appendix A, B and C.

Fields	Operations	Costs
$\mathbb{F}_{p^3}$	Multiplication M_3	$6m_{343} + 17a_{343}$
	Squaring S_3	$6s_{343} + 8a_{343}$
	Inversion I_3	$i_{343} + 9m_{343} + 2s_{343}$
$\mathbb{F}_{p^9}$	Multiplication M_9	$36m_{343} + 149a_{343}$
	Squaring S_9	$36s_{343} + 95a_{343}$
	Inversion I_9	$i_{343} + 63m_{343} + 14s_{343}$
	Frobenius $p^3; p^6$	$6m_{343} + 6a_{343}$
	Frobenius $p; p^2; p^4; p^5; p^7; p^8$	$8m_{343} + 6a_{343}$
	Inversion in $G_{\phi_3(p^3)}$	$36s_{343} + 84a_{343}$
$\mathbb{F}_{p^{27}}$	Multiplication M_{27}	$216m_{514} + 1031a_{514}$
	Squaring S_{27}	$216s_{514} + 788a_{514}$
	Inversion I_{27}	$i_{514} + 387m_{514} + 86s_{514}$
	Frobenius $p^3; p^6; p^9$	$18m_{514} + 18a_{514}$
	Frobenius $p; p^2; p^4; p^5; p^7; p^8$	$26m_{514} + 18a_{514}$
	Inversion in $G_{\phi_3(p^9)}$	$216s_{514} + 759a_{514}$
$\mathbb{F}_{p^5}$	Multiplication M_5	$9m_{575} + 137a_{575}$
	Squaring S_5	$9s_{575} + 137a_{575}$
	Inversion I_5	$1i_{575} + 45m_{575} + 5s_{575}$
$\mathbb{F}_{p^{15}}$	Multiplication M_{15}	$45m_{575} + 635a_{575}$
	Squaring S_{15}	$45s_{575} + 635a_{575}$
	Inversion I_{15}	$1i_{575} + 126m_{575} +$ $23s_{575} + 1507a_{575}$
	Frobenius $p^5; p^{10}$	$10m_{575} + 12a_{575}$
	Frobenius $p; p^2; p^3; p^4; p^6; p^7; p^8; p^9$	$14m_{575} + 12a_{575}$
	Inversion in $G_{\phi_3(p^5)}$	$54s_{575} + 837a_{575}$

Table 2. Cost of operations in extension fields from [26], [32] and [36] and this work (see Appendix A,B,C)

4 Elliptic Curves with Embedding Degree 9

This section describes the computation of optimal ate pairing (Miller step and the final exponentiation) on the parameterized elliptic curve defined in [30]. This family of elliptic curves has embedding degree 9 and a ρ-value 1.33 and is parameterized by :

$$
\begin{aligned}
p &= ((x+1)^2 + ((x-1)^2(2x^3+1)^2)/3)/4 \\
r &= (x^6 + x^3 + 1)/3 \\
t &= x+1
\end{aligned}
\tag{3}
$$

4.1 Optimal ate pairing

Based on the general framework described by Vercauteren in [34], the short vectors obtained from the lattice L defined by equation (2) gives the optimal function $h(z) = \sum_{i=0}^{5} c_i z^i = x - z \in \mathbb{Z}[z]$. A straightforward application of formula (1) yields the optimal pairing :

$$
\begin{aligned}
e_o : \mathbb{G}_2 \times \mathbb{G}_1 &\longrightarrow \mu_r \\
(Q, P) &\longmapsto f_{x,Q}(P)^{\frac{p^9-1}{r}}
\end{aligned}
$$

4.2 Cost of the execution of the Miller loop

The Miller loop consists of the doubling steps (line 3 in the Miller algorithm) and addition steps (line 6 or 8 in the Miller algorithm). These steps use the Miller function $h_{R,S}$ either in affine coordinates or projective coordinates. The work of Zhang *et al.*[36, Section 3] presents the currently fastest formulas in projective coordinates. The doubling step costs $9M_1 + 3M_3 + 9S_3$ and the cost of the addition step is $9M_1 + 12M_3 + 5S_3$. For an explicit cost of the computation of $f_{x,Q}(P)$, we wrote a Pari/GP code to find a suitable x with low Hamming weight and minimal number of bits for the 128 bits security level according to Table 1. The best value we were able to find is $x = 2^{43} + 2^{37} + 2^7 + 1$ which gives $r(x)$ prime of 257 bits and $p(x)$ of 343 bits. The values p and x are both congruent to 1 modulo 6 so that the corresponding elliptic curve is $y^2 = x^3 + 1$ [26]. The computation of $f_{x,Q}(P)$ therefore costs 43 doubling steps, 3 additions, 42 squaring and 45 multiplications in $\mathbb{F}_{p^9}$. Thus the total cost for the computation of the Miller loop for the optimal pairing on elliptic curves of embedding degree 9 is $43(9M_1 + 3M_3 + 9S_3) + 3(9M_1 + 12M_3 + 5S_3) + 42S_9 + 45M_9$. This is equal to $45M_9 + 165M_3 + 414M_1 + 42S_9 + 402S_3$. Using the arithmetic in Table 2, the overall cost is $3024m_{343} + 3924s_{343}$. To our knowledge, no other explicit cost with a specific value of x is reported in the literature.

4.3 Cost of the computation of the final exponentiation

As explained in Section 2, the final exponentiation in this case can be divided as $f^{(p^9-1)/r} = \left(f^{p^3-1}\right)^{(p^6+p^3+1)/r} = \left(f^{p^3-1}\right)^{d}$. The lattice method described by Fuentes *et al.*[15] that we briefly explained in section 2.4 applied to the matrix

$$
M = \begin{pmatrix} 243d(x) \\ 243xd(x) \\ 243x^2d(x) \\ 243x^3d(x) \\ 243x^4d(x) \\ 243x^5d(x) \end{pmatrix}
\tag{4}
$$

enabled us to find the following multiple of d: $d' = x^3 d = k_0 + k_1 p + k_2 p^2 + k_3 p^3 + k_4 p^4 + k_5 p^5$ where the polynomials $k_i, i = 0, ..., 5$ are as follows

$$\begin{array}{lll} k_0 = -x^4 + 2x^3 - x^2, & k_1 = -x^3 + 2x^2 - x, & k_2 = -x^2 + 2x - 1, \\ k_3 = x^7 - 2x^6 + x^5 + 3, & k_4 = x^6 - 2x^5 + x^4, & k_5 = x^5 - 2x^4 + x^3 \end{array}$$

They verify the relations

$$k_2 = -(x-1)^2, \quad k_1 = xk_2, \quad k_0 = xk_1, \quad k_5 = -xk_0, \quad k_4 = xk_5, \quad k_3 = xk_4 + 3$$

If we set $A = f^{p^3-1}$ then

- The cost for the computation of A is 1 p^3-Frobenius, 1 Inversion in $\mathbb{F}_{p^9}$ and 1 multiplication in $\mathbb{F}_{p^9}$.
- The cost of the computation of A^{k_0}, A^{k_1} and A^{k_4} is 3 exponentiation by x,
- The cost of the computation of A^{k_5} is one inversion in the cylotomic subgroup and one exponentiation by x.
- The cost of the computation of A^{k_2} is one inversion in the cyclotomic subgroup and two exponentiations by $(x-1)$.
- The cost of the computation of A^{k_3} is 2 multiplication, one squaring and one exponentiation by x.

Note that the inversion in the cyclotomic subgroup $\mathbb{G}_{\varphi_3(p^3)}$ of order $p^6 + p^3 + 1$ is computed as $A^{-1} = A^{p^3} \cdot A^{p^6}$ (see Appendix A for details and cost). The cost for the hard part $A^{d'}$ is then 2 exponentiations by $x - 1$, 5 exponentiations by x, 7 multiplications in $\mathbb{F}_{p^9}$, one squaring in $\mathbb{F}_{p^9}$ two cyclotomic inversion $I_{\mathbb{G}_{\phi_3(p^3)}}$ and p, p^2, p^3, p^4, p^5-Frobenius maps. Using the value of x given above, one exponentiation by x costs $43S_9 + 3M_9$ whereas one exponentiation by $x - 1$ costs $43S_9 + 2M_9$. Finally the hard part costs $2(43S_9 + 2M_9) + 5(43S_9 + 3M_9) + 7M_9 + 1S_9 + 2I_{\mathbb{G}_{\phi_3(p^3)}} = 302S_9 + 26M_9 + 2I_{\mathbb{G}_{\phi_3(p^3)}}$ and p, p^2, p^3, p^4, p^5-Frobenius maps. The total cost of the final exponentiation is $1I_9 + 27M_9 + 302S_9 + 2I_{\mathbb{G}_{\phi_3(p^3)}}$ and $p, p^2, 2 * p^3, p^4, p^5$-Frobenius maps.

