Field Arithmetic

3.1 Representation of Extension Fields

BN-curves are defined over prime fields, which means the computation of a pairing over a BN-curve relies on arithmetic over finite fields. Hence, efficient implementation of the underlying extension fields is crucial for fast pairing computation. Arithmetic over $\mathbb{F}_{q^2}$ is required for manipulating points on the twisted curve, and the computation of the Miller function. Moreover, accumulating and multiplying values to compute $f_{n,P}$ and the final exponentiation involves arithmetic over $\mathbb{F}_{q^{12}}$. IEEE P1363.3 [1] recommends using towers to represent $\mathbb{F}_{q^k}$. Construction of tower extensions for the purpose of pairing computation has been explored in [8, 17, 24, 7]. Next we outline and analyze two approaches for constructing tower fields.

Note that if $q \equiv 3 \bmod 4$, then both -1 and -2 are quadratic non-residues and we can represent $\mathbb{F}_{q^2}$ by $\mathbb{F}_q[i]/(i^2 - \beta)$ where $\beta = -1$ or -2. Multiplications by i are required throughout the pairing computation, for instance when multiplying two extension field elements. Representing $\mathbb{F}_{q^2}$ as above, multiplications by i are very cheap, requiring either only a simple negation or a negation and an addition. Having the choice of 2 elements for β also leaves us some choice of representation for implementing higher extensions. When x is odd, we get $Q(x) \equiv 3 \bmod 4$, and when x is even, we get $Q(x) \equiv 1 \bmod 4$. When x is even, neither -1 nor -2 is guaranteed to be a quadratic non-residue so multiplication by i can end up being relatively costly. Therefore, when computing BN-curves using the polynomial $Q(x)$, we restrict ourselves to choosing odd x, so that $q \equiv 3 \bmod 4$.

Geovandro et al. [17] recommend a family of implementation friendly BN-curves which has a very natural choice for the suitable representation of extension fields. We give a description of this sub-family and outline its benefits.

Definition 3.1.1. A BN-curve $E_b : y^2 = x^3 + b$ over $\mathbb{F}_q$ is called friendly if $q \equiv 3 \bmod 4$ and there exist $c, d \in \mathbb{F}_q^*$ such that either $b = c^4 + d^6$ or $b = c^6 + 4d^4$.

One can use the following properties of friendly BN-curves to implement the pairing computation in an efficient manner:

1. Let $\xi = c^2 + d^3 i$ if $b = c^4 + d^6$, or $\xi = c^3 + 2d^2 i$ if $b = c^6 + 4d^4$. Then, $b = \xi\overline{\xi}$. Lemma 2 of [17] says that ξ is neither a square nor a cube in $\mathbb{F}_{p^2}$. Thus, we can use ξ to construct $\mathbb{F}_{q^{12}}$ as follows:
$$\mathbb{F}_{q^6} = \mathbb{F}_{q^2}[v]/(v^3 - \xi).$$
$$\mathbb{F}_{q^{12}} = \mathbb{F}_{q^6}[w]/(w^2 - v).$$

2. Theorem 1 in [17] says that the curve E'_b given by:
$$E'_b : y^2 = x^3 + \frac{b}{\xi} = x^3 + \overline{\xi}$$
gives a D-type sextic twist of E_b.

3. Generators for $E'(\mathbb{F}_{p^2})[n]$ can be found as $[h]G$, where $h = 2p - n$ and $G = (-di, c)$ or $G = (-c, d(1 - i))$, respectively.

Using the above sub-family, square or cube detection is not necessary to build field extensions or generate a twist. Moreover, one does not have to compute the order of the curve which may generate the sextic twist, as the correct twist is immediately revealed.

