Efficient Final Exponentiation via Cyclotomic Structure for Pairings over Families of Elliptic Curves

Daiki Hayashida[1], Kenichiro Hayasaka[1], and Tadanori Teruya[2]

[1] Mitsubishi Electric Corporation, Japan.
Hayashida.Daiki@df.mitsubishielectric.co.jp
Hayasaka.Kenichiro@bc.mitsubishielectric.co.jp
[2] National Institute of Advanced Industrial Science and Technology, Japan.
tadanori.teruya@aist.go.jp

Abstract. The final exponentiation, which is the exponentiation by a fixed large exponent, must be performed in the Tate and (optimal) Ate pairing computation to ensure output uniqueness, algorithmic correctness, and security for pairing-based cryptography. In this paper, we propose a new framework of efficient final exponentiation for pairings over families of elliptic curves. Our framework provides two methods: the first method supports families of elliptic curves with arbitrary embedding degrees, and the second method supports families with specific embedding degrees of providing even faster algorithms. Applying our framework to several Barreto–Lynn–Scott families, we obtain faster final exponentiation than the previous state-of-the-art constructions.

Keywords: Pairings · Final exponentiation · Cyclotomic polynomial · Family of elliptic curves · Barreto–Lynn–Scott family

1 Introduction

Pairing-based cryptography is the study area of cryptographic protocols based on pairings defined over elliptic curves, which enable the secure and efficient realization of components for useful information services, such as efficient digital signature in blockchain [11], elliptic curve direct anonymous attestation in trusted computing [37], identity-based encryption and key exchange in real-time applications [18]. Now, pairing-based cryptography is the major field of study.

It is crucial to choose a suitable elliptic curve and an appropriate algorithm for efficient cryptographic protocols based on pairings in practice because the computation of pairing is the bottleneck. Recently, several researchers proposed new recommendations of elliptic curves [29,24,17,6,7,19] and directions [30] based on the state-of-the-art cryptanalysis reports [22,34,23]. A survey of current status and security of elliptic curves is available at a draft [33]. The results of these studies narrowed the choice of appropriate elliptic curves down. However, the best choice is still hard. A careful look at listed up elliptic curves in the recommendations [29,24,17,6,7,19,33], elliptic curves generated by Barreto–Lynn–Scott

(BLS) families [8] are frequently selected to implement cryptographic protocols with 128 bit, 192 bit, and 256 bit levels of security. The BLS families could be considered to have some flexibility; therefore, elliptic curves generated by these families are likely to be chosen in the future, even if there is inevitable progress in the security assessment study. Hence, instead, focus on only one elliptic curve and make it faster, the design of efficient algorithms, which supports many promising elliptic curves, for example, elliptic curves generated by BLS families, would be highly desired.

There are two major types of pairing computation algorithms called Tate pairings and Weil pairings, and their efficient variants are called Ate pairings and Eil pairings, respectively [31,21,38,20]. For both major types, a generalized method to obtain efficient algorithms called pairing function is proposed [38,20]. In terms of the efficiency evaluation and high-speed implementation reports [10,3,4,36,1,39,24,17,28,6,7,19,13], optimal Ate pairings constructed by pairing functions based on the Ate pairings are significantly efficient. Thus we focus on efficient optimal Ate pairings in this paper. The optimal Ate pairing consists of two parts, which are called the Miller loop and final exponentiation. Hence, it is vital to construct efficient these algorithms for high-speed implementations of optimal Ate pairings.

The construction of an efficient Miller loop was not easy until around seven years ago. Today, significantly fast Miller loop computation can be easily implemented based on many studies and results [31,21,38,20,9,27,40,26,10,36,1,13] because existing methods can apply to new recommendations [29,24,6,7,19,33]. In particular, one can immediately obtain the computationally optimal Miller loop over an elliptic curve generated by the BLS family [8,24,17,6,7].

On the other hand, there are a few studies of efficient final exponentiation construction explained below.

Related Work. There are three existing approaches to construct efficient final exponentiation: the vectorial addition chain method [35], the lattice-based method [16], and another heuristic method exploiting the structure of pairings [40]. Since the lattice-based method can provide faster algorithms in the literature [16,7], here we briefly describe only this because it seems to be the state-of-the-art method. The idea of the lattice-based method is finding the expansion suitable for efficient pairing computation via lattice basis reduction. As mentioned in their paper [16], the lattice-based method often requires several trial-and-errors search and may not provide faster algorithms. A careful look at the efficiency evaluation report [7] concerning the state-of-the-art cryptanalysis [22,34,23], the lattice-based method [16] is not always used to construct faster algorithms. A heuristic approach [40] gives a few efficient algorithms. This situation naturally raises a question about the existence of a superior method, which can provide faster algorithms than the existing ones. Because the pairing itself might have the structure of efficient final exponentiation, but it is not well studied in prior work.