4.4 Improvement and comparison with previous work

From the results in [26], the hard part costs $1I_9 + 309S_9 + 50M_9$ and p, p^2, p^3, p^4, p^5-Frobenius maps. If we include the cost $1I_9+1M_9$ and p^3-Frobenius for the easy part and using the arithmetic in Table 2, the overall cost is $i_{343} + 1079m_{343} + 10958s_{343}$ for this work and $i_{343} + 1943m_{343} + 11138s_{343}$ for Le et *al.*[26]. We therefore save $24M_9 + 7S_9 - 2I_{\mathbb{G}_{\phi_3(p^3)}} = 864m_{343} + 180s_{343}$ comparatively to their work.

5 Elliptic Curves with Embedding Degree 15

In this section we give explicit formulas together with their cost for the Miller loop in the optimal ate pairing and compute the cost of the final exponentiation on the parameterized elliptic curve defined in [12]. This family of elliptic curves has embedding degree 15 and a ρ-value 1.5 and is parameterized by :

$$
\begin{aligned}
p &= (x^{12} - 2x^{11} + x^{10} + x^7 - 2x^6 + x^5 + x^2 + x + 1)/3 \\
r &= x^8 - x^7 + x^5 - x^4 + x^3 - x + 1 \\
t &= x + 1
\end{aligned} \tag{5}
$$

5.1 Optimal ate pairing

The Vercauteren approach described in [34] enabled us to obtain the short vectors from the lattice L defined by equation (2) which lead to the optimal function $h(z) = \sum_{i=0}^{5} c_i z^i = x - z \in \mathbb{Z}[z]$. A straightforward application of formula (1) yields the optimal pairing :

$$
\begin{aligned}
e_o : \mathbb{G}_2 \times \mathbb{G}_1 &\longrightarrow \mu_r \\
(Q, P) &\longmapsto f_{x,Q}(P)^{\frac{p^{15}-1}{r}}
\end{aligned}
$$

5.2 Cost of the computation of the Miller loop

In this section, we consider the Miller function given in affine coordinates, following the analysis of Lauter et *al.* [25] who suggested to use affine coordinates at higher security level. Miller function used for the computation of $f_{x,Q}(P)$ in this case is described in [36]. At 192 bits security level on elliptic curves with $k = 15$, the best value of x we were able to find with a Pari/GP code is $x = 2^{48} + 2^{41} + 2^9 + 2^8 + 1$. This value gives a $r(x)$ prime of 385 bits and $p(x)$ of 575 bits which correspond to parameters for 192-bits security level according to Table 1. The value of p is congruent to 1 modulo 5. The Miller loop consists here of computing $f_{x,Q}$ which costs 48 doubling steps, 4 additions steps, 47 squaring and 51 multiplications in $\mathbb{F}_{p^{15}}$. Considering the currently fastest cost for doubling and addition step in [36],
the Miller loop costs $48(15M_1 + 3M_5 + 9S_5) + 4(15M_1 + 12M_5 + 5S_5) + 47S_{15} + 51M_{15}$, which is $51M_{15} + 192M_5 + 780M_1 + 47S_{15} + 452S_5$. Using the arithmetic in Table 2, the overall cost is $4803m_{575} + 6183s_{575}$. To our knowledge no explicit cost is reported in the literature in the case $k = 15$ with a specific value of x.

5.3 Cost of the computation of the final exponentiation

The final exponentiation in this case is written in a different way as $f^{(p^{15}-1)/r} = \left(f^{p^5-1}\right)^{(p^{10}+p^5+1)/r} = \left(f^{p^5-1}\right)^d$. This decomposition is used instead of $\frac{p^{15}-1}{r} = \left[\frac{p^{15}-1}{\phi_{15}(p)}\right] \cdot \left[\frac{\phi_{15}(p)}{r}\right]$ as usually done, for efficiency reasons in computation. Observe that $\frac{p^{15}-1}{\phi_{15}(p)} = p^7 + p^6 + p^5 - p^2 - p - 1$ and $\phi_{15}(p) = p^8 - p^7 + p^5 - p^4 + p^3 - p + 1$ will lead to several multiplications and Frobenius maps operations. Thus the lattice method described by Fuentes *et al.*[15] that we briefly explained in section 2.4 applied to the matrix

$$M = \begin{pmatrix} \frac{59049}{19683} d(x) \\ \frac{59049}{19683} x d(x) \\ \frac{59049}{19683} x^2 d(x) \\ . \\ . \\ \frac{59049}{19683} x^7 d(x) \end{pmatrix} \tag{6}$$

enabled us to find the following multiple of d: $d' = 3x^3 d = k_0 + k_1 p + \ldots k_9 p^9$ where the polynomials $k_i, i = 0, \ldots, 9$ are defined as follows

$$\begin{aligned}
&k_0 = -x^6 + x^5 + x^3 - x^2, && k_1 = -x^5 + x^4 + x^2 - x \\
&k_2 = -x^4 + x^3 + x - 1 && \\
&k_3 = x^{11} - 2x^{10} + x^9 + x^6 - 2x^5 + x^4 - x^3 + x^2 + x + 2 && \\
&k_5 = x^{11} - x^{10} - x^8 + x^7 + 3 && \\
&k_4 = x^{11} - x^{10} - x^9 + x^8 + x^6 - x^5 - x^4 + x^3 - x^2 + 2x + 2 && \\
&k_6 = x^{10} - x^9 - x^7 + x^6 && k_7 = x^9 - x^8 - x^6 + x^5 \\
&k_8 = x^8 - x^7 - x^5 + x^4 && k_9 = x^7 - x^6 - x^4 + x^3
\end{aligned}$$

The polynomials $k_i : i = 0, \ldots 9$ verify the relations

$$\begin{aligned}
&k_2 = -(x-1)^2(x^2 + x + 1), \quad k_1 = x k_2, \quad k_0 = x k_1 \\
&k_9 = -x k_0, \quad k_8 = x k_9, \quad k_7 = x k_8 \\
&k_6 = x k_7, \quad k_5 = x k_6 + 3, \quad k_4 = M - (k_1 + k_7) \\
&k_3 = M - (k_0 + k_6 + k_9) \text{ where } M = (k_2 + k_5 + k_8)
\end{aligned}$$

Set $A = f^{p^5 - 1}$ then

- The cost for the computation of A is 1 p^5-Frobenius, 1 Inversion in $\mathbb{F}_{p^{15}}$ and 1 multiplication in $\mathbb{F}_{p^{15}}$ and .
- The computation of A^{k_2} is 2 exponentiation by x, 2 exponentiation by $x-1$, 2 multiplications and 1 cyclotomic inversion,
- The cost of the computation of the A^{k_0},A^{k_1},A^{k_6},A^{k_7} is 5 exponentiations by x, the computation of A^{k_9} costs 1 exponentiation by x and 1 cyclotomic inversion,
- The computation of A^{k_5} is 1 exponentiation by x, 2 multiplication and 1 squaring in $\mathbb{F}_{p^{15}}$,
- The computation of A^{k_4} costs 4 multiplications in $\mathbb{F}_{p^{15}}$ and 1 cyclotomic inversion,
- The computation of A^{k_3} costs 3 multiplications in $\mathbb{F}_{p^{15}}$ and 1 cyclotomic inversion.

