Optimal Ate Pairing on Elliptic Curves with Embedding Degree 21

Mahamadou Abdou TOURE[1], **Karim SAMAKE**[2], **Sinaly TRAORE**[3]

[1]Centre de Recherche et de Formation pour l'Industrie Textile, Ségou, BP: 323, Mali

[2]Université des Sciences, des Techniques et des Technologies de Bamako, Faculté des Sciences et des Techniques, Bamako, Mali

[3]Université des Sciences, des Techniques et des Technologies de Bamako, Faculté des Sciences et des Techniques, Bamako, Mali

Abstract: ***Since the advent of pairing based cryptography, much research has been done on the efficient computations of elliptic curve pairings with even embedding degrees. However, little work has been done on the cases of odd embedding degrees and the existing few are to be improved. Thus, Fouotsa & al. have lead on the computation of optimal ate pairings on elliptic curves of embedding degrees k = 9; 15 and 27 which have twists of order three in [1]. According to our research, work does not exist on the case of embedding degree k = 21. This paper considers the computation of optimal ate pairings on elliptic curves of embedding degree k = 21 which have twists of order three too. Mainly, we provide a detailed arithmetic and cost estimation of operations in the tower field of the corresponding extension fields. Using the lattice-based method, we obtained good results of the final exponentiation and improved the theoretical cost for the Miller step at the 192-bits security level.***

Keywords: Optimal Pairings, Miller's algorithm, Elliptic Curves, LLL's algorithm

1. Introduction and state of the art

Pairings are bilinear applications defined on groups of rational points of elliptic or hyperelliptic curves. Thanks to the pairings, several cryptographic protocols have been developed such as the Identity-Based cryptosystem [2], the Identity-Based Encryption [3], the Identity-Based undeniable signature [4], short signatures [5] or Broadcast Encryption [6]. Let E be an elliptic curve defined over a finite field F_q and r a large prime divisor of the order of the group $E(F_q)$, the embedding degree of E relatively to r is the smallest integer k such that $r|q^k - 1$, that is, $r|q^k - 1$ but r does not divide any $q^i - 1, \forall i \in \{1, \cdots, k-1\}$. We used Optimal Ate Pairing as a pairing that is one of the most used in cryptography.

Its computation goes through the application of Miller's algorithm [7] and a final exponentiation. An efficient computation of the pairings requires a construction of pairing-friendly elliptic curves over F_q with an embedding degree k (see for example [8] and [9]) and efficient arithmetic in the towers associated with F_{q^k}. Following several work on the reduction of the Miller loop, the final exponentiation step has become a difficult task. In this article, we focus on Barretto, Lynn and Scott Elliptic Curves of embedding degree k = 21.

These curves admit twists of order 3 which make it possible to make the computations in the sub-fields and also lead to the technique of elimination of the denominator.

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

Security level	*Bits length of r*	*Bits length of q^k*	*kρ≈1*	*kρ≈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

This article is organized as follows:

In section 2, we make the state of the art on the work done on the Optimal Ate Pairing on elliptic curves.

In Section 3, we detail the arithmetic in the tower fields of $F_{q^{21}}$, and we compute the costs of the square in $F_{q^{21}}$, cyclotomic inversion and Frobenius operators.

In Section 4, we present the optimal Ate pairing and we talk about the Miller loop and estimate the cost of computing the final exponentiation using the LLL algorithm to reduce the cost of the computation.

Section 5 concerns the conclusion of the presentation and the prospects for future work on security.

2. State of the Art

2.1 LLL's Algorithm

The reduction of lattices consists in transforming any lattice into a one in which the vectors are rather short and almost orthogonal. This is a classic problem in mathematics that goes back to Lagrange and Gauss for rank 2 lattices. Lenstra, Lenstra and Lovász [10] invented a very efficient algorithm for the reduction of lattices with larger dimensions. This algorithm is known as LLL and has been used to solve a lot of problems.

Theorem 2.1 (Orthogonalization method of Gram-Schmidt). Let V be a vector subspace of dimension n and $(b_1, \ldots, b_n)$ a basis of V. We consider the vector family $(b_1^*, \ldots, b_n^*)$ defined by

$$b_1^* = b_1, \quad b_i^* = b_i - \sum_{j=1}^{i-1} m_{i,j} b_j^*; \quad \text{with for} \quad j < i$$

$$m_{i,j} = \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle}$$

Then $(b_1^*, \ldots, b_n^*)$ is a orthogonal basis of V.

Definition 2.1. (The reduction of Lenstra, Lenstra and Lovász).

A basis $(b_1, \ldots, b_n)$ is LLL-reduce if, the basis $(b_1^*, \ldots, b_n^*)$ produced by the Gram-Schmidt orthogonalization method verifies

$$|m_{i,j}| \le \frac{1}{2}, \quad for \quad 1 \le j < i \le n,$$

$$\frac{3}{4}\left\| b_{j-1}^* \right\|^2 \le \left\| b_i^* + m_{i,j-1} b_{i-1}^* \right\|^2, \quad for \quad 1 < i \le n.$$

2.2 Miller's Algorithm

Let E be an elliptic curve defined over F_q, a finite field of characteristic $q > 3$ and r a large prime factor of the curve group order. The Tate reduced pairing e_r is a bilinear and non-degenerate application defined as:

$$e_r : E(F_q)[r] \times E(F_{q^k})[r] \to \mu_r$$

$$(P, Q) \qquad \mapsto f_{r,P}(Q)^{\frac{q^k-1}{r}}$$

where μ_r is the group of r-th roots of the unit in $F_{q^k}^*$.

Set $[i] : P \mapsto [i]P$ the endomorphism defined on $E(F_q)$ which consists of adding P to itself i–1 times. Consider the endomorphism of Frobenius $\pi_q : E(\overline{F_q}) \to E(\overline{F_q}), (x,y) \mapsto (x^q, y^q)$ where $\overline{F_q}$ means the finite field closing F_q. The cardinal of E is obtained according to q and the trace of the endomorphism of Frobenius t as follows: $\# E(F_q) = q + 1 - t$ and π_q has exactly two eigenvalues which are 1 and q. Which allows us to consider $P \in G_1 = E(\overline{F_q})[r] \cap Ker(\pi_q - [1]) = E(F_q)[r]$ and $Q \in G_2 = E(\overline{F_q})[r] \cap Ker(\pi_q - [q])$. In [11], a variant of the Tate pairing called Ate pairing is defined as below:

$$e_A : G_2 \times G_1 \to \mu_r$$

$$(Q, P) \qquad \mapsto f_{t-1,Q}(P)^{\frac{q^k-1}{r}}$$

Optimal ate pairing have needs for a function $f_{m;U}(V)$, with $m \in Z$, which is computed efficiently using Miller's algorithm . To compute $f := f_{m;U}(V)$, Miller uses the double-and-add method as addition string for m (See [12, Chapter 9] for more informations). Write m as linear combination of powers of 2, that is $m = m_n 2^n + \cdots + m_1 2 + m_0 > 0$ with $m_i \in \{-1, 0, 1\}$, the Miller's algorithm (modified) which computes effectively $f_{m,U}(V)^{\frac{q^k-1}{r}}$ of two points U and V is given as follows:

```
Algorithm 1 : Miller's Algorithm
  1. Set $f \leftarrow 1$ and $R \leftarrow U$
  2. For $i = n - 1$ to 0 :
     a)  $f \leftarrow f^2 \times h_{R,R}(V)$
         $R \leftarrow 2R$                          Doubling Step
     b)  If $m_i = 1$ then :
             $f \leftarrow f \times h_{R,U}(V)$
             $R \leftarrow R + U$                   Addition Step
         End if
     c)  If $m_i = -1$ then :
             $f \leftarrow f / h_{R,U}(V)$
             $R \leftarrow R - U$                   Addition Step
         End if
  3.  Return $e = f^{\frac{q^k-1}{r}}$              Final Exponentiation
```

To reduce the length of the Miller loop to improve pairing computations, we use the generalized method developed by Vercauteren, [13].