Our Contribution. In this paper, we address the above question and propose a new framework to obtain more efficient final exponentiation for pairings over families of elliptic curves. Our framework consists of the following two methods:

- The first method is the generalization of the method presented by Zhang and Lin [40]. We show a formal theorem that useful structure for efficient final exponentiation always underlies in the families of elliptic curves with arbitrary embedding degrees.
- The second method is an extension of the first method to obtain more efficient final exponentiation for specific embedding degrees of the forms $k = 2^i$, 3^j, and 2^i3^j for positive integers i and j. We also show formal theorems to visualize the underlying structure of the second method.

The first method is an algorithm that recursively derives the coefficients of the p-adic expansion of the hard part, similar to the three existing approaches to construct efficient final exponentiation. This is a natural generalization of the previous studies. On the other hand, the second method does not derive the coefficients but directly factorizes the hard part as a two-variable polynomial. The factorization can be obtained by using homogeneous cyclotomic polynomials (later) constructed from cyclotomic polynomials, becouse cyclotomic structure underlies in the polynomial parameters with families of elliptic curves.

Also, we compare with the existing approaches. We apply our framework to BLS families with embedding degrees 9, 12, 15, 24, 27, and 48. Then we obtain faster algorithms than the previous state-of-the-art algorithms presented in the literature [40,2,17,14,28]. As these experimental results, the improvements are modest, but it is confirmed that our framework can provide the fastest final exponentiation. Our results reduce the number of multiplication operations on the prime field in final exponentiation for BLS family with $k = 9, 12, 15, 24, 27$ and 48 by about *18.6%*, *6.1%*, *13.7%*, *9.7%*, *4.7%* and *14.8%* respectively. See the Table 1 and for details in Section 5.

	Previous work	This work
BLS-9 [14]	$I_9 + 1052M_1 + 10908S_1$	$I_9 + 856M_1 + 10872S_1$
BLS-12 [17]	$I_{12} + 1135M_1 + 28890S_1$	$I_{12} + 1066M_1 + 28890S_1$
BLS-15 [14]	$I_{15} + 3632M_1 + 28674S_1$	$I_{15} + 3133M_1 + 28647S_1$
BLS-24 [17]	$I_{24} + 5220M_1 + 69984S_1$	$I_{24} + 4716M_1 + 69984S_1$
BLS-27 [40]	$I_{27} + 19884M_1 + 115128S_1$	$I_{27} + 18916M_1 + 115128S_1$
BLS-48 [28]	$I_{48} + 36222M_1 + 264870S_1$	$I_{48} + 30849M_1 + 264384S_1$

Table 1: Complexity of final exponentiation on the various BLS families

Note that our framework does not always provide the fastest algorithm. However, our framework is useful in practice because our framework can support and accelerate many practical elliptic curves with efficiently computable pairings, for example, all the elliptic curves generated by BLS families. Recall that

these elliptic curves are frequently selected as new recommendations to achieve 128 bit, 192 bit, and 256 bit levels of security in the literature of security assessments [29,24,6,7,19,17]; thus, our framework is useful to implement secure and efficient pairing-based cryptography in practice.

Organization. In Section 2, we describe preliminaries, terminology, and notation of pairings. An overview of the final exponentiation and prior work for its efficient computations are described in Section 3. We show our main result: our framework, two methods, related theorems, and lemmata, in Section 4. In Section 5, we explain the application of our methods to BLS families and the comparison with the prior work. We conclude in Section 6.

2 Preliminaries

In this section, we briefly describe mathematical preliminaries, terminology, and notation of elliptic curves and pairings [13].