Another approach to finding appropriate irreducible polynomials for constructing tower extensions of fields is to use the following theorem of Benger and Scott [8]:

Theorem 3.1.2 ([8])**.** *Let $m > 1, n > 0$ be integers, q an odd prime and $\alpha \in \mathbb{F}_{q^n}^*$. The binomial $x^m - \alpha$ is irreducible in $\mathbb{F}_{q^n}[x]$ if the following two conditions are satisfied:*

- *Each prime factor p of m divides $q - 1$ and $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) \in \mathbb{F}_q$ is not a p-th residue in $\mathbb{F}_q$;*
- *If $m \equiv 0 \bmod 4$ then $q^4 \equiv 1 \bmod 4$.*

Based on the above theorem, Benger and Scott [8] give the following construction for BN primes congruent to 3 mod 8. The same conclusion is also drawn in Shirase [41]:

Construction 3.1.3. *Let $q = q(x)$ be the prime characteristic of the field over which a BN-curve is defined. If $x \equiv 7$ or $11 \bmod 12$ then $y^6 - (1 + \sqrt{-1})$ is irreducible over $\mathbb{F}_{q^2} = \mathbb{F}_q(\sqrt{-1})$.*

We are able to use the above construction in 2/3rds of the cases when $q \equiv 3 \bmod 8$; i.e. $x \equiv 3 \bmod 4$. It only fails when $x \equiv 2 \bmod 3$. Since we are restricting ourselves to choosing odd x, we also need to consider the case when $x \equiv 1 \bmod 4$. Following [8], we give the following construction for BN-primes congruent to 7 mod 8:

Construction 3.1.4. *Let $q = q(x)$ be the prime characteristic of the field over which a BN-curve is defined. If $x \equiv 2, 3, 4, 6, 7$ or $8 \bmod 9$ then $y^6 - (1 + \sqrt{-2})$ is irreducible over $\mathbb{F}_{q^2} = \mathbb{F}_q(\sqrt{-2})$.*

Proof. We will show that the conditions in Theorem 3.1.2 are satisfied two-thirds of the time for $m = 6, n = 2$, when q a BN-prime congruent to 7 mod (8), and $\alpha = 1 + \sqrt{-2}$. To satisfy condition (2), it suffices to show that $q^4 \equiv 1 \bmod 4$. This is trivial because $q \equiv 3 \bmod 4$. Now, $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = (1 + \sqrt{-2})(1 - \sqrt{-2}) = 3$; and the prime factors of 12 are 2 and 3. To satisfy condition (1) we need to show the following:

- $2 \mid q - 1$ and $3 \mid q - 1$;
- 3 is not a cubic or a quadratic residue in $\mathbb{F}_q$.

Recall that q is given by the polynomial $q(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$ for some $x \equiv 1 \bmod 4$. As a result $2 \mid q - 1$ and $3 \mid q - 1$. Morevoer, $x \equiv 1 \bmod 4$ implies that $x \equiv 1, 5$ or $9 \bmod 12$, which in turn implies that $q \equiv 7 \bmod 12$. As a result, 3 is not a quadratic residue in $\mathbb{F}_q$. We now need to determine when 3 is a cubic residue in $\mathbb{F}_q$. A prime $q \equiv 1 \bmod 3$ can be written as $q = a^2 + 3b^2$ for some integers a, b. It was conjectured by Euler and proven by Gauss that 3 is a cubic residue if and only if $9 \mid b$, or $9 \mid (a \pm b)$ [26]. For BN-primes we can write $q(x) = a(x) + 3x^2$, where $a(x) = 6x^2 + 3x + 1$ [41]. Hence, 3 is a cubic residue if $9 \mid x$, or $9 \mid 6x^2 + 4x + 1$, or $9 \mid 6x^2 + 2x + 1$. This occurs when $x \equiv 0, 1,$ or $5 \bmod 9$ which happens with probability 1/3. Thus 3 is a cubic non-residue modulo q for approximately 2/3rds of the values $q \equiv 7 \bmod 8$.

When deciding on the above construction for BN-primes congruent to 7 mod 8, we tried to choose α so that $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ is minimized. This means that the polynomials used to construct tower extensions will have small coefficents, so arithmetic will be efficient.