2.3 Final exponentiation and the lattice-based method for calculating it

After getting the function from the Miller loop, the result is raised to the power $\frac{q^k-1}{r}$. This step is called the final exponentiation (line 3 in the Miller's algorithm). It can be seen that this exponent can be divided into two parts as follows:

$$\frac{q^k-1}{r} = \frac{q^k-1}{\phi_k(q)} \times \frac{\phi_k(q)}{r}$$

where $\phi_k(x)$ is the k-th cyclotomic polynomial. The final exponentiation is therefore computed as $f^{\frac{q^k-1}{r}} = \left[f^{\frac{q^k-1}{\phi_k(q)}} \right]^{\frac{\phi_k(q)}{r}}$. The computation of the first part $A = f^{\frac{q^k-1}{\phi_k(q)}}$ is generally less expensive since it requires little multiplication, inversion and q-th powering in F_{q^k}. The second part $A^{\frac{\phi_k(q)}{r}}$, more difficult, is called the hard part. We use the more efficient method described by Fuentes et al., [14] based on that developed by Scott et al. [15] to the hard part.

3. Arithmetic in the tower fields of $F_{q^{21}}$

Although the pairing is computed as an element of the F_{q^k} extension, the optimization of this computation uses the subfield arithmetic of F_{q^k} which are organized as a tower extension. In this section, we recall the round of finite field extensions $F_{q^{21}}$ and we detail the explicit costs of arithmetic operations.

Let q be a prime number other than 2, and $n; m > 0$ two integers. The easiest way to build a tower fields $F_{q^{nm}}$ over F_{q^n} would be to use a binomial $x^m - \alpha$ which is irreducible over F_{q^n} and successively add the roots of the root previously obtained until the tower has been completely constructed as the general method described by Benger & Scott [16].

To apply this theory on $F_{q^{21}}$, let's take $\alpha \in F_q$ such as $x^7 - \alpha$ be irreducible in F_q. A tower extension for $F_{q^{21}}$ can be constructed as follows:

$$F_{q^7} = F_q[u] \text{ with } u^7 = \alpha$$

$$F_{q^{21}} = F_{q^7}[v] \text{ with } v^3 = u \quad \text{where } u \in F_{q^7}$$

3.1 Squaring in $F_{q^{21}}$

Let $a = a_0 + a_1 v + a_2 v^2 \in F_{q^{21}}$ with $a_0,\ a_1, a_2 \in F_{q^7}$. We have : $a^2 = A_0 + A_1 v + A_2 v^2$ where :

$$\begin{cases} A_0 = a_0^2 + 2\alpha^{1/7} a_1 a_2 \\ A_1 = 2a_0 a_1 + \alpha^{1/7} a_2^2 \\ A_2 = 2a_0 a_2 + a_1^2 \end{cases}$$

Indeed,

$$\begin{aligned} a^2 &= \left(a_0 + a_1 v + a_2 v^2\right)^2 \\ &= a_0^2 + a_1^2 v^2 + a_2^2 v^4 + 2a_0 a_1 v + 2a_0 a_2 v^2 + 2a_1 a_2 v^3 \\ &= a_0^2 + a_1^2 v^2 + a_2^2 (uv) + 2a_0 a_1 v + 2a_0 a_2 v^2 + 2a_1 a_2 (u) \end{aligned}$$

because $v^3 = u.$

$$a^2 = \left(a_0^2 + 2\alpha^{1/7} a_1 a_2\right) + \left(\alpha^{1/7} a_2^2 + 2a_0 a_1\right)v + \left(a_1^2 + 2a_0 a_2\right)v^2$$

with $u^7 = \alpha$

The computation of the square costs $3m + 3c + 3a$.

Considering that $2xy = (x+y)^2 - x^2 - y^2$, we obtain:

$$\begin{cases} A_0 = a_0^2 + \alpha^{1/7}\left[(a_1 + a_2)^2 - a_1^2 - a_2^2\right] \\ A_1 = (a_0 + a_1)^2 - a_0^2 - a_1^2 + \alpha^{1/7} a_2^2 \\ A_2 = (a_0 + a_2)^2 - a_0^2 - a_2^2 + a_1^2 \end{cases}$$

The computation of the square costs $6c + 12a$.

3.2 Cyclotomic inversion

Let $a \in F_{q^{21}}$ as defined in the sub section 3.1.1, in the cyclotomic subgroup $G_{\phi_3(q^7)}$. Then, a satisfies $a^{q^{14}+q^7+1} = 1$ and so, $a^{-1} = a^{q^{14}+q^7} = a^{q^{14}} \cdot a^{q^7}$. To compute the cyclotomic inversion in $F_{q^{21}}$, just determine the two factors and make their product. For that, we need to know the value of $v^{q^7} = v^{3\cdot\frac{q^7-1}{3}+1} = \left(v^3\right)^{\cdot\frac{q^7-1}{3}} v = \left(\alpha^{\frac{1}{7}}\right)^{\cdot\frac{q^7-1}{3}} v$.