Elliptic Curves. Let E be an elliptic curve defined over a finite field $\mathbb{F}_p$ of field order $p > 3$. The rational points group of E over the m-th extension field $\mathbb{F}_{p^m}$ of $\mathbb{F}_p$ is denoted by $E(\mathbb{F}_{p^m})$, and its unit element is the point at infinity $\mathcal{O}$. The scalar multiplication by an integer a over E is denoted by $[a]$. A map $\pi_p : (x, y) \mapsto (x^p, y^p)$ is the Frobenius endomorphism over E. An integer $t = p + 1 - \#E(\mathbb{F}_p)$ is the trace of Frobenius. If E is ordinary, then the complex multiplication (CM) discriminant D is a square-free integer such that $DV^2 = 4p - t^2$, where V is an integer. Let r be another prime number such that $\gcd(p, r) = 1$, $r \mid \#E(\mathbb{F}_p)$, and $r^2 \nmid \#E(\mathbb{F}_p)$. The r-th torsion group of E is denoted by $E[r]$. We say that a positive integer k is the embedding degree with respect to r and p of E if k is the smallest positive integer satisfying $r \mid (p^k - 1)$. The r-th roots of unity over the multiplicative group $\mathbb{F}_{p^k}^{\times}$ of $\mathbb{F}_{p^k}$ is denoted by μ_r. As seen above, the main property of an elliptic curve can be specified by a quintuple of the above integers (k, D, p, r, t). (Usually, only focus on a triple (p, r, t).) Note that the CM method [5,32] can give a corresponding elliptic curve E such that $r \mid \#E(\mathbb{F}_p)$ from this quintuple.

Properties of Pairing. Let $\mathbb{G}_1 \coloneqq E[r] \cap \ker(\pi_p - [1])$, let $\mathbb{G}_2 \coloneqq E[r] \cap \ker(\pi_p - [p])$, and let $\mathbb{G}_{\mathrm{T}} \coloneqq \mu_r$. The pairing function is a function $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_{\mathrm{T}}$ (or $e : \mathbb{G}_2 \times \mathbb{G}_1 \to \mathbb{G}_{\mathrm{T}}$) satisfying the following three properties:

Bilinearity: For all $P \in \mathbb{G}_1$, for all $Q \in \mathbb{G}_2$, and for all $a \in \mathbb{Z}$, $e([a]P, Q) = e(P, [a]Q) = e(P, Q)^a$.
Non-degeneracy: $e(P, Q) = 1$ if and only if $P = \mathcal{O}$ or $Q = \mathcal{O}$.
Efficiency: The number of operations to compute the pairing is a polynomial in $\log r$.

Optimal Ate Pairing. Suppose an elliptic curve E holds the conditions described above. Let κ be an integer such that $\kappa = mr$ with $r \nmid m$, where m is an integer, and let $\nu = (c_0, c_1, \ldots, c_w)$ be a vector of $w+1$ integers such that $\kappa = \sum_{i=0}^{w} c_i p^i$. Then the following function a_ν with suitable conditions forms a pairing function based on the Ate pairing [38,20]:

$$a_\nu : \mathbb{G}_2 \times \mathbb{G}_1 \to \mathbb{G}_{\mathrm{T}},$$
$$(Q, P) \mapsto \left(\prod_{i=0}^{w} f_{c_i,Q}^{p^i}(P) \cdot \prod_{i=0}^{w-1} \frac{\ell_{[s_{i+1}]Q,[c_i p^i]Q}(P)}{v_{[s_i]Q}(P)} \right)^{\frac{p^k-1}{r}},$$

where $s_i \coloneqq \sum_{j=i}^{w} c_j p^j$, $\ell_{R,S}$ and v_R are the two normalized polynomial functions over E with the divisors $(R) + (S) + (-R-S) - 3(\mathcal{O})$ and $(R) + (-R) - 2(\mathcal{O})$, respectively, and $f_{a,R}$ is the Miller function (normalized rational function) over E with the divisor $a(R) - ([a]R) - (a-1)(\mathcal{O})$ [31]. Typically, the computation of products of the above functions f, ℓ, and v with input P and Q is called the Miller loop (also called the Miller's algorithm), and the remaining exponentiation by $(p^k - 1)/r$ is called the final exponentiation.

For above ν, define $\|\nu\|_1 = \sum_{i=0}^{w} |c_i|$. Miller showed the square-and-multiply algorithm that computes $f_{a,R}(S)$ in $O(\log a)$ times operations [31], and its singed-binary variants have been proposed [10,40,36]. Therefore, it is essential to find ν with very small $\|\nu\|_1$. According to the literature [38,20], any non-degenerate a_ν satisfies $\|\nu\|_1 \geq r^{1/\varphi(k)}$, where φ is the Euler's totient function. Roughly saying, a_ν is an optimal Ate pairing if $\|\nu\|_1$ is very close to $r^{1/\varphi(k)}$ [38].