Therefore, the cost of the computation of $A^{d'}$ is 2 exponentiations by $x - 1$, 9 exponentiations by x, 20 multiplications, one squaring in $\mathbb{F}_{p^{15}}$, four inversions in the cyclotomic subgroup $\mathbb{G}_{\phi_3(p^5)}$ of order $p^{10} + p^5 + 1$ (note that $A^{-1} = A^{p^5} \cdot A^{p^{10}}$ see Appendix C for details) and

$p, p^2, p^3, p^4, p^5, p^6, p^7, p^8, p^9$-Frobenius maps. Using the value of x given above, the cost of the hard part is $2(48S_{15}+3M_{15})+9(48S_{15}+4M_{15})+20M_{15}+1S_{15}+4I_{\mathbb{G}_{\varphi_3(p^5)}} = 529S_{15}+62M_{15}+4I_{\mathbb{G}_{\varphi_3(p^5)}}$ and $p, p^2, p^3, p^4, p^5, p^6, p^7, p^8, p^9$-Frobenius maps. The total cost of the final exponentiation in this work is therefore $1I_{15}+529S_{15}+63M_{15}+4I_{\mathbb{G}_{\varphi_3(p^5)}}$ and $p, p^2, p^3, p^4, 2*p^5, p^6, p^7, p^8, p^9$-Frobenius maps.

Remark 1. The cost given by Le *et al.* [26] for the hard part is 11 exponentiations by x, 22 multiplications, 2 inversions in $\mathbb{F}_{p^{15}}$ and 9 Frobenius maps. The authors said that the cost of an inversion in $\mathbb{F}_{p^{15}}$ is free with a reference to a similar computation but on elliptic curves with even embedding degree, unfortunately we do not see how this is possible. Also, they considered a x of 64 bits and hamming weight 7 and claimed that the cost is $88M_{15} + 528S_{15}$ instead of $11(6M_{15}+64S_{15}) = 88M_{15}+704S_{15}$. Therefore if we count the 2 inversions in $\mathbb{F}_{p^{15}}$ (these inverses are in fact in the cyclotomic subgroup $\mathbb{G}_{\varphi_3(p^5)}$), then their final cost is $88M_{15}+704S_{15}+2I_{\mathbb{G}_{\varphi_3(p^5)}}$ and 11 Frobenius maps, whereas our cost is $529S_{15} + 62M_{15} + 4I_{\mathbb{G}_{\varphi_3(p^5)}}$.

5.4 Improvement and comparison with previous work

Considering the previous remark the cost of the final exponentiation in [26] is $1I_{15} + 704S_{15} + 89M_{15} + 2I_{\mathbb{G}_{\varphi_3(p^5)}}$ and $p, p^2, p^3, p^4, 2*p^5, p^6, p^7, p^8, p^9$-Frobenius maps. We observe that we have improved the results by saving $26M_{15} + 175S_{15} - 2I_{\mathbb{G}_{\varphi_3(p^5)}}$. Using the arithmetic in Table 2, the overall cost is $i_{575} + 3093m_{575} + 24044s_{575}$ for this work and $i_{575} + 4263m_{575} + 31811s_{575}$ for Le et *al.*[26]. We therefore save $26M_{15} + 175S_{15} - 2I_{\mathbb{G}_{\varphi_3(p^5)}} = 1170m_{575} + 7767s_{575}$ comparatively to their work.

6 Elliptic Curves with Embedding Degree 27

The parameterized elliptic curves with embedding degree 27 is defined in [4]. This family has a ρ-value 10/9 and is parameterized by the following polynomials:

$$\begin{aligned} p &= 1/3(x-1)^2(x^{18}+x^9+1)+x \\ r &= 1/3(x^{18}+x^9+1) \\ t &= x+1 \end{aligned} \tag{7}$$

6.1 The Miller loop and the final exponentiation

The Miller loop and the final exponentiation has been studied in [36]. They found the optimal function $h(z) = \sum_{i=0}^{17} c_i z^i = x - z \in \mathbb{Z}[z]$ and the optimal pairing is given by

$$e_o : \mathbb{G}_2 \times \mathbb{G}_1 \longrightarrow \mu_r; (Q, P) \longmapsto f_{x,Q}(P)^{\frac{p^{27}-1}{r}}$$

The authors in [36] used the parameter $x = 2^{28} + 2^{27} + 2^{25} + 2^8 - 2^3$ for their computation at 256-bits security level. The cost of the Miller step that they obtained is therefore $28(3M_9 + 2S_9 + 1I_9 + 9M_1) + 4(3M_9 + 2S_9 + 1I_9 + 9M_1) + 27(6S_9) + 30(6M_9) + 1I_{27} =$

$276M_9+226S_9+32I_9+288M_1$ operations. The computation of the final exponentiation in [36] requires $1I_{27}+12M_{27}$, 17 powers of x, 2 powers of $x-1$ and $p, p^2, p^3, p^4, p^5, p^6, p^7, p^8, 2*p^9$-Frobenius maps. Therefore the explicit cost of the final exponentiation is $1I_{27} + 17(5(6M_9) + 28(6S_9) + 36M_1) + 2(6(6M_9) + 28(6S_9) + 36M_1) + 11(6M_9) + 228M_1 = 1I_{27} + 648M_9 + 3192S_9 + 912M_1$. Then the explicit cost for the computation of the Miller loop and the final exponentiation given in that work is $12627m_{573} + 8670m_{573} + 33i_{573}$ and $24627m_{573} + 114998m_{573} + 1i_{573}$ respectively.

Remark 2. The negative coefficient in the value of x affects the efficiency since one full inversion in $\mathbb{F}_{p^{27}}$ is required in the Miller algorithm (line 8) and also 19 inversions in the cyclotomic subgroup are required when raising to power x during the final exponentiation.

In the next section we explain the choice of another parameter to avoid these additional operations.

6.2 Improvement and comparison with previous work

We use the arithmetic (especially the computation of inversion in cyclotomic subgroup) and a specific value of x to improve the costs in [36]. Precisely, a careful search with a Pari/GP code enabled us to find the value $x = 2^{29} + 2^{19} + 2^{17} + 2^{14}$ so that r has a prime factor of 514 bits length and the prime p has a bit length of 579 for 256-bits security level according to Table 1. Although we have an extra doubling step, we avoid the full inversion in $\mathbb{F}_{p^{27}}$ and 17 inversions in the cyclotomic subgroup $\mathbb{G}_{\phi_3(p^9)}$ when raising to power x. We perform 2 inversions in the cyclotomic subgroup only when raising to power $x-1$.
The cost of the Miller loop now becomes $29(3M_9 + 2S_9 + 1I_9 + 9M_1) + 3(3M_9 + 2S_9 + 1I_9 + 9M_1) + 27(6S_9) + 30(6M_9) = 276M_9 + 226S_9 + 32I_9 + 288M_1$. Using the arithmetic in Table 3, the overall cost for the Miller loop is $12240m_{579} + 8584s_{579}$ for this work where we saved one inversion in $\mathbb{F}_{p^{27}}$.
Our cost for the final exponentiation is $1I_{27} + 17(3(6M_9) + 29(6S_9)) + 2(4(6M_9) + 29(6S_9) + 2I_{\mathbb{G}_{\phi_3(p^9)}}) + 11(6M_9) = 1I_{27} + 420M_9 + 3306S_9 + 2I_{\mathbb{G}_{\phi_3(p^9)}}$ and $p, p^2, p^3, p^4, p^5, p^6, p^7, p^8, 2*p^9$-Frobenius maps. Using the arithmetic in Table 2, the overall cost is $i_{579} + 15735m_{579} + 119534s_{579}$ for this work.

7 General Comparison

In this section, we summarize the different costs obtained in this work and compare our results with previous works.

If we assume that the cost of a squaring is the same as the cost of a multiplication then the cost of the final exponentiation is $i_{575} + 27137m_{575}$ and $i_{575} + 36074m_{575}$ for this work and previous work [26] respectively. The theoretical improvement obtained in this work is therefore up to 25%. A similar analysis with $k = 9$ and $k = 27$ yields an improvement of 8% and 3% respectively.

Curves	References	Miller loop	Final Exponentiation
$k = 9$, 128-bits security level	Previous work [26]	*No specific cost reported*	$i_{343} + 1943m_{343} + 11138s_{343}$
	This work	$3024m_{343} + 3924s_{343}$	$i_{343} + 1079m_{343} + 10958s_{343}$
$k = 15$, 192-bits security level	Previous work [26]	*No specific cost reported*	$i_{575} + 4263m_{575} + 31811s_{575}$
	This work	$4803m_{575} + 6183s_{575}$	$i_{575} + 3093m_{575} + 24044s_{575}$
$k = 27$, 256-bits security level	Previous work [36]	$33i_{573} + 12627m_{573} + 8670m_{573}$	$i_{573} + 24627m_{573} + 114998s_{573}$
	This work	$12240m_{579} + 8584s_{579}$	$i_{579} + 15735m_{579} + 119534s_{579}$

Table 3. Comparison of the cost of the Miller loop and the final exponentiation.