Set $\beta = \left(\alpha^{\frac{1}{7}}\right)^{\cdot\frac{q^7-1}{3}}$. We have $\beta \neq 1$ and $\beta^3 = 1$. Therefore β is a cubic primitive root of unity in F_{q^7}. We obtain $v^{q^7} = \beta v$. If necessary, the value of $v^{q^{14}}$ is obtained as follows:

$$v^{q^{14}} = \left(v^{q^7}\right)^{q^7} = (\beta v)^{q^7} = \beta^{q^7} v^{q^7} = \beta\beta v = \beta^2 v$$

$$\begin{aligned} a^{q^7} &= \left(a_0 + a_1 v + a_2 v^2\right)^{q^7} = a_0^{q^7} + a_1^{q^7} v^{q^7} + a_2^{q^7}\left(v^2\right)^{q^7} \\ &= a_0 + a_1 v^{q^7} + a_2\left(v^{q^7}\right)^2 = a_0 + a_1\beta v + a_2(\beta v)^2 \\ &= a_0 + a_1\beta v + a_2\beta^2 v^2 \end{aligned}$$

$$\begin{aligned} a^{q^{14}} &= \left(a^{q^7}\right)^{q^7} = \left(a_0 + a_1\beta v + a_2\beta^2 v^2\right)^{q^7} \\ &= a_0^{q^7} + a_1^{q^7}\beta^{q^7} v^{q^7} + a_2^{q^7}\left(\beta^2\right)^{q^7}\left(v^2\right)^{q^7} \\ &= a_0 + a_1\beta(\beta v) + a_2\beta^2(\beta v)^2 = a_0 + a_1\beta^2 v + a_2\beta^4 (v)^2 \\ &= a_0 + a_1\beta^2 v + a_2\beta v^2 \end{aligned}$$

$$\begin{aligned} a^{q^{14}} \cdot a^{q^7} &= \left(a_0 + a_1\beta^2 v + a_2\beta v^2\right)\left(a_0 + a_1\beta v + a_2\beta^2 v^2\right) \\ &= a_0^2 + a_0 a_1\beta v + a_0 a_2\beta^2 v^2 + a_0 a_1\beta^2 v + a_1^2\beta^3 v^2 \\ &\quad + a_1 a_2\beta^4 v^3 + a_0 a_2\beta v^2 + a_1 a_2\beta^2 v^3 + a_2^2\beta^3 v^4 \\ &= a_0^2 + \left(\beta + \beta^2\right)a_0 a_1 v + \left(\beta + \beta^2\right)a_0 a_2 v^2 + a_1^2 v^2 \\ &\quad + \left(\beta + \beta^2\right)a_1 a_2 v^3 + a_2^2 v^4 \end{aligned}$$

because $\beta^3 = 1$

$$a^{q^{14}} \cdot a^{q^7} = \left(a_0^2 - u a_1 a_2\right) + \left(u a_2^2 - a_0 a_1\right)v + \left(a_1^2 - a_0 a_2\right)v^2$$

because $v^3 = u$ and $1 + \beta + \beta^2 = 0$

$$a^{q^{14}} \cdot a^{q^7} = \left(a_0^2 - \alpha^{\frac{1}{7}} a_1 a_2\right) + \left(\alpha^{\frac{1}{7}} a_2^2 - a_0 a_1\right)v + \left(a_1^2 - a_0 a_2\right)v^2$$

The computation of cyclotomic inversion costs $3c + 3a + 3m$ in F_{q^7} .

3.3 Computation of Frobenius operators

The q^i Frobenius is the application

$\pi^i : F_{q^{21}} \to F_{q^{21}},\ a \mapsto a^{q^i}$.

Set $a = a_0 + a_1 v + a_2 v^2 \in F_{q^{21}}$ with $a_0, a_1, a_2 \in F_{q^7}$.

$\pi(a) = a^q = a_0^q + a_1^q v^q + a_2^q\left(v^2\right)^q$.

$a_0 \in F_{q^7} \Rightarrow a_0 = g_0 + g_1 u + g_2 u^2 + g_3 u^3 + g_4 u^4 + g_5 u^5 + g_6 u^6$;

$g_i \in F_q;\ i \in \{0,1,\cdots,6\}$.

Then, we obtain:

$$\begin{aligned} a_0^q &= g_0^q + g_1^q u^q + g_2^q\left(u^2\right)^q + g_3^q\left(u^3\right)^q + g_4^q\left(u^4\right)^q \\ &\quad + g_5^q\left(u^5\right)^q + g_6^q\left(u^6\right)^q \\ &= g_0 + g_1 u^q + g_2\left(u^2\right)^q + g_3\left(u^3\right)^q + g_4\left(u^4\right)^q \\ &\quad + g_5\left(u^5\right)^q + g_6\left(u^6\right)^q \end{aligned}$$

because $g_i^q = g_i \quad \forall i \in \{0,1,\cdots,6\}$

$u^q = u^{3\cdot\frac{q-1}{3}+1} = \left(u^3\right)^{\frac{q-1}{3}} u$. Set $\beta = \left(u^3\right)^{\frac{q-1}{3}}$

We have $\beta = \left(u^3\right)^{\frac{q-1}{3}} \neq 1$ and $\beta^3 = \left(u^3\right)^{q-1} = 1$. Which means that β is a primitive cubic root of unity in F_q and $u^q = \beta u$.

$$\begin{aligned} a_0^q &= g_0 + g_1 u^q + g_2\left(u^2\right)^q + g_3\left(u^3\right)^q + g_4\left(u^4\right)^q + g_5\left(u^5\right)^q \\ &\quad + g_6\left(u^6\right)^q \\ &= g_0 + g_1\beta u + g_2\beta^2u^2 + g_3u^3 + g_4\beta u^4 + g_5\beta^2u^5 + g_6u^6 \end{aligned}$$

Set

$a_1 = h_0 + h_1u + h_2u^2 + h_3u^3 + h_4u^4 + h_5u^5 + h_6u^6;$
$h_i \in F_q;\ i \in \{0, 1, \cdots, 6\}$ and

$a_2 = l_0 + l_1u + l_2u^2 + l_3u^3 + l_4u^4 + l_5u^5 + l_6u^6;$
$l_i \in F_q;\ i \in \{0, 1, \cdots, 6\}$

Similarly, we find:

$$a_1^q = h_0 + h_1\beta u + h_2\beta^2u^2 + h_3u^3 + h_4\beta u^4 + h_5\beta^2u^5 + h_6u^6$$
$$a_2^q = l_0 + l_1\beta u + l_2\beta^2u^2 + l_3u^3 + l_4\beta u^4 + l_5\beta^2u^5 + l_6u^6$$

$v^q = v^{3\cdot\frac{q-1}{3}+1} = \left(v^3\right)^{\frac{q-1}{3}} v = u^{\frac{q-1}{3}} v = \theta v$ with $\theta = u^{\frac{q-1}{3}}$. We have $\theta \neq 1$ and $\theta^3 = 1$. Then θ is a primitive cubic root of unity in F_q and $v^q = \theta v$.

$$\begin{aligned} a^q &= \left(a_0 + a_1v + a_2v^2\right)^q = a_0^q + a_1^q v^q + a_0^q\left(v^q\right)^2 \\ &= g_0 + g_1\beta u + g_2\beta^2u^2 + g_3u^3 + g_4\beta u^4 + g_5\beta^2u^5 + g_6u^6 \\ &\quad + \left(h_0 + h_1\beta u + h_2\beta^2u^2 + h_3u^3 + h_4\beta u^4 + h_5\beta^2u^5 + h_6u^6\right)\theta v \\ &\quad + \left(l_0 + l_1\beta u + l_2\beta^2u^2 + l_3u^3 + l_4\beta u^4 + l_5\beta^2u^5 + l_6u^6\right)\theta^2v^2 \end{aligned}$$

$$\begin{aligned} a^q &= g_0 + g_1\beta u + g_2\beta^2u^2 + g_3u^3 + g_4\beta u^4 + g_5\beta^2u^5 + g_6u^6 \\ &\quad + \left(h_0\theta + h_1\theta\beta u + h_2\theta\beta^2u^2 + h_3\theta u^3 + h_4\theta\beta u^4 + h_5\theta\beta^2u^5 \right. \\ &\quad \left. + h_6\theta u^6\right)v + \left(l_0\theta^2 + l_1\theta^2\beta u + l_2\theta^2\beta^2u^2 + l_3\theta^2u^3 \right. \\ &\quad \left. + l_4\theta^2\beta u^4 + l_5\theta^2\beta^2u^5 + l_6\theta^2u^6\right)v^2 \end{aligned}$$