Family of Elliptic Curves. As described above, elliptic curves with pairings suitable for cryptographic purposes must have specific properties that randomly chosen elliptic curves rarely have. Several researchers [15] have proposed methods of how to obtain appropriate quintuples satisfying the requirements. To resolve the search problem, a method of how to obtain appropriate quintuples has been proposed. The idea is the parameterization of three integers p, r, and t of a part of quintuple by polynomials over $\mathbb{Q}$ as $p(x)$, $r(x)$, and $t(x)$, respectively, that satisfy several conditions to direct where appropriate quintuples are. Then the search problem is transformed into the enumeration of integers of x, which provide appropriate quintuples. For example, find an integer z such that $p(z)$ and $r(z)$ are distinct large prime numbers simultaneously. This parameterized quintuple $(k, D, p(x), r(x), t(x))$ (or triple $(p(x), r(x), t(x))$) is called a family of elliptic curves. We say that an elliptic curve E is in the family $(k, D, p(x), r(x), t(x))$ (or $(p(x), r(x), t(x))$) if there exists an integer z such that E is defined over $\mathbb{F}_{p(z)}$ with trace of Frobenius $t(z)$. We refer the reader to a survey [15] for details.

The method of the family of elliptic curves also contributes to high-speed implementations. As described above, the Miller loop and final exponentiation are square-and-multiply algorithms, and their loop parameters are $\nu = (c_0, c_1, \ldots, c_w)$ and $(p^k - 1)/r$, respectively. Using the family of elliptic curves, they are also parameterized as $\nu(x) = (c_0(x), c_1(x), \ldots, c_w(x))$ and $(p(x)^k - 1)/r(x)$, respectively. In short, one can investigate and construct efficient

algorithms based on such polynomial representations. Eventually, the construction can be reduced to find integers which provide appropriate quintuples with efficiently computable pairings over corresponding elliptic curves. For example, the optimal Ate pairing of each elliptic curve generated by BLS families [8] can be written as $a_{\nu(x)}(Q,P) = (f_{x,Q}(P))^{(p(x)^k-1)/r(x)}$; thus, an appropriate integer of x with low Hamming weight yields an efficient Miller loop.

3 Overview of Final Exponentiation and Prior Work

In this section, we describe an overview of the final exponentiation and prior work for its efficient algorithms.

3.1 Basic Structure

The computation of pairings consists of two parts called the Miller loop and final exponentiation. After the computation of the Miller loop, obtain an element of $\mathbb{F}_{p^k}^{\times}/(\mathbb{F}_{p^k}^{\times})^r$. Then the final exponentiation, namely exponentiation by a fixed large exponent $(p^k-1)/r$, must be performed to obtain an element of $\mathbb{G}_{\mathrm{T}}$ of order r. This operation is also known as the cofactor clearing to ensure output uniqueness, algorithmic correctness, and security for pairing-based cryptography.

Let k be the embedding degree such that $k = ds$, where d is a positive integer. The fixed large exponent $(p^k-1)/r$ of final exponentiation can be broken down into two parts called the easy part and the hard part:

$$\frac{p^k-1}{r} = \underbrace{(p^s-1)\cdot\frac{\sum_{i=0}^{d-1}p^{is}}{\Phi_k(p)}}_{\text{Easy part}}\cdot\underbrace{\frac{\Phi_k(p)}{r}}_{\text{Hard part}},$$

where Φ_k is the k-th cyclotomic polynomial.

The easy part is usually products of sparse summations of powers of p, and its specific form depends on the embedding degree k. For example, the easy part can be decomposed by $(p^6-1)\cdot(p^2+1)$ if $k=12$, and it can be decomposed by $(p^5-1)\cdot(p^2+p+1)$ if $k=15$. The exponentiation of the easy part is almost free since there is only one inversion and the computation of exponentiation by a power of p over $\mathbb{F}_{p^k}$ is significantly efficient.

Remark 1. Note that there obviously exists another decomposition of the easy part. Indeed, we can also factorize $(p^5-1)\cdot(p^2+p+1) = (p^3-1)\cdot(p^4+p^3+p^2+p+1)$ if $k=15$, however, we should select $(p^5-1)\cdot(p^2+p+1)$ in practice from the viewpoint of the number of operations.