8 Conclusion

In this work we provided details and important improvements in the computation of the Miller loop and the final exponentiation for optimal pairings on elliptic curves admitting cubic twists. An explicit cost evaluation is given for the Miller loop in the case of elliptic curves of embedding degree 9 and 15. We obtained an improvement up to 25% in the computation of the final exponentiation. A brief look at the parameters used in this work reveals that the corresponding curves are not *subgroup secure* ordinary curves [3] and are not protected against *small-subgroup attacks*[29]. However this is not a particular case of elliptic curves of odd embedding degree but it appears from [3] that most of such parameters that have been found for curves with even embedding degree such as BN12 curves [5], KSS16 curves [21] or BLS12 curves [4] do not satisfied these security properties. As future work we could search for parameters to fulfil this security issue.

References

1. Diego F. Aranha, Laura Fuentes-Castañeda, Edward Knapp, Alfred Menezes, and Francisco Rodríguez-Henríquez. Implementing pairings at the 192-bit security level. In *Pairing-Based Cryptography - Pairing 2012 - 5th International Conference, Cologne, Germany, May 16-18, 2012, Revised Selected Papers*, pages 177–195, 2012.
2. R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, and F. Vercauteren. *Handbook of Elliptic and Hyperelliptic curve Cryptography.* Discrete Math. Aplli. Chapman and Hall, 2006.
3. Paulo S. L. M. Barreto, Craig Costello, Rafael Misoczki, Michael Naehrig, Geovandro C. C. F. Pereira, and Gustavo Zanon. Subgroup security in pairing-based cryptography. In *Progress in Cryptology - LATINCRYPT 2015 - 4th International Conference on Cryptology and Information Security in Latin America, Guadalajara, Mexico, August 23-26, 2015, Proceedings*, pages 245–265, 2015.
4. Paulo S. L. M. Barreto, Ben Lynn, and Michael Scott. Constructing elliptic curves with prescribed embedding degrees. In *Security in Communication Networks, Third International Conference, SCN 2002, Amalfi, Italy, September 11-13, 2002. Revised Papers*, pages 257–267, 2002.
5. Paulo S. L. M. Barreto and Michael Naehrig. Pairing-friendly elliptic curves of prime order. In *Selected Areas in Cryptography, 12th International Workshop, SAC 2005, Kingston, ON, Canada, August 11-12, 2005, Revised Selected Papers*, pages 319–331, 2005.
6. I.F. Blake, G. Seroussi, and N.P. Smart. *Advances in Elliptic Curves in Cryptography.* London Mathematic Society, Cambridge University Press, (2005).
7. Dan Boneh and Matthew K. Franklin. Identity-based encryption from the Weil pairing. In *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings*, pages 213–229, 2001.
8. Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the weil pairing. *J. Cryptology*, 17(4):297–319, 2004.

9. Clifford Cocks. An identity based encryption scheme based on quadratic residues. In *Cryptography and Coding, 8th IMA International Conference, Cirencester, UK, December 17-19, 2001, Proceedings*, pages 360–363, 2001.
10. Craig Costello, Tanja Lange, and Michael Naehrig. Faster pairing computations on curves with high-degree twists. In *Public Key Cryptography - PKC 2010, 13th International Conference on Practice and Theory in Public Key Cryptography, Paris, France, May 26-28, 2010. Proceedings*, pages 224–242, 2010.
11. Augusto Jun Devegili, Michael Scott, and Ricardo Dahab. Implementing cryptographic pairings over barreto-naehrig curves. In *Pairing-Based Cryptography - Pairing 2007, First International Conference, Tokyo, Japan, July 2-4, 2007, Proceedings*, pages 197–207, 2007.
12. Pu Duan, Shi Cui, and Choong Wah Chan. Special polynomial families for generating more suitable elliptic curves for pairing-based cryptosystems. *IACR Cryptology ePrint Archive*, 2005:342, 2005.
13. Ratna Dutta, Rana Barua, and Palash Sarkar. Pairing-based cryptographic protocols : A survey. *IACR Cryptology ePrint Archive*, 2004:64, 2004.
14. David Freeman, Michael Scott, and Edlyn Teske. A taxonomy of pairing-friendly elliptic curves. *J. Cryptology*, 23(2):224–280, 2010.
15. Laura Fuentes-Castañeda, Edward Knapp, and Francisco Rodríguez-Henríquez. Faster hashing to $\mathbb{G}_2$. In *Selected Areas in Cryptography - 18th International Workshop, SAC 2011, Toronto, ON, Canada, August 11-12, 2011, Revised Selected Papers*, pages 412–430, 2011.
16. Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS 2006, Alexandria, VA, USA, Ioctober 30 - November 3, 2006*, pages 89–98, 2006.
17. Robert Granger and Michael Scott. Faster squaring in the cyclotomic subgroup of sixth degree extensions. In *Public Key Cryptography - PKC 2010, 13th International Conference on Practice and Theory in Public Key Cryptography, Paris, France, May 26-28, 2010. Proceedings*, pages 209–223, 2010.
18. Aurore Guillevic. Kim-barbulescu variant of the number field sieve to compute discrete logarithms in finite fields. In *https://ellipticnews.wordpress.com/2016/05/02/kim-barbulescu-variant-of-the-number-field-sieve-to-compute-discrete-logarithms-in-finite-fields*, ellipticnews, May 2016.
19. Florian Hess. Pairing lattices. In *Pairing-Based Cryptography - Pairing 2008, Second International Conference, Egham, UK, September 1-3, 2008. Proceedings*, pages 18–38, 2008.
20. Florian Hess, Nigel P. Smart, and Frederik Vercauteren. The eta pairing revisited. *IEEE Transactions on Information Theory*, 52(10):4595–4602, 2006.
21. Ezekiel J. Kachisa, Edward F. Schaefer, and Michael Scott. Constructing brezing-weng pairing friendly elliptic curves using elements in the cyclotomic field. *IACR Cryptology ePrint Archive*, 2007:452, 2007.
22. Koray Karabina. Squaring in cyclotomic subgroups. *Math. Comput.*, 82(281), 2013.
23. Taechan Kim and Razvan Barbulescu. Extended tower number field sieve: A new complexity for the medium prime case. In *CRYPTO (1)*, volume 9814 of *Lecture Notes in Computer Science*, pages 543–571. Springer, 2016.
24. Neal Koblitz and Alfred Menezes. Pairing-based cryptography at high security levels. In *Cryptography and Coding, 10th IMA International Conference, Cirencester, UK, December 19-21, 2005, Proceedings*, pages 13–36, 2005.
25. Kristin E. Lauter, Peter L. Montgomery, and Michael Naehrig. An analysis of affine coordinates for pairing computation. In *Pairing-Based Cryptography - Pairing 2010 - 4th International Conference, Yamanaka Hot Spring, Japan, December 2010. Proceedings*, pages 1–20, 2010.
26. Duc-Phong Le and Chik How Tan. Speeding up ate pairing computation in affine coordinates. In *Information Security and Cryptology - ICISC 2012 - 15th International Conference, Seoul, Korea, November 28-30, 2012, Revised Selected Papers*, pages 262–277, 2012.
27. Benoît Libert and Jean-Jacques Quisquater. Identity based undeniable signatures. In *Topics in Cryptology - CT-RSA 2004, The Cryptographers' Track at the RSA Conference 2004, San Francisco, CA, USA, February 23-27, 2004, Proceedings*, pages 112–125, 2004.
28. R Lidl and H Niederreiter. *Finite Fields*. Cambridge university Press, Cambridge, 1997.
29. Chae Hoon Lim and Pil Joong Lee. A key recovery attack on discrete log-based schemes using a prime order subgroupp. In *Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, Proceedings*, pages 249–263, 1997.
30. Xibin Lin, Changan Zhao, Fangguo Zhang, and Yanming Wang. Computing the ate pairing on elliptic curves with embedding degree $k = 9$. *IEICE Transactions*, 91-A(9):2387–2393, 2008.