We can compute the existing products first $\beta^i\theta^j$ in the expression of a^q. Set

$b_0 = \beta^2; \quad b_1 = \theta\beta; \quad b_2 = \theta\beta^2 = b_0\theta; \quad b_3 = \theta^2;$

$b_4 = \theta^2\beta = \beta b_3; \quad b_5 = \theta^2\beta^2 = b_0b_3.$

What costs *2c + 4m*.

Putting these values in the place of their corresponding in a^q, we obtain:

$$\begin{aligned} a^q &= g_0 + g_1\beta u + g_2\beta^2u^2 + g_3u^3 + g_4\beta u^4 + g_5\beta^2u^5 + g_6u^6 \\ &\quad + \left(h_0\theta + h_1b_1u + h_2b_2u^2 + h_3\theta u^3 + h_4b_1u^4 + h_5b_2u^5 + h_6\theta u^6\right)v \\ &\quad + \left(l_0b_3 + l_1b_4u + l_2b_5u^2 + l_3b_3u^3 + l_4b_4u^4 + l_5b_5u^5 + l_6b_3u^6\right)v^2 \end{aligned}$$

The computation of q-Frobenius costs $(4 + 7 \times 2)m + 3 \times 6a$. Adding the previous cost, we have *18m + 18a + 2c + 4m*.

That is a total cost of *22m + 18a + 2c* in F_q.

We have the same cost for q^2, q^3, q^4, q^5, q^6, q^8, q^9, q^{10}, q^{11}, q^{12}, q^{13}-Frobenius.

For the operator q^7-Frobenius, the subsection 3.1.2 gives us $v^{q^7} = \beta v$ Thus

$$\begin{aligned} a^{q^7} &= a_0^{q^7} + a_1^{q^7} v^{q^7} + a_2^{q^7}\left(v^2\right)^{q^7} = a_0 + a_1\beta v + a_2\beta^2v^2 \\ &= g_0 + g_1u + g_2u^2 + g_3u^3 + g_4u^4 + g_5u^5 + g_6u^6 \\ &\quad + \left(h_0 + h_1u + h_2u^2 + h_3u^3 + h_4u^4 + h_5u^5 + h_6u^6\right)\beta v \\ &\quad + \left(l_0 + l_1u + l_2u^2 + l_3u^3 + l_4u^4 + l_5u^5 + l_6u^6\right)\beta^2v^2 \end{aligned}$$

because $g_i^{q^7} = g_i$, $h_i^{q^7} = h_i$ and $l_i^{q^7} = l_i$.

$$\begin{aligned} a^{q^7} &= a_0^{q^7} + a_1^{q^7} v^{q^7} + a_2^{q^7}\left(v^2\right)^{q^7} = a_0 + a_1\beta v + a_2\beta^2v^2 \\ &= g_0 + g_1u + g_2u^2 + g_3u^3 + g_4u^4 + g_5u^5 + g_6u^6 \\ &\quad + \left(h_0\beta + h_1\beta u + h_2\beta u^2 + h_3\beta u^3 + h_4\beta u^4 + h_5\beta u^5 + h_6\beta u^6\right)v \\ &\quad + \left(l_0c + l_1cu + l_2cu^2 + l_3cu^3 + l_4cu^4 + l_5cu^5 + l_6cu^6\right)v^2 \end{aligned}$$

with $c = \beta^2$

We have *14m + 18a + 1c* in F_q as a cost for computing the q^7-Frobenius. We have the same cost for q^{14}-Frobenius.

Lemma 3.1. In the finite field $F_{q^{21}}$,

i) The computation of q^7; q^{14}-Frobenius costs *14m + 18a + 1c;*
ii) The computation of morphisms q, q^2, q^3, q^4, q^5, q^6, q^8, q^9, q^{10}, q^{11}, q^{12}, q^{13}-Frobenius costs *22m + 18a + 2c;*
iii) The inverse of α, an element of the cyclotomic subgroup $G_{\phi_3(q^7)}$ is computed as $\alpha^{-1} = \alpha^{q^7} \times \alpha^{q^{14}}$ and costs 3c+3a+3m in F_{q^7}.

4. Elliptic Curves with an embedding degree 21

This section describes the computation of the optimal Ate pairing (Miller's step and the final exponentiation) on the elliptic curves parameterized in [17].

This family of elliptic curves has the embedding degree 21, and is parameterized by:

$$q = \frac{1}{3}\left(x^{16} - 2x^{15} + x^{14} + x^9 - 2x^8 + x^7 + x^2 + x + 1\right)$$

$$r = x^{12} - x^{11} + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1$$

$$t = x + 1$$

4.1 Optimal Ate pairing

The Vercauteren approach describes in [13] allows us to get the short vectors from the *L* lattice defined by the equation:

$e_0 : G_2 \times G_1 \to \mu_r$

$$(Q,P) \mapsto \left(\prod_{i=0}^{l} f_{c_i,Q}^{q^i}(P) \cdot \prod_{i=0}^{l-1} h_{[s_{i+1}]Q,[c_i q^i]Q}(P) \right)^{\frac{q^k-1}{r}} \qquad (1)$$

which gave the optimal function $h(z) = \sum_{i=0}^{l} c_i z^i = x - z \in Z[z]$.

A direct application of the formula (1) yields the optimal pairing:

$e_0 : G_2 \times G_1 \to \mu_r$

$$(Q,P) \mapsto f_{x,Q}(P)^{\frac{q^{21}-1}{r}}$$

4.2 Determination of the cost of the execution of the Miller loop

In this subsection, we consider the Miller function given in affine coordinates, following the analysis of Montgomery, Lauter & Naehrig [18] who suggested using affine coordinates at the highest level of security. The Miller function used for computing $f_{x,Q}(P)$ in this case is described in [19]. At a 192-bit security level on elliptic curves with k = 21, the best x value we could find with a SAGE (SageMath) code is:
$x = 2^{36} + 2^{35} + 2^{34} + 2^{31} + 2^{30} + 2^{28} + 2^{27} + 2^{25} + 2^{24} + 2^{22} + 2^{20} + 2^{18} + 2^{17} + 2^{16} + 2^{14} + 2^{12} + 2^{9} + 2^{8} + 2^{4} + 2^{3} + 1$.
This value gives a *r(x)* prime of 443 bits and *q(x)* of 589 bits that match the 192-bit security level setting according to Table 1. The value of q is congruent to 1 modulo 6, as is the value of x so the corresponding elliptic curve is $y^2 = x^3 + 1$ [20]. The Miller loop here consists of computing $f_{x,Q}$ which costs 36 dubbing steps, 20 additions, 35 squares and 55 multiplications in $F_{q^{21}}$. To our knowledge no explicit cost exists in the literature for the k = 21 with a specific value of x.