On the other hand, the hard part computation is usually expensive because it requires exponentiation by large exponents, not a power of p. The basic approach of efficient computation is base-p expansion. Let λ be an integer such that $\lambda = m\cdot\Phi_k(p)/r$ with $r \nmid m$, find a vector τ of $w+1$ integers $\tau = (\lambda_0, \lambda_1, \ldots, \lambda_w)$ such

that $\lambda = \sum_{i=0}^{w} \lambda_i p^i$ and very small $\|\tau\|_1$. The hard part is also parameterized as $m(x) \cdot \Phi_k(p(x))/r(x)$ by a family of elliptic curves. In this case, the construction of efficient hard part computation is finding suitable expansion based on $p(x)$ and x, and then also finding an appropriate integer z of x with low Hamming weight.

3.2 Prior Work of Hard Part Computation

There are three existing approaches to construct efficient final exponentiation: the vectorial addition chain method [35], the lattice-based method [16], and another heuristic method [40]. Several researchers [2,14,40,28] applied their methodology to several BLS families in the study of efficiency evaluation and high-speed implementation of pairings.

The vectorial addition chain method is used to efficiently compute a product $\prod_{i=0}^{w} g_i^{\lambda_i}$ for fixed exponents $\lambda_0, \lambda_1, \ldots, \lambda_w$ and input bases $g_0, g_1, \ldots, g_w$. The computation of hard part of the final exponentiation over family of elliptic curves can be translated into this setting, for example, consider an expansion $y^{\Phi_k(p(x))/r(x)} = \prod_{i=0}^{w} y^{\lambda_i(x)p(x)^i}$ by $p(x)$ and x as $g_{i+j\cdot\varphi(k)} \coloneqq y^{p(x)^i x^j}$. Scott et al. [35] reported that this method could provide fast algorithms.

Fuentes-Castañeda et al. [16] showed a method of finding more efficient algorithms. The idea is drawn from Vercauteren [38] that is the base-p expansion by lattice basis reduction employed to find an efficient Miller loop. The construction of the target basis of a lattice is different and complicated to adapt this method for expansion by $p(x)$ and x. Its advantage is that giving a hint to find an appropriate multiple of the exponent $m(x) \cdot \Phi_k(p(x))/r(x)$, which enables a faster algorithm. Fuentes-Castañeda et al. [16] reported that this method could provide faster algorithms. However, as mentioned in [16], this method often requires several trial-and-errors search, and may not provide a faster algorithm than that provided by the vectorial addition chain method [35]. A detailed numerical example is in a book [13] of the survey.

Zhang and Lin [40] pointed out that a recursive relation over the BLS family with embedding degree 27 (called BLS27) as follows: $p(x)^{m+1} = r(x) \cdot (x-1)^2 \cdot p(x)^m + x \cdot p(x)^m$, then the hard part of this family is expanded by $p(x)$ and x. The resulting formula can be efficiently computable because it is a product of summations of sparse terms. However, the background structure of such recursive relation is still unclear, and a question remains about how to exploit it to construct even faster algorithms than existing ones.

4 Main Result

In this section, we propose a new framework for efficient hard part computation of the final exponentiation. Intuitively, our framework utilizes the underlying structure of the cyclotomic polynomial that is substantially satisfied by families of elliptic curves with efficient pairing. Concretely, our framework provides two methods of obtaining suitable formulas of the exponent $\Phi_k(p(x))/r(x)$ of the

hard part computation via the underlying relationship of k, $p(x)$, $r(x)$, and others. The first method is a generalization of the previous method proposed by Zhang and Lin [40]. We show a theorem that there is a beneficial formula to obtain a faster algorithm in an arbitrary embedding degree. The second method is an extension of the first method to obtain an even faster algorithm for a specific embedding degree. We also show a theorem that there is a beneficial decomposition of the exponent $\Phi_k(p(x))/r(x)$ instead of the complete expansion by $p(x)$ and x considered in the prior work, and this decomposition approach is a significant difference from the previous methods.

We describe the first method, related theorem, and an algorithm in Section 4.1. Next, we introduce a new tool, called *homogeneous cyclotomic polynomials*, and describe its properties in Section 4.2. The purpose of this tool is visualizing the decomposition of $\Phi_k(p(x))/r(x)$ with specific embedding degree. Finally, we describe detailed explanations of our second method using homogeneous cyclotomic polynomials in Section 4.3. The application to BLS families and efficiency evaluation of our methods and comparisons with prior work are given in the next section.

Remark 2. Note that both methods cannot always provide faster algorithms than previous ones. According to explanations in this section later, applications and efficiency comparisons in the next section, our framework can provide faster algorithms if the trace of Frobenius is $t(x) = x + 1$. This limitation cannot be an issue in practice because the number of elliptic curves with efficient pairing and trace of Frobenius $t(x) = x + 1$ is somewhat large. For example, the trace of Frobenius of all the BLS families is $t(x) = x + 1$ (see Appendix A), and the recently published recommendations [29,24,17,6,7,19,33] frequently choose elliptic curves generated by the BLS families. Also, the applicability of our methods is not limited to BLS families.