31. Victor S. Miller. The weil pairing, and its efficient calculation. *J. Cryptology*, 17(4):235–261, 2004.
32. Nadia El Mrabet, Nicolas Guillermin, and Sorina Ionica. A study of pairing computation for elliptic curves with embedding degree 15. *IACR Cryptology ePrint Archive*, 2009:370, 2009.
33. Michael Scott, Naomi Benger, Manuel Charlemagne, Luis J. Dominguez Perez, and Ezekiel J. Kachisa. Fast hashing to $\mathbb{G}_2$ on pairing-friendly curves. In *Pairing-Based Cryptography - Pairing 2009, Third International Conference, Palo Alto, CA, USA, August 12-14, 2009, Proceedings*, pages 102–113, 2009.
34. Frederik Vercauteren. Optimal pairings. *IEEE Transactions on Information Theory*, 56(1):455–461, 2010.
35. L.C. Washington. *Elliptic Curves, Number Theory and Cryptography.* Discrete Math .Aplli, Chapman and Hall, 2008.
36. Xusheng Zhang and Dongdai Lin. Analysis of optimum pairing products at high security levels. In *Progress in Cryptology - INDOCRYPT 2012, 13th International Conference on Cryptology in India, Kolkata, India, December 9-12, 2012. Proceedings*, pages 412–430, 2012.

A Arithmetic in $\mathbb{F}_{p^9}$

A.1 Squaring in $\mathbb{F}_{p^9}$

Let $a = a_0 + a_1 v + a_2 v^2 \in \mathbb{F}_{p^9}$ with $a_i \in \mathbb{F}_{p^3}$. $a^2 = A_0 + A_1 v + A_2 v^2$ where

$$\begin{cases} A_0 = a_0^2 + 2a_1a_2 2^{1/3} \\ A_1 = 2a_0a_1 + a_2^2 2^{1/3} \\ A_2 = \quad 2a_0a_2 + a_1^2 \end{cases}$$

This costs $3m + 3s$ or $6s$ since the computation of $2xy$ can be done as $(x+y)^2 - x^2 - y^2$ when the squares x^2 and y^2 are known.

A.2 Cyclotomic inversion

We assume that a lies in the cyclotomic subgroup $G_{\varphi_3(p^3)}$, so that $a^{p^6+p^3+1} = 1$ i.e. $a^{-1} = a^{p^6} a^{p^3}$. In order to compute $a^{p^6} a^{p^3}$, we need the values of v^{p^3} and v^{p^6}. But $v^{p^3} = v^{3(p^3-1)/3+1} = v^{3(p^3-1)/3} v = (v^3)^{(p^3-1)/3} v = (2^{1/3})^{(p^3-1)/3} v$ since $v^3 = 2^{1/3}$.
Let $\mu = (2^{1/3})^{(p^3-1)/3}$; we have $\mu \neq 1$ and $\mu^3 = 1$ so that μ is a primitive cubic root of unity in $\mathbb{F}_{p^3}$. We obtain $v^{p^3} = \mu v$ and $v^{p^6} = (v^{p^3})^{p^3} = (\mu v)^{p^3} = \mu (v)^{p^3} = \mu\mu v = \mu^2 v$. We then have $a^{p^3} = a_0^{p^3} + a_1^{p^3} v^{p^3} + a_2^{p^3} (v^2)^{p^3} = a_0 + a_1 v^{p^3} + a_2 (v^2)^{p^3} = a_0 + a_1 \mu v + a_2 \mu^2 v^2$ and $a^{p^6} = (a^{p^3})^{p^3} = a_0 + a_1 (\mu v)^{p^3} + a_2 (\mu^2 v^2)^{p^3} = a_0 + a_1 \mu^2 v + a_2 \mu^4 v^2$. So that when using $v^3 = 2^{1/3}$ and $\phi_3(\mu) = \mu^2 + \mu + 1 = 0$, we finally have:

$$a^{p^6} a^{p^3} = (a_0^2 - a_1 a_2 2^{1/3}) + (a_2^2 2^{1/3} - a_0 a_1) v + (a_1^2 - a_0 a_2) v^2$$

This costs $3m + 3s$ or $6s$ with additional additions.

A.3 Frobenius operators

The p^i−Frobenius is the map $\pi^i \colon \mathbb{F}_{p^9} \to \mathbb{F}_{p^9}, a \mapsto a^{p^i}$.
Let $a \in \mathbb{F}_{p^9}$, $a = a_0 + a_1 v + a_2 v^2$ with $a_i \in \mathbb{F}_{p^3}$ then $\pi(a) = a_0^p + a_1^p v^p + a_2^p (v^2)^p$. Now $a_0 \in \mathbb{F}_{p^3}$ can be written as $a_0 = g_0 + g_1 u + g_2 u^2$, $g_i \in \mathbb{F}_p$ so that $a_0^p = g_0 + g_1 u^p + g_2 (u^2)^p$.
We have $u^p = u^{3(p-1)/3+1} = (u^3)^{(p-1)/3} u = 2^{(p-1)/3} u$ and since 2 is not a cube in $\mathbb{F}_p$, $2^{(p-1)/3} \neq 1$.

Let $\alpha = 2^{(p-1)/3}$ then $\alpha \neq 1$ and $\alpha^3 = 1$; it means that α is a primitive cubic root of unity in $\mathbb{F}_p$ and $u^p = \alpha u$. Therefore $a_0^p = g_0 + g_1 u^p + g_2(u^2)^p = g_0 + g_1\alpha u + g_2\alpha^2 u^2$ and similarly $a_1^p = g_3 + g_4 u^p + g_5(u^2)^p = g_3 + g_4\alpha u + g_5\alpha^2 u^2$ and
$a_2^p = g_6 + g_7 u^p + g_8(u^2)^p = g_6 + g_7\alpha u + g_8\alpha^2 u^2$. Now for the computation of v^p observe that $v^p = v^{3(p-1)/3+1} = (v^3)^{(p-1)/3} v = (2^{1/3})^{(p-1)/3} v = 2^{(p-1)/9} v$ so that if $\beta = 2^{(p-1)/9}$ then we have $\beta \neq 1$, $\beta^3 = 2^{(p-1)/3} = \alpha \neq 1$, $\beta^9 = 1$. Thus β is a primitive ninth root of unity in $\mathbb{F}_p$ and $v^p = \beta v$.
Finally $a^p = g_0 + g_1\alpha u + g_2\alpha^2 u^2 + (g_3\beta + g_4\alpha\beta u + g_5\alpha^2\beta u^2)v + (g_6\beta^2 + g_7\alpha\beta^2 u + g_8\alpha^2\beta^2 u^2)v^2$ and the following algebraic relations: $\alpha = \beta^3$, $\alpha\beta = \beta^4$, $\alpha\beta^2 = \beta^5$, $\alpha^2\beta = \beta^7$, $\alpha^2\beta^2 = \beta^8$ yield to $a^p = (g_0 + g_1\beta^3 u + g_2\beta^6 u^2) + (g_3\beta + g_4\beta^4 u + g_5\beta^7 u^2)v + (g_6\beta^2 + g_7\beta^5 u + g_8\beta^8 u^2)v^2$.
The cost of p-Frobenius: $8m_{512} + 6a_{512}$. This is the same as the cost of p^2, p^4, p^5, p^7 and p^8-Frobenius.
For the p^3-Frobenius operator, observe from A.2 that $v^{p^3} = \mu v$. Then
$a^{p^3} = a_0 + a_1\mu v + a_2\mu^2 v^2 = (g_0 + g_1 u + g_2 u^2) + (g_3 + g_4 u + g_5 u^2)\mu v + (g_6 + g_7 u + g_8 u^2)\mu^2 v^2$.
As $t = \mu^2$ is precomputed; we finally have
$a^{p^3} = (g_0 + g_1 u + g_2 u^2) + (g_3\mu + g_4\mu u + g_5\mu u^2)v + (g_6 t + g_7 t u + g_8 t u^2)v^2$.
The cost of p^3-Frobenius: $6m + 6a$. This is the same as the cost of p^6-Frobenius.