4.3 Estimation of the cost of computing the final exponentiation

As explained in the subsection 2.3, the final exponentiation can be divided as $f^{\frac{q^{21}-1}{r}} = \left(f^{q^7-1}\right)^{\frac{q^{14}+q^7+1}{r}} = \left(f^{q^7-1}\right)^{d}$.

The lattice method that we briefly described in the 2.3 sub-section applied to the matrix

$$M = \begin{pmatrix} 3d(x) \\ 3xd(x) \\ 3x^2 d(x) \\ 3x^3 d(x) \\ 3x^4 d(x) \\ 3x^5 d(x) \\ 3x^6 d(x) \\ 3x^7 d(x) \\ 3x^8 d(x) \\ 3x^9 d(x) \\ 3x^{10} d(x) \\ 3x^{11} d(x) \end{pmatrix}$$

allows us to get the next multiple of d (see Appendix for more details):

$$d' = 3x^3 d(x) = \gamma_0 + \gamma_1 q + \gamma_2 q^2 + \gamma_3 q^3 + \gamma_4 q^4 + \gamma_5 q^5 + \gamma_6 q^6$$
$$+ \gamma_7 q^7 + \gamma_8 q^8 + \gamma_9 q^9 + \gamma_{10} q^{10} + \gamma_{11} q^{11} + \gamma_{12} q^{12} + \gamma_{13} q^{13}$$

where the polynomials γ_i i = 0; : : : ; 13 are defined as follows

$\gamma_0 = -x^6 + x^5 + x^3 - x^2;$ $\quad \gamma_1 = -x^5 + x^4 + x^2 - x;$

$\gamma_2 = -x^4 + x^3 + x - 1;$

$\gamma_3 = x^{15} - 2x^{14} + x^{13} + x^8 - 2x^7 + x^6 - x^3 + x^2 + x + 2;$

$\gamma_4 = x^{15} - x^{14} - x^{13} + x^{12} + x^8 - x^7 - x^6 + x^5 - x^2 + 2x + 2;$

$\gamma_5 = x^{15} - x^{14} - x^{12} + x^{11} + x^8 - x^7 - x^5 + x^4 + 3;$

$\gamma_6 = x^{14} - x^{13} - x^{11} + x^{10} + x^7 - x^6 - x^4 + x^3;$

$\gamma_7 = x^{13} - x^{12} - x^{10} + x^9;$

$\gamma_8 = x^{12} - x^{11} - x^9 + x^8;$ $\quad \gamma_9 = x^{11} - x^{10} - x^8 + x^7;$

$\gamma_{10} = x^{10} - x^9 - x^7 + x^6;$ $\quad \gamma_{11} = x^9 - x^8 - x^6 + x^5;$

$\gamma_{12} = x^8 - x^7 - x^5 + x^4;$ $\quad \gamma_{13} = x^7 - x^6 - x^4 + x^3.$

These polynomials verify the following relationships:

$\gamma_2 = -(x-1)(x^3 - 1) = -(x-1)^2 (x^2 + x + 1);$

$\gamma_1 = x\gamma_2;$ $\quad \gamma_0 = x^2\gamma_2 = x\gamma_1;$ $\quad \gamma_{13} = -x^3\gamma_2 = -x\gamma_0;$

$\gamma_{12} = -x^4\gamma_2 = x\gamma_{13};$ $\quad \gamma_{11} = -x^5\gamma_2 = x\gamma_{12};$

$\gamma_{10} = -x^6\gamma_2 = x\gamma_{11};$ $\quad \gamma_9 = -x^7\gamma_2 = x\gamma_{10};$

$\gamma_8 = -x^8\gamma_2 = x\gamma_9;$ $\quad \gamma_7 = -x^9\gamma_2 = x\gamma_8;$

$\gamma_6 = x\gamma_7 + \gamma_{13};$ $\quad \gamma_5 = x\gamma_6 + 3;$

$\gamma_4 = \gamma_5 - \gamma_7 + \gamma_8 - \gamma_{10} + \gamma_{11} - \gamma_{13} - \gamma_1 + \gamma_2;$

$\gamma_3 = \gamma_5 - \gamma_6 + \gamma_8 + \gamma_{11} - \gamma_{12} - \gamma_0 + \gamma_2.$

Computations of γ_3 and γ_4 can be simplified by using another intermediate polynomial $\gamma_{14} = \gamma_2 + \gamma_5 + \gamma_8 + \gamma_{11}$. Thus, we obtain: $\gamma_3 = \gamma_{14} - (\gamma_6 + \gamma_{12} + \gamma_0)$ and $\gamma_4 = \gamma_{14} - (\gamma_7 + \gamma_{10} + \gamma_{13} + \gamma_1)$.

Set $A = f^{q^7-1}$:

- The cost for computing A est 1 q^7-Frobenius, 1 inversion in $F_{q^{21}}$ and 1 multiplication in $F_{q^{21}}$.
- The cost for computing A^{γ_2} est: 1 inversion in the cyclotomic subgroup, 2 exponentiations by $(x-1)$ and 1 exponentiation by $(x^2 + x + 1)$.

- Computations of A^{γ_1}, A^{γ_0}, $A^{\gamma_{12}}$, $A^{\gamma_{11}}$, $A^{\gamma_{10}}$, A^{γ_9}, A^{γ_8} and A^{γ_7} each cost 1 exponentiation by *x*. In total, 8 exponentiations by *x*.
- The computation of $A^{\gamma_{13}}$ costs 1 exponentiation by *x* and 1 inversion in the cyclotomic subgroup.
- The cost for computing A^{γ_5} is: 2 multiplications, 1 squaring, and 1 exponentiation by *x*.
- The cost for computing A^{γ_6} is: 1 exponentiation by *x* and 1 multiplication.
- The computation of $A^{\gamma_{14}}$ costs 3 multiplications.
- The computation of A^{γ_3} costs 3 multiplications and 1 inversion in the cyclotomic subgroup.
- And finally the computation of A^{γ_4} cost 4 multiplications and 1 inversion in the cyclotomic subgroup.

As said in 3.1.2 the cyclotomic inversion is computed as $A^{-1} = A^{q^{14}} \cdot A^{q^7}$. The cost of the difficult part $A^{d'}$ is then 26 multiplications in $F_{q^{21}}$, 11 exponentiations by *x*, 1 exponentiation by $\left(x^2 + x + 1\right)$, 4 cyclotomic inversions , 2 exponentiations by $(x-1)$, 1 squaring and q , q^2, q^3, q^4, q^5, q^6, $2 \times q^7$, q^8, q^9, q^{10}, q^{11}, q^{12}, q^{13}-Frobenius maps.