4.1 Arbitrary Embedding Degree

We generalize the efficient hard part computation of the final exponentiation for optimal Ate pairings over families of elliptic curves.

Let $\Phi_k(x)$ denote the k-th cyclotomic polynomial and let E an elliptic curve with embedding degree k parametrized as families. Then the polynomial parameters $t(x)$, $r(x)$, $p(x)$ of E have the following representation:

$$\begin{cases} r(x) = \Phi_k(T(x))/h_2(x), \\ p(x) = h_1(x)r(x) + T(x), \\ t(x) = T(x) + 1, \end{cases} \tag{1}$$

where the polynomial $h_1(x) \in \mathbb{Q}[x]$ is the quotient of $p(x)$ divided by $r(x)$ and $h_2(x), T(x) \in \mathbb{Q}[x]$.

For $f \in \mathbb{F}_{p^k}$ computed in Miller loop, the value $f^{(p^k-1)/r}$ is computed in the final exponentiation of optimal Ate pairings. This power $(p^k - 1)/r$ can be decomposed by two parts $(p^k - 1)/\Phi_k(p)$ and $\Phi_k(p)/r$. The exponent $\Phi_k(p)/r$ can be decomposed as follows:

Theorem 1. *Set* $\Phi_k(x) = \sum_{i=0}^{d} c_i x^i \in \mathbb{Z}[x]$. *Then we claim that:*

$$\Phi_k(p(x))/r(x) = h_1(x)\left(\sum_{i=0}^{d-1} \lambda_i(x) p(x)^i\right) + h_2(x),$$

where:

$$\begin{cases} \lambda_{d-1}(x) = c_d, \\ \quad \lambda_i(x) = T(x)\lambda_{i+1}(x) + c_{i+1}. \end{cases}$$

See Appendix B.1 for the proof of Theorem 1.

4.2 Homogeneous Cyclotomic Polynomial

In this section, we first describe the definition and properties of cyclotomic polynomials, then give a new concept of homogeneous cyclotomic polynomials, and prove the lemma that can be used in the main theorems.

Let ζ_n denote a primitive n-th root of unity in $\mathbb{C}$. The n-th cyclotomic polynomial $\Phi_n(x)$ is

$$\Phi_n(x) = \prod_{\substack{1 \le i \le n \\ \gcd(i,n)=1}} (x - \zeta_n^i).$$

The cyclotomic polynomials are irreducible in $\mathbb{Q}$, and its degree can be represented by the Euler's totient function $\varphi(n)$. Also, it is well known that the cyclotomic polynomials have integer coefficients. When enumerating the cyclotomic polynomials from the smallest order n, we have

$$\Phi_1(x) = x - 1, \quad \Phi_2(x) = x + 1, \quad \Phi_3(x) = x^2 + x + 1, \quad \Phi_4(x) = x^2 + 1, \ldots$$

The basic equation for cyclotomic polynomials is that

$$x^m - 1 = \prod_{i|m} \Phi_i(x). \tag{2}$$

Definition 1. *For any positive integer* n, *we define an* n-th homogeneous cyclotomic polynomial $\Psi_n(x, p)$ *as:*

$$\Psi_n(x,p) := \begin{cases} p^{\varphi(n)}\Phi_n(x/p) & \text{if } n > 1, \\ 1 & \text{if } n = 1. \end{cases}$$

where φ *is the Euler's totient function.*

When enumerating the homogeneous cyclotomic polynomials from the smallest order n, we have

$$\Psi_1(x,p) = 1, \qquad \Psi_2(x,p) = x + p,$$
$$\Psi_3(x,p) = x^2 + px + p^2, \qquad \Psi_4(x,p) = x^2 + p^2, \ldots$$

The important properties of homogeneous cyclotomic polynomials is the following lemma.