B Arithmetic in $\mathbb{F}_{p^{27}}$

B.1 Cyclotomic inversion

We follow the same procedure as in A.2. The element $a = a_0 + a_1 w + a_2 w^2 \in \mathbb{F}_{p^{27}}$ with $a_i \in \mathbb{F}_{p^9}$ in the cyclotomic subgroup $G_{\phi_3(\mathbb{F}_{p^9})}$ satisfies $a^{p^{18}+p^9+1} = 1$ so that $a^{-1} = a^{p^{18}} a^{p^9}$.
In order to compute $a^{p^{18}} a^{p^9}$, we need the values of w^{p^9} and $w^{p^{18}}$. We have
$w^{p^9} = w^{3(p^9-1)/3+1} = w^{3(p^9-1)/3} w = (w^3)^{(p^9-1)/3} w = (2^{1/9})^{(p^9-1)/3} w$ since $w^3 = 2^{1/9}$. Let $\sigma = (2^{1/9})^{(p^9-1)/3}$ then $\sigma \neq 1$ and $\sigma^3 = 1$. Hence σ is a primitive cubic root of unity in $\mathbb{F}_{p^9}$ i.e. $\phi_3(\sigma) = 0$. We obtain $w^{p^9} = \sigma w$ and we now compute $w^{p^{18}}$ as $w^{p^{18}} = (w^{p^9})^{p^9} = (\sigma w)^{p^9} = \sigma(w)^{p^9} = \sigma\sigma w = \sigma^2 w$.
$a^{p^9} = a_0 + a_1 w^{p^9} + a_2 (w^2)^{p^9} = a_0 + a_1\sigma w + a_2\sigma^2 w^2$ and
$a^{p^{18}} = (a^{p^9})^{p^9} = a_0 + a_1(\sigma w)^{p^9} + a_2(\sigma^2 w^2)^{p^9} = a_0 + a_1\sigma^2 w + a_2\sigma^4 w^2$. After expanding and reducing using $w^3 = 2^{1/9}$ and $\phi_3(\sigma) = \sigma^2 + \sigma + 1 = 0$ we obtain

$$a^{p^{18}} a^{p^9} = (a_0^2 - a_1 a_2 2^{1/9}) + (a_2^2 2^{1/9} - a_0 a_1)w + (a_1^2 - a_0 a_2)w^2$$

The computation costs $3(36m + 95a) + 3(36m + 149a) + 3(9a) = 216m + 759a$.

B.2 Frobenius operators

The p^i−Frobenius is the map $\pi^i\colon \mathbb{F}_{p^{27}} \to \mathbb{F}_{p^{27}}, a \mapsto a^{p^i}$.
Let $a = a_0 + a_1 w + a_2 w^2$ with $a_i \in \mathbb{F}_{p^9}$ an element of $\mathbb{F}_{p^{27}}$.
$\pi(a) = a^p = (a_0 + a_1 w + a_2 w^2)^p = a_0^p + a_1^p w^p + a_2^p (w^2)^p$. The element $a_0 \in \mathbb{F}_{p^9}$ can be written as $a_0 = (h_0 + h_1 u + h_2 u^2) + (h_3 + h_4 u + h_5 u^2)v + (h_6 + h_7 u + h_8 u^2)v^2$, $h_i \in \mathbb{F}_p$. We have $a_0^p = (h_0 + h_1 u + h_2 u^2 + (h_3 + h_4 u + h_5 u^2)v + (h_6 + h_7 u + h_8 u^2)v^2)^p$, $h_i^p = h_i$.

$u^p = u^{3(p-1)/3+1} = (u^3)^{(p-1)/3}u = 2^{(p-1)/3}u$. Since 2 is not a cube in $\mathbb{F}_p$, we have $\alpha = 2^{(p-1)/3}$ $\alpha \neq 1$ and $\alpha^3 = 1$. It means that α is a primitive cubic root of unity in $\mathbb{F}_p$ and $u^p = \alpha u$.
$v^p = v^{3(p-1)/3+1} = (v^3)^{(p-1)/3}v = (2^{1/3})^{(p-1)/3}v = 2^{(p-1)/9}v$.
We have $\beta = 2^{(p-1)/9} \neq 1$ and $\beta^9 = 1$. Thus β is a primitive ninth root of unity in $\mathbb{F}_p$ and $v^p = \beta v$;
$w^p = w^{3(p-1)/3+1} = (w^3)^{(p-1)/3}v = (2^{1/9})^{(p-1)/3}v = 2^{(p-1)/27}v$. We also observe that $\gamma = 2^{(p-1)/27} \neq 1$, $\gamma^3 = 2^{(p-1)/9} = \beta \neq 1$, $\gamma^9 = 2^{(p-1)/3} = \alpha \neq 1$, $\gamma^{27} = 1$. Thus γ is a primitive twenty-seventh root of unity in $\mathbb{F}_p$ and $w^p = \gamma w$.

$$\begin{aligned}
a_0^p &= ((h_0 + h_1u + h_2u^2) + (h_3 + h_4u + h_5u^2)v + (h_6 + h_7u + h_8u^2)v^2)^p \\
&= (h_0 + h_1u^p + h_2(u^2)^p) + (h_3 + h_4u^p + h_5(u^2)^p)v^p + (h_6 + h_7u^p + h_8(u^2)^p)(v^2)^p \\
&= (h_0 + h_1\alpha u + h_2\alpha^2u^2) + (h_3 + h_4\alpha u + h_5\alpha^2u^2)\beta v + (h_6 + h_7\alpha u + h_8\alpha^2u^2)\beta^2v^2 \\
&= (h_0 + h_1\alpha u + h_2\alpha^2u^2) + (h_3\beta + h_4\alpha\beta u + h_5\alpha^2\beta u^2)v + (h_6\beta^2 + h_7\alpha\beta^2u + h_8\alpha^2\beta^2u^2)v^2. \\
a_1^p &= (h_9 + h_{10}u + h_{11}u^2) + (h_{12} + h_{13}u + h_{14}u^2)v + (h_{15} + h_{16}u + h_{17}u^2)v^2)^p \\
&= (h_9 + h_{10}u^p + h_{11}(u^2)^p) + (h_{12} + h_{13}u^p + h_{14}(u^2)^p)v^p + (h_{15} + h_{16}u^p + h_{17}(u^2)^p)(v^2)^p \\
&= (h_9 + h_{10}\alpha u + h_{11}\alpha^2u^2) + (h_{12} + h_{13}\alpha u + h_{14}\alpha^2u^2)\beta v + (h_{15} + h_{16}\alpha u + h_{17}\alpha^2u^2)\beta^2v^2 \\
&= (h_9 + h_{10}\alpha u + h_{11}\alpha^2u^2) + (h_{12}\beta + h_{13}\alpha\beta u + h_{14}\alpha^2\beta u^2)v + (h_{15}\beta^2 + h_{16}\alpha\beta^2u + \\
&\quad h_{17}\alpha^2\beta^2u^2)v^2. \\
a_2^p &= (h_{18} + h_{19}u + h_{20}u^2) + (h_{21} + h_{22}u + h_{23}u^2)v + (h_{24} + h_{25}u + h_{26}u^2)v^2)^p \\
&= (h_{18} + h_{19}u^p + h_{20}(u^2)^p) + (h_{21} + h_{22}u^p + h_{23}(u^2)^p)v^p + (h_{24} + h_{25}u^p + h_{26}(u^2)^p)(v^2)^p \\
&= (h_{18} + h_{19}\alpha u + h_{20}\alpha^2u^2) + (h_{21} + h_{22}\alpha u + h_{23}\alpha^2u^2)\beta v + (h_{24} + h_{25}\alpha u + h_{26}\alpha^2u^2)\beta^2v^2. \\
&= (h_{18} + h_{19}\alpha u + h_{20}\alpha^2u^2) + (h_{21}\beta + h_{22}\alpha\beta u + h_{23}\alpha^2\beta u^2)v + (h_{24}\beta^2 + h_{25}\alpha\beta^2u + \\
&\quad h_{26}\alpha^2\beta^2u^2)v^2. \\
\pi(a) &= (a_0 + a_1w + a_2w^2)^p = a_0^p + a_1^pw^p + a_2^p(w^2)^p = a_0^p + a_1^p\gamma w + a_2^p\gamma^2w^2 \\
&= (h_0 + h_1\alpha u + h_2\alpha^2u^2) + (h_3\beta + h_4\alpha\beta u + h_5\alpha^2\beta u^2)v + (h_6\beta^2 + h_7\alpha\beta^2u + h_8\alpha^2\beta^2u^2)v^2 + \\
&\quad ((h_9 + h_{10}\alpha u + h_{11}\alpha^2u^2) + (h_{12}\beta + h_{13}\alpha\beta u + h_{14}\alpha^2\beta u^2)v + (h_{15}\beta^2 + h_{16}\alpha\beta^2u + \\
&\quad h_{17}\alpha^2\beta^2u^2)v^2)\gamma w + ((h_{18} + h_{19}\alpha u + h_{20}\alpha^2u^2) + (h_{21}\beta + h_{22}\alpha\beta u + h_{23}\alpha^2\beta u^2)v + \\
&\quad (h_{24}\beta^2 + h_{25}\alpha\beta^2u + h_{26}\alpha^2\beta^2u^2)v^2)\gamma^2w^2.
\end{aligned}$$