5. Conclusion

In this paper, we have provided details on the computation of the Miller loop and the final exponentiation for the optimal pairing on the elliptic curves of BLS with an embedding degree 21. An explicit cost estimate is given for the Miller loop. It would be interesting to look at their behavior against small-subgroup attacks and security of subgroups.

References

[1] Emanuel Fouotsa, Nadia El Mrabet, Aminatou Pecha. “Optimal Ate Pairing on Elliptic Curves with Embedding Degree 9, 15 and 27”, 2016. https://pdfs.semanticscholar.org/becb/5303543239084ac4bc92af662e07eccba0c9.pdf

[2] Dan Boneh & 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, pp. 213–229, 2001.

[3] 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, pp. 360–363, 2001.

[4] Benoît Libert, Jean-Jacques Quisquater. “Identity based undeniable signatures”. In Topics in Cryptology – CTRSA 2004, The Cryptographers Track at the RSA Conference 2004, San Francisco, CA, USA, February 23-27, 2004, Proceedings, pp. 112–125, 2004.

[5] Ben Lynn Dan Boneh & Hovav Shacham. “Short signatures from the weil pairing”. In Advances in Cryptology - Asiacrypt 2001, volume 2248 of Lecture Notes in Computer Science, Springer, pp. 514–532, 2001.

[6] Amit Sahai, Vipul Goyal, Omkant Pandey & 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, october 30 - November 3, 2006, pp. 89–98, 2006.

[7] Victor S. Miller. “The weil pairing, and its efficient calculation”. J. Cryptology, 17(4), pp. 235–261, 2004.

[8] Paulo S. L. M. Barreto & 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, pp. 319–331, 2005.

[9] Michael Scott David Freeman & Edlyn Teske. “A taxonomy of pairing-friendly elliptic curves”. J. Cryptology, 23(2), pp. 224–280, 2010.

[10] H.W. Lenstra A.K. Lenstra & L. Lovász. “Factoring polynomials with rational coefficients”. Mathematische Annalen, Vol. 261, pp. 513–534, 1982.

[11] Nigel P. Smart Florian Hess & Frederik Vercauteren . “The eta pairing revisited”. IEEE Transactions on Information Theory, 52(10), pp. 4595–4602, 2006.

[12] C. Doche, G. Frey, T. Lange, K. Nguyen, R. Avanzi, H. Cohen & F. Vercauteren . “Handbook of elliptic and hyperelliptic curve cryptography”. Discrete Math. Aplli. Chapman and Hall, 2006.

[13] Frederik Vercauteren. “Optimal pairings”. IEEE Transactions on Information Theory, 56(1), pp. 455–461, 2010.

[14] Edward Knapp Laura Fuentes-Castañeda & Francisco Rodríguez-Henríquez. “Faster hashing to G_2”. In Selected Areas in Cryptography - 18th International Workshop, SAC 2011, Toronto, ON, Canada, August 11-12, 2011, Revised Selected Papers, pp. 412–430, 2011.

[15] Manuel Charlemagne, Luis J. Dominguez Perez, Michael Scott, Naomi Benger & Ezekiel J. Kachisa. “Fast hashing to G_2 on pairing-friendly curves”. In Pairing-Based Cryptography - Pairing 2009, Third International Conference, Palo Alto, CA, USA, August 12-14, 2009, Proceedings, pp. 102–113, 2009.

[16] Naomi Benger & Michael Scott. “Constructing tower extensions of finite fields for implementation of pairing-based cryptography”. Lecture Notes in computer Science book series (LNCS, volume 6087), pp. 180–195, 2010.

[17] Ben Lynn Paulo S. L. M. Barreto, Michael Scott. “Constructing elliptic curves with prescribed embedding degrees”. In Stelvio Cimato, Clemente Galdi, and Giuseppe Persiano, editors, SCN, 2576 of Lecture Notes in Computer Science, Springer, pp. 257–267, 2002.

[18] Peter L. Montgomery Kristin E. Lauter & 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, pp. 1–20, 2010.

[19] Xusheng Zhang & 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, pp. 412–430, 2012.

[20] Duc-Phong Le & 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, pp. 262–277, 2012.

Appendix

$$\begin{aligned}
d(x)= \frac{1}{3}(& (x^{15}-2x^{14}+x^{13}+x^{8}-2x^{7}+x^{6}-x^{3}+x^{2}+x+2) \\
&+(x^{15}-x^{14}-x^{13}+x^{12}+x^{8}-x^{7}-x^{6}+x^{5}-x_{2}+2x+2)q \\
&+(x^{15}-x^{14}-x^{12}+x^{11}+x^{8}-x^{7}-x^{5}+x^{4}+3)q^{2} \\
&+(x^{14}-x^{13}-x^{11}+x^{10}+x^{7}-x^{6}-x^{4}+x^{3})q^{3} \\
&+(x^{13}-x^{12}-x^{10}+x^{9}+x^{6}-x^{5}-x^{3}+x^{2})q^{4} \\
&+(x^{12}-x^{11}-x^{9}+x^{8}+x^{5}-x^{4}-x^{2}+x)q^{5} \\
&+(x^{11}-x^{10}-x^{8}+x^{7}+x^{4}-x^{3}-x+1)q^{6} \\
&+(x^{10}-x^{9}-x^{7}+x^{6})q^{7}+(x^{9}-x^{8}-x^{6}+x^{5})q^{8} \\
&+(x^{8}-x^{7}-x^{5}+x^{4})q^{9}+(x^{7}-x^{6}-x^{4}+x^{3})q^{10} \\
&+(x^{6}-x^{5}-x^{3}+x^{2})q^{11}+(x^{5}-x^{4}-x^{2}+x)q^{12} \\
&+(x^{4}-x^{3}-x+1)q^{13})
\end{aligned}$$

$$\begin{aligned}
xd(x)= \frac{1}{3}(& (-x^{4}+x^{3}+x-1)+(x^{15}-2x^{14}+x^{13}+x^{8}-2x^{7} \\
&+x^{6}-x^{3}+x^{2}+x+2)q \\
&+(x^{15}-x^{14}-x^{13}+x^{12}+x^{8}-x^{7}-x^{6}+x^{5}-x^{2}+2x+2)q^{2} \\
&+(x^{15}-x^{14}-x^{12}+x^{11}+x^{8}-x^{7}-x^{5}+x^{4}+3)q^{3} \\
&+(x^{14}-x^{13}-x^{11}+x^{10}+x^{7}-x^{6}-x^{4}+x^{3})q^{4} \\
&+(x^{13}-x^{12}-x^{10}+x^{9}+x^{6}-x^{5}-x^{3}+x^{2})q^{5} \\
&+(x^{12}-x^{11}-x^{9}+x^{8}+x^{5}-x^{4}-x^{2}+x)q^{6} \\
&+(x^{11}-x^{10}-x^{8}+x^{7})q^{7}+(x^{10}-x^{9}-x^{7}+x^{6})q^{8} \\
&+(x^{9}-x^{8}-x^{6}+x^{5})q^{9}+(x^{8}-x^{7}-x^{5}+x^{4})q^{10} \\
&+(x^{7}-x^{6}-x^{4}+x^{3})q^{11}+(x^{6}-x^{5}-x^{3}+x^{2})q^{12} \\
&+(x^{5}-x^{4}-x^{2}+x)q^{13})
\end{aligned}$$