Lemma 1. *Let $m \geq 2$. Then the polynomial $x^{m-1}+px^{m-2}+\cdots+p^{m-2}x+p^{m-1}$ can be decomposed by homogeneous cyclotomic polynomials, i.e. we have:*

$$\sum_{j=0}^{m-1} p^j x^{m-1-j} = \prod_{i|m} \Psi_i(x,p).$$

Proof. Dividing both sides of the equation (2) by $\Phi_1(x) = x - 1$, it leads:

$$x^{m-1} + x^{m-2} + \cdots + x^2 + x + 1 = \prod_{\substack{i|m \\ i\neq 1}} \Phi_i(x).$$

Substituting a variable x for x/p and multiplying both sides by p^{m-1}, we have the equation:

$$x^{m-1} + px^{m-2} + \cdots + p^{m-3}x^2 + p^{m-2}x + p^{m-1} = p^{m-1} \prod_{\substack{i|m \\ i\neq 1}} \Phi_i(x/p).$$

Here it holds that $\sum_{i|n} \varphi(i) = n$ for any $n \in \mathbb{Z}_{>0}$ from the basic property of the Euler's totient function. Hence we obtain that:

$$\begin{aligned} x^{m-1} + px^{m-2} + \cdots + p^{m-3}x^2 + p^{m-2}x + p^{m-1} &= \prod_{\substack{i|m \\ i\neq 1}} p^{\varphi(i)} \Phi_i(x/p) \\ &= \prod_{i|m} \Psi_i(x,p). \end{aligned}$$

Note that the first homogeneous cyclotomic polynomial $\Psi_1(x,p) = 1$ conveniently by Definition 1. □

4.3 Specific Embedding Degree

Let E be an elliptic curve defined over $\mathbb{F}_p$ with embedding degree k parametrized as families. In other words, each parameter p, r, t of the elliptic curve E can be expressed by polynomials, which satisfies the equation (1).

The hard part of the final exponentiation for optimal Ate pairings is computed as $f^{\Phi_k(p(x))/r(x)}$ for a value $f \in \mathbb{F}_{p^k}$. This exponentiation part $\Phi_k(p(x))/r(x)$ is decomposed by using homogeneous cyclotomic polynomials with $k = 2^i$, 3^j, and 2^i3^j. Prior works on the hard part focused on how to search the coefficients λ_i in $\Phi_k(p(x))/r(x) = \sum \lambda_i(x)p(x)^i$, however this time, it is essentially the same, we propose to decompose the hard part directly without searching the coefficients.

Theorem 2. *Let E be an elliptic curve with embedding degree $k = 2^n$ for some positive integer n parametrized as families. The hard part of the final exponentiation for the optimal Ate pairing defined over E can be decomposed as follows:*

$$\frac{\Phi_k(p)}{r} = h_1 \left(\prod_{i|(k/2)} \Psi_i(T,p) \right) + h_2,$$

where the notation h_1, h_2, T are the polynomials stated in the equation (1).

See Appendix B.2 for a proof of Theorem 2.

Theorem 3. *Let E be an elliptic curve with embedding degree $k = 3^n$ for some positive integer n parametrized as families. The hard part of the final exponentiation for the optimal Ate pairing defined over E can be decomposed as follows:*

$$\frac{\Phi_k(p)}{r} = h_1 \left(\prod_{i|(k/3)} \Psi_i(T,p) \right) (T^{k/3} + p^{k/3} + 1) + h_2,$$

where the notation h_1, h_2, T are the polynomials stated in the equation (1).

See Appendix B.3 for a proof of Theorem 3.

Theorem 4. *Let E be an elliptic curve with embedding degree $k = 2^m 3^n$ for some positive integers m and n parametrized as families. The hard part of the final exponentiation for the optimal Ate pairing defined over E can be decomposed as follows:*

$$\frac{\Phi_k(p)}{r} = h_1 \left(\prod_{i|(k/6)} \Psi_i(T,p) \right) (T^{k/6} + p^{k/6} - 1) + h_2,$$

where the notation h_1, h_2, T are the polynomials stated in the equation (1).

See Appendix B.4 for a proof of Theorem 4.

5 Application to BLS families

In this section, we apply the decomposition of final exponentiation for optimal Ate pairings obtained in Section 4 to various BLS families, estimate the number of operations in the finite field $\mathbb{F}_{p^k}$ and convert the cost to the number of operations in the prime field $\mathbb{F}_p$ for the cost of the multiplication and squaring in $\mathbb{F}_{p^k}$.