3.1.1 Towering Scheme for Primes Congruent to 3 mod 8

Aranha et al. [4] use $E : y^2 = x^3 + 2$ for the BN-curve, and $x = -(2^{62} + 2^{55} + 1)$ to generate the 254-bit prime $Q(x)$. As a result, both methods outlined above yield the same towering scheme for the prime field over which this curve is defined:

- $\mathbb{F}_{q^2} = \mathbb{F}_q[i]/(i^2 - \beta)$, where $\beta = -1$.
- $\mathbb{F}_{q^6} = \mathbb{F}_{q^2}[v]/(v^3 - \xi)$, where $\xi = 1 + i$.
- $\mathbb{F}_{q^{12}} = \mathbb{F}_{q^6}[w]/(w^2 - v)$.

This towering scheme is ideal since it keeps the coefficents of the irreducible polynomials as small as possible. At some points during the pairing computation, it is required that finite field elements be multiplied by ξ (for example, when multiplying two elements over $\mathbb{F}_{q^{12}}$). Using the above towering scheme, multiplication by i requires one negation over $\mathbb{F}_q$, and multiplication by ξ requires only one addition over $\mathbb{F}_{q^2}$. For primes congruent to 3 mod 8, we use the above towering scheme.

We represent all prime and extension fields using a towering scheme as above, varying the choice of ξ and v to suit the prime q in question.

3.1.2 Towering Scheme for Primes Congruent to 7 mod 8

We now illustrate explicit towering schemes for primes congruent to 7 mod 8 using the 446-bit prime given by $Q(x)$, where $x = 2^{110} + 2^{36} + 1$. This prime was recommended in [17] and used in [3] to implement the O-Ate pairing. In this case, the above scheme does not work because $1 + i$ is not a cubic non-residue in $\mathbb{F}_{p^2}$. Following the recommendation in [3], the BN-curve used is:

$$E_{257} : y^2 = x^3 + 257$$

We then get the following towering scheme which we refer to as **Scheme 1**:

- $\mathbb{F}_{q^2} = \mathbb{F}_q[i]/(i^2 - \beta)$, where $\beta = -1$.
- $\mathbb{F}_{q^6} = \mathbb{F}_{q^2}[v]/(v^3 - \xi)$, where $\xi = 16 + i$.
- $\mathbb{F}_{q^{12}} = \mathbb{F}_{q^6}[w]/(w^2 - v)$.

Here β is minimal, however ξ is slightly large. Minimizing β might be beneficial because a large chunk of the arithmetic during pairing computation is performed over $\mathbb{F}_{q^2}$. Multiplication by i requires a negation; multiplication by ξ requires five additions in $\mathbb{F}_{q^2}$.

To increase the efficiency of the pairing computation we can try a towering scheme as dictated by Construction 2. This will make multiplication by ξ cheaper:

- $\mathbb{F}_{q^2} = \mathbb{F}_q[i]/(i^2 - \beta)$, where $\beta = -2$.
- $\mathbb{F}_{q^6} = \mathbb{F}_{q^2}[v]/(v^3 - \xi)$, where $\xi = 1 + i$.
- $\mathbb{F}_{q^{12}} = \mathbb{F}_{q^6}[w]/(w^2 - v)$.

We refer to the above scheme as **Scheme 2**. Here, multiplication by i requires one addition and one negation in $\mathbb{F}_q$, and multiplication by ξ requires two additions in $\mathbb{F}_{q^2}$. Note that here we have taken the opposite approach to the one suggested in [17]. Instead of choosing a curve that gives the right twist, and then letting these choices dictate the towering scheme, we first choose a towering scheme that optimizes extension field arithmetic and deal with the curve later. As illustrated in Appendix A using the curve BN446, using Scheme 2 results in a faster pairing than using Scheme 1. Since we did not follow the recommendations of [17], we lose the benefit of being able to generate towering schemes and twists without performing additional mathematical operations. However, in pairing-based protocols, these operations need only be performed once, whereas there may be thousands of pairing computations required. As the bulk of the pairing computation requires extension field arithmetic, optimizing the arithmetic leads to better performance overall.