$$\begin{aligned}
x^{2}d(x)= \frac{1}{3}(& (-x^{5}+x^{4}+x^{2}-x)+(-x^{4}+x^{3}+x-1)q \\
&+(x^{15}-2x^{14}+x^{13}+x^{8}-2x^{7}+x^{6}-x^{3}+x^{2}+x+2)q^{2} \\
&+(x^{15}-x^{14}-x^{13}+x^{12}+x^{8}-x^{7}-x^{6}+x^{5}-x^{2}+2x+2)q^{3} \\
&+(x^{15}-x^{14}-x^{12}+x^{11}+x^{8}-x^{7}-x^{5}+x^{4}+3)q^{4} \\
&+(x^{14}-x^{13}-x^{11}+x^{10}+x^{7}-x^{6}-x^{4}+x^{3})q^{5} \\
&+(x^{13}-x^{12}-x^{10}+x^{9}+x^{6}-x^{5}-x^{3}+x^{2})q^{6} \\
&+(x^{12}-x^{11}-x^{9}+x^{8})q^{7}+(x^{11}-x^{10}-x^{8}+x^{7})q^{8} \\
&+(x^{10}-x^{9}-x^{7}+x^{6})q^{9}+(x^{9}-x^{8}-x^{6}+x^{5})q^{10} \\
&+(x^{8}-x^{7}-x^{5}+x^{4})q^{11}+(x^{7}-x^{6}-x^{4}+x^{3})q^{12} \\
&+(x^{6}-x^{5}-x^{3}+x^{2})q^{13})
\end{aligned}$$

$$\begin{aligned}
x^{3}d(x)= \frac{1}{3}(& (-x^{6}+x^{5}+x^{3}-x^{2})+(-x^{5}+x^{4}+x^{2}-x)q \\
&+(-x^{4}+x^{3}+x-1)q^{2} \\
&+(x^{15}-2x^{14}+x^{13}+x^{8}-2x^{7}+x^{6}-x^{3}+x^{2}+x+2)q^{3} \\
&+(x^{15}-x^{14}-x^{13}+x^{12}+x^{8}-x^{7}-x^{6}+x^{5}-x^{2}+2x+2)q^{4} \\
&+(x^{15}-x^{14}-x^{12}+x^{11}+x^{8}-x^{7}-x^{5}+x^{4}+3)q^{5} \\
&+(x^{14}-x^{13}-x^{11}+x^{10}+x^{7}-x^{6}-x^{4}+x^{3})q^{6} \\
&+(x^{13}-x^{12}-x^{10}+x^{9})q^{7}+(x^{12}-x^{11}-x^{9}+x^{8})q^{8} \\
&+(x^{11}-x^{10}-x^{8}+x^{7})q^{9}+(x^{10}-x^{9}-x^{7}+x^{6})q^{10} \\
&+(x^{9}-x^{8}-x^{6}+x^{5})q^{11}+(x^{8}-x^{7}-x^{5}+x^{4})q^{12} \\
&+(x^{7}-x^{6}-x^{4}+x^{3})q^{13})
\end{aligned}$$

$$\begin{aligned}
x^{4}d(x)= \frac{1}{3}(& (-x^{7}+x^{6}+x^{4}-x^{3})+(-x^{6}+x^{5}+x^{3}-x^{2})q \\
&+(-x^{5}+x^{4}+x^{2}-x)q^{2}+(-x^{4}+x^{3}+x-1)q^{3} \\
&+(x^{15}-2x^{14}+x^{13}+x^{8}-2x^{7}+x^{6}-x^{3}+x^{2}+x+2)q^{4} \\
&+(x^{15}-x^{14}-x^{13}+x^{12}+x^{8}-x^{7}-x^{6}+x^{5}-x^{2}+2x+2)q^{5} \\
&+(x^{15}-x^{14}-x^{12}+x^{11}+x^{8}-x^{7}-x^{5}+x^{4}+3)q^{6} \\
&+(x^{14}-x^{13}-x^{11}+x^{10})q^{7}+(x^{13}-x^{12}-x^{10}+x^{9})q^{8} \\
&+(x^{12}-x^{11}-x^{9}+x^{8})q^{9}+(x^{11}-x^{10}-x^{8}+x^{7})q^{10} \\
&+(x^{10}-x^{9}-x^{7}+x^{6})q^{11}+(x^{9}-x^{8}-x^{6}+x^{5})q^{12} \\
&+(x^{8}-x^{7}-x^{5}+x^{4})q^{13})
\end{aligned}$$

$$\begin{aligned}
x^{5}d(x)= \frac{1}{3}(& (-x^{8}+x^{7}+x^{5}-x^{4})+(-x^{7}+x^{6}+x^{4}-x^{3})q \\
&+(-x^{6}+x^{5}+x^{3}-x^{2})q^{2}+(-x^{5}+x^{4}+x^{2}-x)q^{3} \\
&+(-x^{4}+x^{3}+x-1)q^{4} \\
&+(x^{15}-2x^{14}+x^{13}+x^{8}-2x^{7}+x^{6}-x^{3}+x^{2}+x+2)q^{5} \\
&+(x^{15}-x^{14}-x^{13}+x^{12}+x^{8}-x^{7}-x^{6}+x^{5}-x^{2}+2x+2)q^{6} \\
&+(x^{15}-x^{14}-x^{12}+x^{11}+3)q^{7}+(x^{14}-x^{13}-x^{11}+x^{10})q^{8} \\
&+(x^{13}-x^{12}-x^{10}+x^{9})q^{9}+(x^{12}-x^{11}-x^{9}+x^{8})q^{10} \\
&+(x^{11}-x^{10}-x^{8}+x^{7})q^{11}+(x^{10}-x^{9}-x^{7}+x^{6})q^{12} \\
&+(x^{9}-x^{8}-x^{6}+x^{5})q^{13})
\end{aligned}$$

$$\begin{aligned}
x^{6}d(x)= \frac{1}{3}(& (-x^{9}+x^{8}+x^{6}-x^{5})+(-x^{8}+x^{7}+x^{5}-x^{4})q \\
&+(-x^{7}+x^{6}+x^{4}-x^{3})q^{2}+(-x^{6}+x^{5}+x^{3}-x^{2})q^{3} \\
&+(-x^{5}+x^{4}+x^{2}-x)q^{4}+(-x^{4}+x^{3}+x-1)q^{5} \\
&+(x^{15}-2x^{14}+x^{13}+x^{8}-2x^{7}+x^{6}-x^{3}+x^{2}+x+2)q^{6} \\
&+(x^{15}-x^{14}-x^{13}+x^{12}-x^{9}+2x^{8}-x^{7}-x^{2}+2x+2)q^{7} \\
&+(x^{15}-x^{14}-x^{12}+x^{11}+3)q^{8}+(x^{14}-x^{13}-x^{11}+x^{10})q^{9} \\
&+(x^{13}-x^{12}-x^{10}+x^{9})q^{10}+(x^{12}-x^{11}-x^{9}+x^{8})q^{11} \\
&+(x^{11}-x^{10}-x^{8}+x^{7})q^{12}+(x^{10}-x^{9}-x^{7}+x^{6})q^{13})
\end{aligned}$$