We have these following algebraic relations: $\alpha = \beta^3$, $\alpha\beta = \beta^4$, $\alpha\beta^2 = \beta^5$, $\alpha^2\beta = \beta^7$ and $\alpha^2\beta^2 = \beta^8$. Therefore

$$\begin{aligned}
\pi(a) = {} & ((h_0 + h_1\beta^3u + h_2\beta^6u^2) + (h_3\beta + h_4\beta^4u + h_5\beta^7u^2)v + (h_6\beta^2 + h_7\beta^5u + h_8\beta^8u^2)v^2) + \\
& ((h_9\gamma + h_{10}\beta^3\gamma u + h_{11}\beta^6\gamma u^2) + (h_{12}\beta\gamma + h_{13}\beta^4\gamma u + h_{14}\beta^7\gamma u^2)v + (h_{15}\beta^2\gamma + h_{16}\beta^5\gamma u + \\
& h_{17}\beta^8\gamma u^2)v^2)w + ((h_{18}\gamma^2 + h_{19}\beta^3\gamma^2u + h_{20}\beta^6\gamma^2u^2) + (h_{21}\beta\gamma^2 + h_{22}\beta^4\gamma^2u + h_{23}\beta^7\gamma^2u^2)v + \\
& (h_{24}\beta^2\gamma^2 + h_{25}\beta^5\gamma^2u + h_{26}\beta^8\gamma^2u^2)v^2)w^2.
\end{aligned}$$

The following values are precomputed: $\lambda_0 = \beta^2$, $\lambda_1 = \beta^3$, $\lambda_2 = \beta^4$, $\lambda_3 = \beta^5$, $\lambda_4 = \beta^6$, $\lambda_5 = \beta^7$, $\lambda_6 = \beta_8$, $\lambda_7 = \gamma^2$, $\lambda_8 = \beta\gamma$, $\lambda_9 = \lambda_0\gamma$, $\lambda_{10} = \lambda_1\gamma$, $\lambda_{11} = \lambda_2\gamma$, $\lambda_{12} = \lambda_3\gamma$, $\lambda_{13} = \lambda_4\gamma$, $\lambda_{14} = \lambda_5\gamma$, $\lambda_{15} = \lambda_6\gamma$, $\lambda_{16} = \lambda_0\lambda_7$, $\lambda_{17} = \lambda_1\lambda_7$, $\lambda_{18} = \lambda_2\lambda_7$, $\lambda_{19} = \lambda_3\lambda_7$, $\lambda_{20} = \lambda_4\lambda_7$, $\lambda_{21} = \lambda_5\lambda_7$, $\lambda_{22} = \lambda_6\lambda_7$. $\lambda_{23} = \beta\lambda_7$.

Thus
$$\begin{aligned}
\pi(a) = {} & ((h_0 + h_1\lambda_1u + h_2\lambda_4u^2) + (h_3\beta + h_4\lambda_2u + h_5\lambda_5u^2)v + (h_6\lambda_0 + h_7\lambda_3u + \\
& h_8\lambda_6u^2)v^2) + ((h_9\gamma + h_{10}\lambda_{10}u + h_{11}\lambda_{13}u^2) + (h_{12}\lambda_8 + h_{13}\lambda_{11}u + h_{14}\lambda_{14}u^2)v + \\
& (h_{15}\lambda_9 + h_{16}\lambda_{12}u + h_{17}\lambda_{15}u^2)v^2)w + ((h_{18}\lambda_7 + h_{19}\lambda_{17}u + h_{20}\lambda_{20}u^2) + (h_{21}\lambda_{23} + \\
& h_{22}\lambda_{18}u + h_{23}\lambda_{21}u^2)v + (h_{24}\lambda_{16} + h_{25}\lambda_{19}u + h_{26}\lambda_{22}u^2)v^2)w^2.
\end{aligned}$$

The cost of p-Frobenius: $26m + 18a$. This is also equal to the cost of p^2, p^4, p^5, p^7, p^8 Frobenius
For the p^9 Frobenius operator, observe from B.1 that $w^{p^9} = \sigma w$. Then

$$a^{p^9} = a_0 + a_1\sigma w + a_2\sigma^2 w^2 = ((h_0 + h_1 u + h_2 u^2) + (h_3 + h_4 u + h_5 u^2)v + (h_6 + h_7 u + h_8 u^2)v^2) + ((h_9 + h_{10} u + h_{11} u^2) + (h_{12} + h_{13} u + h_{14} u^2)v + (h_{15} + h_{16} u + h_{17} u^2)v^2)\sigma w + ((h_{18} + h_{19} u + h_{20} u^2) + (h_{21} + h_{22} u + h_{23} u^2)v + (h_{24} + h_{25} u + h_{26} u^2)v^2)\sigma^2 w^2.$$

We then have $a^{p^9} = ((h_0 + h_1 u + h_2 u^2) + (h_3 + h_4 u + h_5 u^2)v + (h_6 + h_7 u + h_8 u^2)v^2) + ((h_9\sigma + h_{10}\sigma u + h_{11}\sigma u^2) + (h_{12}\sigma + h_{13}\sigma u + h_{14}\sigma u^2)v + (h_{15}\sigma + h_{16}\sigma u + h_{17}\sigma u^2)v^2)w + ((h_{18}\sigma^2 + h_{19}\sigma^2 u + h_{20}\sigma^2 u^2) + (h_{21}\sigma^2 + h_{22}\sigma^2 u + h_{23}\sigma^2 u^2)v + (h_{24}\sigma^2 + h_{25}\sigma^2 u + h_{26}\sigma^2 u^2)v^2)w^2.$

As $s = \sigma^2$ is precomputed; we have $a^{p^9} = ((h_0+h_1u+h_2u^2)+(h_3+h_4u+h_5u^2)v+(h_6+h_7u+h_8u^2)v^2)+((h_9\sigma+h_{10}\sigma u+h_{11}\sigma u^2)+(h_{12}\sigma+h_{13}\sigma u+h_{14}\sigma u^2)v+(h_{15}\sigma+h_{16}\sigma u+h_{17}\sigma u^2)v^2)w+((h_{18}s + h_{19}su + h_{20}su^2) + (h_{21}s + h_{22}su + h_{23}su^2)v + (h_{24}s + h_{25}su + h_{26}su^2)v^2)w^2$.
The cost of p^9-Frobenius: $18m + 18a$. This is the same as the cost of p^3 and p^6 Frobenius.

C Arithmetic in $\mathbb{F}_{p^{15}}$

The arithmetic of the extension field F_{p^5} is studied in [32]. In this section we only consider inversion in cyclotomic subgroup and Frobenius operators.