3.2 Field Arithmetic

3.2.1 Lazy Reduction

Before proceeding, we fix some notation regarding field operation algorithms and costs. Lower case variables denote single-precision integers, and upper case variables denote double-precision integers. $\times$ represents multiplication without reduction, and $\otimes$ represents multiplication with reduction. The letters m, s, a, and i denote a multiplication, squaring, addition, and inversion in $\mathbb{F}_q$ respectively. Likewise $\tilde{m}, \tilde{s}, \tilde{a}$, and $\tilde{\imath}$ denote multiplication, squaring, addition and inversion in $\mathbb{F}_{q^2}$ respectively. $m_u, \tilde{m}_u, s_u$ and $\tilde{s}_u$ denote unreduced multiplications and squarings in the respective field. We write m_b, m_i, m_ξ, and m_v for multiplication by b, i, ξ, and v respectively. To perform arithmetic over finite fields, we use Karatsuba multiplication and squaring with lazy reduction as in [4]. We extend their idea of lazy reduction to field inversion. By applying lazy reduction, we are able to save one $\mathbb{F}_q$ reduction per $\mathbb{F}_{q^2}$ inversion, and 13 $\mathbb{F}_q$ reductions per $\mathbb{F}_{q^{12}}$ inversion. This speeds up the inversion routine in $\mathbb{F}_{q^2}$ by 4%, and in $\mathbb{F}_{q^{12}}$ by 10%. Algorithms 3.1, 3.2, and 3.3 present our routines for inversion in the extension fields using lazy reduction. All costs for algorithms presented in this chapter are for the 254-bit BN prime used in [4].

Algorithm 3.1 Inversion in $\mathbb{F}_{q^2}$ (Cost $= i + 4m + 3r + 2a$)

Input: $a = a_0 + a_1 i;\ a_0, a_1 \in \mathbb{F}_q$
Output: $c = a^{-1} \in \mathbb{F}_{q^2}$
$T_0 \leftarrow a_0 \times a_0$
$T_1 \leftarrow -\beta \cdot (a_1 \times a_1)$
$T_0 \leftarrow T_0 + T_1$
$t_0 \leftarrow T_0 \bmod p$
$t \leftarrow t_0^{-1} \bmod p$
$c_0 \leftarrow a_0 \otimes t$
$c_1 \leftarrow -(a_1 \otimes t)$
return $c = c_0 + c_1 i$

3.2.2 Multiplication of Sparse Elements

Using the above towering scheme, the elements $\{1, v, v^2, w, vw, v^2 w\}$ form a basis for $\mathbb{F}_{q^{12}}$ over $\mathbb{F}_{q^2}$. When using projective and jacobian coordinates, the line function in the Miller

Algorithm 3.2 Inversion in $\mathbb{F}_{q^6}$ (Cost $= \tilde{i} + 9\tilde{m} + 3\tilde{s} + 9\tilde{r} + 14\tilde{a}$)

Input: $a = a_0 + a_1 v + a_2 v^2;\ a_0, a_1, a_2 \in \mathbb{F}_{q^2}$
Output: $c = a^{-1} \in \mathbb{F}_{q^6}$

$T_0 \leftarrow a_0 \times a_0$
$V_0 \leftarrow a_1 \times a_2$
$V_0 \leftarrow \xi V_0$
$V_0 \leftarrow T_0 - V_0$
$v_0 \leftarrow V_0 \bmod p$
$T_0 \leftarrow a_2 \times a_2$
$T_0 \leftarrow \xi T_0$
$V_1 \leftarrow a_1 \times a_0$
$V_1 \leftarrow T_0 - V_1$
$v_1 \leftarrow V_1 \bmod p$
$T_0 \leftarrow a_1 \times a_1$
$V_2 \leftarrow a_2 \times a_0$
$V_2 \leftarrow T_0 - V_2$
$v_2 \leftarrow V_2 \bmod p$
$c_1 \leftarrow a_1 \otimes v_2$
$c_1 \leftarrow \xi c_1$
$c_0 \leftarrow a_0 \otimes v_0$
$c_2 \leftarrow a_2 \otimes v_1$
$c_2 \leftarrow \xi c_2$
$t_0 \leftarrow c_0 + c_1$
$t_0 \leftarrow t_0 + c_2$
$t_0 \leftarrow t_0^{-1} \bmod p$
$c_0 \leftarrow v_0 \otimes t_0$
$c_1 \leftarrow v_1 \otimes t_0$
$c_2 \leftarrow v_2 \otimes t_0$
return $c = c_0 + c_1 v + c_2 v^2$