$$\begin{aligned}
x^7 d(x) &= \frac{1}{3}((-x^{10}+x^9+x^7-x^6)+(-x^9+x^8+x^6-x^5)q \\
&+(-x^8+x^7+x^5-x^4)q^2+(-x^7+x^6+x^4-x^3)q^3 \\
&+(-x^6+x^5+x^3-x^2)q^4+(-x^5+x^4+x^2-x)q^5 \\
&+(-x^4+x^3+x-1)q^6 \\
&+(x^{15}-2x^{14}+x^{13}-x^{10}+x^9+x^8-x^7-x^3+x^2+x+2)q^7 \\
&+(x^{15}-x^{14}-x^{13}+x^{12}-x^9+2x^8-x^7-x^2+2x+2)q^8 \\
&+(x^{15}-x^{14}-x^{12}+x^{11}+3)q^9+(x^{14}-x^{13}-x^{11}+x^{10})q^{10} \\
&+(x^{13}-x^{12}-x^{10}+x^9)q^{11}+(x^{12}-x^{11}-x^9+x^8)q^{12} \\
&+(x^{11}-x^{10}-x^8+x^7)q^{13})
\end{aligned}$$

$$\begin{aligned}
x^8 d(x) &= \frac{1}{3}((-x^{11}+x^{10}+x^8-x^7)+(-x^{10}+x^9+x^7-x^6)q \\
&+(-x^9+x^8+x^6-x^5)q^2+(-x^8+x^7+x^5-x^4)q^3 \\
&+(-x^7+x^6+x^4-x^3)q^4+(-x^6+x^5+x^3-x^2)q^5 \\
&+(-x^5+x^4+x^2-x)q^6 \\
&+(.x^{11}+x^{10}+x^8-x^7-x^4+x^3+x-1)q^7 \\
&+(x^{15}-2x^{14}+x^{13}-x^{10}+x^9+x^8-x^7-x^3+x^2+x+2)q^8 \\
&+(x^{15}-x^{14}-x^{13}+x^{12}-x^9+2x^8-x^7-x^2+2x+2)q^9 \\
&+(x^{15}-x^{14}-x^{12}+x^{11}+3)q^{10}+(x^{14}-x^{13}-x^{11}+x^{10})q^{11} \\
&+(x^{13}-x^{12}-x^{10}+x^9)q^{12}+(x^{12}-x^{11}-x^9+x^8)q^{13})
\end{aligned}$$

$$\begin{aligned}
x^9 d(x) &= \frac{1}{3}((-x^{12}+x^{11}+x^9-x^8)+(-x^{11}+x^{10}+x^8-x^7)q \\
&+(-x^{10}+x^9+x^7-x^6)q^2+(-x^9+x^8+x^6-x^5)q^3 \\
&+(-x^8+x^7+x^5-x^4)q^4+(-x^7+x^6+x^4-x^3)q^5 \\
&+(-x^6+x^5+x^3-x^2)q^6 \\
&+(-x^{12}+x^{11}+x^9-x^8-x^5+x^4+x^2-x)q^7 \\
&+(-x^{11}+x^{10}+x^8-x^7-x^4+x^3+x-1)q^8 \\
&+(x^{15}-2x^{14}+x^{13}-x^{10}+x^9+x^8-x^7-x^3+x^2+x+2)q^9 \\
&+(x^{15}-x^{14}-x^{13}+x^{12}-x^9+2x^8-x^7-x^2+2x+2)q^{10} \\
&+(x^{15}-x^{14}-x^{12}+x^{11}+3)q^{11}+(x^{14}-x^{13}-x^{11}+x^{10})q^{12} \\
&+(x^{13}-x^{12}-x^{10}+x^9)q^{13})
\end{aligned}$$

$$\begin{aligned}
x^{10} d(x) &= \frac{1}{3}((-x^{13}+x^{12}+x^{10}-x^9)+(-x^{12}+x^{11}+x^9-x^8)q \\
&+(-x^{11}+x^{10}+x^8-x^7)q^2+(-x^{10}+x^9+x^7-x^6)q^3 \\
&+(-x^9+x^8+x^6-x^5)q^4+(-x^8+x^7+x^5-x^4)q^5 \\
&+(-x^7+x^6+x^4-x^3)q^6 \\
&+(-x^{13}+x^{12}+x^{10}-x^9-x^6+x^5+x^3-x^2)q^7 \\
&+(-x^{12}+x^{11}+x^9-x^8-x^5+x^4+x^2-x)q^8 \\
&+(-x^{11}+x^{10}+x^8-x^7-x^4+x^3+x-1)q^9 \\
&+(x^{15}-2x^{14}+x^{13}-x^{10}+x^9+x^8-x^7-x^3+x^2+x+2)q^{10} \\
&+(x^{15}-x^{14}-x^{13}+x^{12}-x^9+2x^8-x^7-x^2+2x+2)q^{11} \\
&+(x^{15}-x^{14}-x^{12}+x^{11}+3)q^{12}+(x^{14}-x^{13}-x^{11}+x^{10})q^{13})
\end{aligned}$$

$$\begin{aligned}
x^{11} d(x) &= \frac{1}{3}((-x^{14}+x^{13}+x^{11}-x^{10})+(-x^{13}+x^{12}+x^{10}-x^9)q \\
&+(-x^{12}+x^{11}+x^9-x^8)q^2+(-x^{11}+x^{10}+x^8-x^7)q^3 \\
&+(-x^{10}+x^9+x^7-x^6)q^4+(-x^9+x^8+x^6-x^5)q^5 \\
&+(-x^8+x^7+x^5-x^4)q^6 \\
&+(-x^{14}+x^{13}+x^{11}-x^{10}-x^7+x^6+x^4-x^3)q^7 \\
&+(-x^{13}+x^{12}+x^{10}-x^9-x^6+x^5+x^3-x^2)q^8 \\
&+(-x^{12}+x^{11}+x^9-x^8-x^5+x^4+x^2-x)q^9 \\
&+(-x^{11}+x^{10}+x^8-x^7-x^4+x^3+x-1)q^{10} \\
&+(x^{15}-2x^{14}+x^{13}-x^{10}+x^9+x^8-x^7-x^3+x^2+x+2)q^{11} \\
&+(x^{15}-x^{14}-x^{13}+x^{12}-x^9+2x^8-x^7-x^2+2x+2)q^{12} \\
&+(x^{15}-x^{14}-x^{12}+x^{11}+3)q^{13})
\end{aligned}$$