C.1 Cyclotomic inversion

An element $a = a_0 + a_1 v + a_2 v^2 \in \mathbb{F}_{p^{15}}$ with $a_i \in \mathbb{F}_{p^5}$ in the cyclotomic subgroup $G_{\phi_3(p^5)}$ satisfies $a^{p^{10}+p^5+1} = 1$ so that $a^{-1} = a^{p^{10}} a^{p^5}$.
$v^{p^5} = v^{5(p^5-1)/5+1} = v^{5(p^5-1)/5} v = (v^5)^{(p^5-1)/5} v = (2^{1/3})^{(p^5-1)/5} v$ since $v^5 = 2^{1/3}$.
Let $\omega = (2^{1/3})^{(p^5-1)/5}$. We have $\omega \neq 1$ and $\omega^5 = 1$.
Hence ω is a primitive fifth root of unity in $\mathbb{F}_{p^5}$.
We obtain $v^{p^5} = \omega v$, and $v^{p^{10}} = (v^{p^5})^{p^5} = (\omega v)^{p^5} = \omega (v)^{p^5} = \omega\omega v = \omega^2 v$.
$a^{p^5} = (a_0 + a_1 v + a_2 v^2)^{p^5} = a_0^{p^5} + a_1^{p^5} v^{p^5} + a_2^{p^5} (v^2)^{p^5} = a_0 + a_1 v^{p^5} + a_2 (v^2)^{p^5} = a_0 + a_1 \omega v + a_2 \omega^2 v^2$.
$a^{p^{10}} = (a^{p^5})^{p^5} = a_0 + a_1(\omega v)^{p^5} + a_2(\omega^2 v^2)^{p^5} = a_0 + a_1\omega^2 v + a_2 \omega^4 v^2$.
$a^{p^{10}} a^{p^5} = (a_0 + a_1\omega^2 v + a_2\omega^4 v^2)(a_0 + a_1\omega v + a_2\omega^2 v^2)$

After expanding and reducing using $v^3 = u$ and $\phi_5(\omega) = 0$ we obtain

$$a^{p^{10}} a^{p^5} = (a_0^2 + (1+\omega^4)a_1 a_2 u) + \omega(a_2^2 u + (1+\omega)a_0 a_1)v + \omega^2(a_1^2\omega + (1+\omega^2)a_0 a_2)v^2$$

This costs $3(9m + 137a) + 3(9m + 137a) + 3(5a) + 2m_u = 54m + 822a + 2m_u$

C.2 Frobenius operators

The p^i−Frobenius is the map $\pi^i \colon \mathbb{F}_{p^{15}} \to \mathbb{F}_{p^{15}}, a \mapsto a^{p^i}$.
Let $a \in \mathbb{F}_{p^{15}}$; $a = a_0 + a_1 v + a_2 v^2$ with $a_i \in \mathbb{F}_{p^5}$.
$\pi(a) = a^p = (a_0 + a_1 v + a_2 v^2)^p = a_0^p + a_1^p v^p + a_2^p (v^2)^p$.
$a_0 \in \mathbb{F}_{p^5}$ i.e. $a_0 = g_0 + g_1 u + g_2 u^2 + g_3 u^3 + g_4 u^4, \quad g_i \in \mathbb{F}_p$.
$a_0^p = (g_0 + g_1 u + g_2 u^2 + g_3 u^3 + g_4 u^4)^p = g_0 + g_1 u^p + g_2 (u^2)^p + g_3 (u^3)^p + g_4 (u^4)^p$,

since $g_i^p = g_i$.
$u^p = u^{5(p-1)/5+1} = (u^5)^{(p-1)/5}u = 2^{(p-1)/5}u$.
2 is not a fifth power in $\mathbb{F}_p$; so $2^{(p-1)/5} \neq 1$.
Let $\theta = 2^{(p-1)/5}$, $\theta \neq 1$ and $\theta^5 = 1$.
It means that θ is a primitive fifth root of unity in $\mathbb{F}_p$ and $u^p = \theta u$.
$a_0^p = g_0 + g_1u^p + g_2(u^2)^p + g_3(u^3)^p + g_4(u^4)^p = g_0 + g_1\theta u + g_2\theta^2u^2 + g_3\theta^3u^3 + g_4\theta^4u^4$.
$a_1^p = g_5 + g_6u^p + g_7(u^2)^p + g_8(u^3)^p + g_9(u^4)^p = g_5 + g_6\theta u + g_7\theta^2u^2 + g_8\theta^3u^3 + g_9\theta^4u^4$.
$a_2^p = g_{10} + g_{11}u^p + g_{12}(u^2)^p + g_{13}(u^3)^p + g_{14}(u^4)^p = g_{10} + g_{11}\theta u + g_{12}\theta^2u^2 + g_{13}\theta^3u^3 + g_{14}\theta^4u^4$.
$v^p = v^{5(p-1)/5+1} = (v^5)^{(p-1)/5}v = (2^{1/3})^{(p-1)/5}v = (2^{1/3})^{(p-1)/5}v$. $2^{1/3}$ is not a fifth power in $\mathbb{F}_p$; so $(2^{1/3})^{(p-1)/5} \neq 1$.
Set $\beta = (2^{1/3})^{(p-1)/5}$, we have $\beta \neq 1$; $\beta^5 = 1$. Thus β is a primitive fifth root of unity in $\mathbb{F}_p$ and $v^p = \beta v$. $a^p = (a_0+a_1v+a_2v^2)^p = a_0^p+a_1^pv^p+a_2^p(v^2)^p \quad = (g_0+g_1\theta u+g_2\theta^2u^2+g_3\theta^3u^3+g_4\theta^4u^4)+ (g_5+g_6\theta u+g_7\theta^2u^2+g_8\theta^3u^3+g_9\theta^4u^4)v^p \quad +(g_{10}+g_{11}\theta u+g_{12}\theta^2u^2+g_{13}\theta^3u^3+g_{14}\theta^4u^4)(v^p)^2 = (g_0 + g_1\theta u + g_2\theta^2u^2 + g_3\theta^3u^3 + g_4\theta^4u^4) + (g_5\beta + g_6\theta\beta u + g_7\theta^2\beta u^2 + g_8\theta^3\beta u^3 + g_9\theta^4\beta u^4)v +(g_{10}\beta^2 + g_{11}\theta\beta^2u + g_{12}\theta^2\beta^2u^2 + g_{13}\theta^3\beta^2u^3 + g_{14}\theta^4\beta^2u^4)v^2$.
We precomputed these following values: $c_0 = \theta^2$ $c_1 = \theta^3$, $c_2 = \theta^4$, $c_3 = \beta^2$, $c_4 = \theta\beta$, $c_5 = c_0\beta$, $c_6 = c_1\beta$, $c_7 = c_2\beta$, $c_8 = \theta c_3$, $c_9 = c_0c_3$, $c_{10} = c_1c_3$, $c_{11} = c_2c_3$. So $\pi(a) = (g_0 + g_1\theta u + g_2c_0u^2 + g_3c_1u^3 + g_4c_2u^4) + (g_5\beta + g_6c_4u + g_7c_5u^2 + g_8c_6u^3 \quad +g_9c_7u^4)v + (g_{10}c_3 + g_{11}c_8u + g_{12}c_9u^2 + g_{13}c_{10}u^3 + g_{14}c_{11}u^4)v^2$.

The cost of p-Frobenius: $14m+12a$. This is the same cost as computing $p^2, p^3, p^4, p^6, p^7, p^8, p^9$ Frobenius.

For the p^5 Frobenius operator, observe from C.1 that $v^{p^5} = \omega v$. Then

$$a^{p^5} = (g_0 + g_1u + g_2u^2 + g_3u^3 + g_4u^4) + (g_5 + g_6u + g_7u^2 + g_8u^3 + g_9u^4)v^{p^5} + (g_{10} + g_{11}u + g_{12}u^2 + g_{13}u^3 + g_{14}u^4)(v^{p^5})^2.$$
$$= (g_0 + g_1u + g_2u^2 + g_3u^3 + g_4u^4) + (g_5\omega + g_6\omega u + g_7\omega u^2 + g_8\omega u^3 + g_9\omega u^4)v + (g_{10}\omega^2 + g_{11}\omega^2u + g_{12}\omega^2u^2 + g_{13}\omega^2u^3 + g_{14}\omega^2u^4)v^2.$$

We precomputed $d = \omega^2$.
$\pi^5(a) = a^{p^5} = (g_0 + g_1u + g_2u^2 + g_3u^3 + g_4u^4) + (g_5\omega + g_6\omega u + g_7\omega u^2 + g_8\omega u^3 + g_9\omega u^4)v + (g_{10}d + g_{11}du + g_{12}du^2 + g_{13}du^3 + g_{14}du^4)v^2$. The cost of p^5-Frobenius: $10m_{576} + 12a_{576}$. This is the same as the cost of p^{10} Frobenius.