Algorithm 3.3 Inversion in $\mathbb{F}_{q^{12}}$ (Cost $= \tilde{i} + 15\tilde{m} + 9\tilde{s} + 18\tilde{r} + 69\tilde{a}$)

Input: $a = a_0 + a_1 w;\ a_0, a_1 \in \mathbb{F}_{q^6}$
Output: $c = a^{-1} \in \mathbb{F}_{q^{12}}$
$T_0 \leftarrow a_0 \times a_0$
$T_1 \leftarrow v \cdot (a_1 \times a_1)$
$T_0 \leftarrow T_0 - T_1$
$t_0 \leftarrow T_0 \bmod p$
$t_0 \leftarrow t_0^{-1} \bmod p$
$c_0 \leftarrow a_0 \otimes t_0$
$c_1 \leftarrow -a_1 \otimes t_0$
return $c = c_0 + c_1 w$

loop evaluates to a sparse $\mathbb{F}_{q^{12}}$ element containing only three of the six basis elements. In the case of a D-type twist, the line function evaluates to an element of the form

$$a_0 + a_1 w + a_2 v w, \qquad a_0, a_1, a_2 \in \mathbb{F}_{q^2}.$$

In the case of an M-type twist, it evaluates to an element of the form -

$$a_0 + a_1 v + a_2 v w, \qquad a_0, a_1, a_2 \in \mathbb{F}_{q^2}.$$

In both cases, when multiplying the line function evaluation with $f_{i,Q}(P)$, one can utilize its sparseness to avoid full $\mathbb{F}_{q^{12}}$ arithmetic. We use Algorithm 3.4 to multiply a sparse $\mathbb{F}_{q^{12}}$ element with a non-sparse $\mathbb{F}_{q^{12}}$ element. In this case, the sparse element arises as the evaluation of a line function when a D-type twist is involved. Note that multiplication by v involves a multiplication by ξ, which in turn is equal to one $\mathbb{F}_{q^2}$ addition. The dense-sparse multiplication algorithm presented in Algorithms 3.4 and 3.5 requires 17 fewer $\mathbb{F}_{q^2}$ additions than in [4]. The dense-sparse multiplication algorithm is similar when we are using an M-type twist, and requires an extra multiplication by v.

3.2.3 Mapping from the Twisted Curve to the Original Curve

Suppose we take ξ (as used in the towering scheme) to be the cubic and quadratic non-residue to generate the sextic twist of the BN-curve E. In the case of a D-type twist, the untwisting isomorphism is given by:

$$\Psi \colon (x, y) \mapsto (\xi^{\frac{1}{3}} x, \xi^{\frac{1}{2}} y) = (w^2 x, w^3 y).$$

Algorithm 3.4 D-type sparse-dense Multiplication in $\mathbb{F}_{q^{12}}$ (Cost = $13\tilde{m} + 6\tilde{r} + 44\tilde{a}$)

Input: $a = a_0 + a_1 w + a_2 vw,\ a_0, a_1, a_2 \in \mathbb{F}_{q^2}; b = b_0 + b_1 w,\ b_0, b_1 \in \mathbb{F}_{q^6}$
Output: $ab \in \mathbb{F}_{q^{12}}$

$A_0 \leftarrow a_0 \times b_0[0],\ A_1 \leftarrow a_0 \times b_0[1],\ A_2 \leftarrow a_0 \times b_0[2]$
$A \leftarrow A_0 + A_1 v + A_2 v^2$
$B \leftarrow \text{Fq6SparseMul}(a_1 w + a_2 vw, b_1)$
$c_0 \leftarrow a_0 + a_1, c_1 \leftarrow a_2, c_2 \leftarrow 0$
$c \leftarrow c_0 + c_1 v + c_2 v^2$
$d \leftarrow b_0 + b_1$
$E \leftarrow \text{Fq6SparseMul}(c, d)$
$F \leftarrow E - (A + B)$
$G \leftarrow Bv$
$H \leftarrow A + G$
$c_0 \leftarrow H \bmod p$
$c_1 \leftarrow F \bmod p$
return $c = c_0 + c_1 w$

Algorithm 3.5 Fq6SparseMul (Cost = $5\tilde{m} + 12\tilde{a}$)

Input: $a = a_0 + a_1 v,\ a_0, a_1 \in \mathbb{F}_{q^2}; b = b_0 + b_1 v + b_2 v^2,\ b_0, b_1, b_2 \in \mathbb{F}_{q^2}$
Output: $ab \in \mathbb{F}_{q^6}$

$A \leftarrow a_0 \times b_0,\ B \leftarrow a_1 \times b_1$
$C \leftarrow a_1 \times b_2 \xi$
$D \leftarrow A + C$
$e \leftarrow a_0 + a_1, f \leftarrow b_0 + b_1$
$E \leftarrow e \times f$
$G \leftarrow E - (A + B)$
$H \leftarrow a_0 \times b_2$
$I \leftarrow H + B$
return $D + Gv + Iv^2$

Following the construction of the tower extensions, both w^3 and w^2 are basis elements used to represent an element in $\mathbb{F}_{p^{12}}$. Therefore, the untwisting map is almost free.

The efficient untwisting described above is lost if we use a M-type twist where the untwisting isomorphism is given by:

$$\Psi\colon (x, y) \mapsto (\xi^{-\frac{2}{3}}x, \xi^{-\frac{1}{2}}y) = (\xi^{-1}w^4x, \xi^{-1}w^3y).$$

The cost of the untwisting in this case is 2 multiplications by ξ. However, if we compute the pairing value on the twisted curve instead of the original curve, then we do not need to use the untwisting map. Instead, we require the twisting map which is given by

$$\Psi^{-1}\colon (x, y) \mapsto (w^2x, w^3y).$$

Therefore, in order to make the pairing computation as efficient as possible, we compute the pairing on the original curve E when a D-type twist is involved, and on the twisted curve E' when an M-type twist is involved.

3.3 Final Exponentiation

As discussed earlier, the hard part of the final exponentiation is raising to the exponent $\frac{q^6+1}{n}$. In this section we focus on computing this for BN-curves. We can further split the remaining exponent into two additional parts:

$$\frac{q^6+1}{n} = (q^2+1)\frac{q^4-q^2+1}{n}.$$

Raising to q^2+1 is two applications of the Frobenius operator, which is considered a cheap operation (details to follow). Again, we are left with a hard to compute exponent — $\frac{q^4-q^2+1}{n}$. We outline the fastest way currently known to compute this exponent, described by Fuentes-Castañeda et al. [16].

We observe that if the Tate pairing is raised to some power, then the new function given by $e(P, Q)^m$ also gives a bilinear pairing. This pairing is non-degenerate as long as $n \nmid m$ since $e(P, Q)$ evaluates to an element in μ_n. Hence, instead of using $\frac{q^4-q^2+1}{n}$, we use a multiple of it which still gives a valid pairing.

Recall that for BN-curves, q and n are polynomials in x. Therefore, $\frac{q^4-q^2+1}{n}$ is also a polynomial in x. We call this polynomial $d(x)$. Fuentes-Castañeda et al. [16] showed that

$$\begin{aligned} 2x(6x^2+3x+1)d(x) = 1 &+ 6x + 12x^2 + 12x^3 \\ &+ (4x + 6x^2 + 12x^3)p(x) \\ &+ (6x + 6x^2 + 12x^3)p(x)^2 \\ &+ (-1 + 4x + 6x^2 + 12x^3)p(x)^3. \end{aligned}$$

The above value can be computed as follows. First, the following exponentiations are computed

$$f \mapsto f^x \mapsto f^{2x} \mapsto f^{4x} \mapsto f^{6x} \mapsto f^{6x^2} \mapsto f^{12x^2} \mapsto f^{12x^3}$$

which requires three exponentiations by x, three squarings and one multiplication. Then we compute the terms $a = f^{12x^3} f^{6x^2} f^{6x}$ and $b = a(f^{2x})^{-1}$ which require 3 multiplications. Finally, the final pairing value is obtained as

$$af^{6x^2} fb^p a^{p^2} (bf^-1)^{p^3}$$

which requires 6 multiplications and 6 Frobenius operations. In total, this part of the final exponentiation requires three exponentiations by x, three squarings, ten multiplications, and three Frobenius operations. In comparison, the previous fastest known method requires three additional multiplications and an additional squaring [4].

3.3.1 Exponentiation by x

The final exponentiation requires three exponentiations by x. This is traditionally done using a square-and-multiply method. Before we raise the output of the Miller loop to the power x, we exponentiate it to $(q^6-1)(q^2+1)$. This ensures that the value we need to exponentiate to the power x lies in the cyclotomic subgroup $\mathbb{G}_{\phi_6}(\mathbb{F}_{q^2})$.

Definition 3.3.1. We denote by $\mathbb{G}_{\phi_{12}}(\mathbb{F}_q)$ the cyclotomic subgroup of $\mathbb{F}^*_{q^{12}}$. This is the subgroup of all elements $\alpha \in \mathbb{F}_{q^{12}}$ such that $\alpha^{q^4-q^2+1} = 1$.

For more details on $\mathbb{G}_{\phi_{12}}(\mathbb{F}_q)$, refer to [18]. Now, we have

$$(q^6-1)(q^2+1) = (q^6-1)\frac{(q^6+1)}{q^4-q^2+1} = \frac{q^{12}-1}{q^4-q^2+1}.$$

Thus, an element raised to $(q^6-1)(q^2+1)$ lies in $\mathbb{G}_{\phi_{12}}(\mathbb{F}_q)$. Fast formulas for computing squarings in $\mathbb{G}_{\phi_{12}}(\mathbb{F}_q)$ are given in [4] which we use in our implementation. To compute a square, an element is first compressed, then squared in compressed form, and then decompressed. It is not known how to perform multiplication of compressed elements. Hence, when raising an element to the exponent x, one may keep squaring in compressed form, but when multiplication is required, one needs to decompress the elements. A compressed squaring requires $6\tilde{s}$, $28\tilde{a}$, and $3m_\xi$. A decompression requires $1\tilde{i}, 2\tilde{m}, 3\tilde{s}$, $9\tilde{a}$, and $2m_\xi$. Let h be the Hamming weight of x and l be the bit-length of x. Using Montogomery's simultaneous inversion trick, an exponentiation by x requires l compressed squarings, $l-1$ multiplications in $\mathbb{F}_{q^{12}}$, and $h(3\tilde{m}+3\tilde{s}+9\tilde{a}+2m_\xi)+3(h-1)\tilde{m}+\tilde{i}$ additional operations.

3.4 The Frobenius Operator

Let $a=\alpha+i\beta \in \mathbb{F}_{q^2}$ where $i=\sqrt{-1}$ is an adjoined square root. Then

$$\begin{aligned} a^q &= (\alpha+i\beta)^q \\ &= \alpha^q + i^q\beta^q \\ &= \alpha + i^3\beta && (\text{ since } q \equiv 3 \bmod 4) \\ &= \alpha - i\beta. \end{aligned}$$

Thus, computing a^q requires one base field addition.

Now, suppose $A=\sum_{i=0}^{5} a_i w^i \in \mathbb{F}_{q^{12}}$, with each $a_i \in \mathbb{F}_{q^2}$ and w is defined as in the towering schemes given in subsections 3.1.1 and 3.1.2. By examining the polynomial $q(x)$, we note that $q \equiv 1 \bmod 6$. Then,