Let M_k, S_k, I_k, F_n, E_x denote the cost of the multiplication, squaring, inversion, n-th Frobenius operation and the power of x in $\mathbb{F}_{p^k}$ respectively. Let I_{cyc} denote the cost of the inversion in the cyclotomic subgroup $\mathbb{G}_{\Phi_k}$. We use the estimation $M_2 = 3M_1, M_3 = 6M_1$ and $M_5 = 9M_1$ (resp. $S_2 = 3S_1, S_3 = 6S_1$ and $S_5 = 9S_1$), as mentioned in [25,12]

Remark 3. It is assumed that there exists a more efficient extension operation taking the cost of addition into account. However, to evaluate the complexity equally, we ignore the cost of addition operation in common and use the above estimation. Also, the costs E_x and F_n depend on the parameters x and p when converting to the number of operations on the prime field. However, for the same reason, we evaluate the cost of final exponentiation with the parameters used in each prior work.

BLS family with $k = 9$. The elliptic curve E parametrized as BLS family with embedding degree 9 has the following polynomial parameter:

$$\begin{cases} r(x) = \Phi_9(x)/3, \\ p(x) = (x-1)^2(x^2+x+1)r(x) + x, \\ t(x) = x + 1. \end{cases}$$

The exponent to be computed in final exponentiation for optimal Ate pairings over E is

$$\frac{p^9 - 1}{r} = (p^3 - 1) \cdot \frac{\Phi_9(p)}{r}.$$

The final exponentiation of the BLS family with $k = 9$ is studied in [14]. In [14], using the LLL algorithm, they decomposed $x^3 \cdot \Phi_9(p)/r$ into $\sum \lambda_i p^i$ instead of decomposing $\Phi_9(p)/r$, and searched its coefficient λ_i. The total complexity [14] of the final exponentiation using the decomposition is

$$\begin{aligned} &I_9 + 27M_9 + 302S_9 + 2I_{cyc} + F_1 + F_2 + 2F_3 + F_4 + F_5 \\ =&I_9 + 1052M_1 + 10908S_1. \end{aligned}$$

See [14] for the cost of each operation.

Next, we evaluate the complexity of the final exponentiation using the decomposition which we propose as in section 4. Let h_1, h_2, T be

$$\begin{cases} h_1(x) = (x-1)^2, \\ h_2(x) = 3, \\ T(x) = x. \end{cases}$$

First, we apply Theorem 1 to this BLS family with $k = 9$. The exponent $\Phi_9(p(x))/r(x)$ of the hard part is

$$\Phi_9(p(x))/r(x) = (x-1)^2 \left(\sum_{i=0}^{5} \lambda_i(x) p(x)^i \right) + 3,$$

where

$$\begin{aligned} &\lambda_5(x) = 1, && \lambda_4(x) = x, && \lambda_3(x) = x\lambda_4(x), \\ &\lambda_2(x) = x\lambda_3(x) + 1, && \lambda_1(x) = x\lambda_2(x), && \lambda_0(x) = x\lambda_1(x). \end{aligned}$$

For the value $f \in \mathbb{F}_{p^k}$, the final exponentiation can be computed by the following values:

$$g_0 = f^{p^3} \cdot f^{-1}, \qquad g_1 = g_0^{(x-1)^2}, \qquad g_2 = g_1^{\sum \lambda_i p^i}, \qquad g_3 = g_2 \cdot g_0^2 \cdot g_0.$$

To compute the value g_2, we can deal with the following:

$$h_0 = g_1, \quad h_1 = h_0^x, \quad h_2 = h_1^x, \quad h_3 = h_2^x \cdot h_0, \quad h_4 = h_3^x, \quad h_5 = h_4^x.$$

Using these values, we can compute $g_2 = h_0^{p^5} \cdot h_1^{p^4} \cdot h_2^{p^3} \cdot h_3^{p^2} \cdot h_4^p \cdot h_5$. Therefore, the total cost of the final exponentiation is

$$\begin{aligned}&(I_9 + F_3 + M_9) + 2E_{x-1} + (5E_x + 6M_9 + F_1 + F_2 + F_3 + F_4 + F_5) + (2M_9 \\ &+ S_9) \\ =&I_9 + 25M_9 + 302S_9 + F_1 + F_2 + 2F_3 + F_4 + F_5 \\ =&I_9 + 956M_1 + 10872S_1,\end{aligned}$$

where we use the parameter $x = 2^{43} + 2^{37} + 2^7 + 1$ in [14].

Second, we apply Theorem 3 to this BLS family with $k = 9$. The exponent $\Phi_9(p(x))/r(x)$ of the hard part is

$$\begin{aligned}\Phi_9(p(x))/r(x) &= (x-1)^2 \cdot \Psi_1(x,p)\Psi_3(x,p) \cdot (x^3 + p^3 + 1) + 3 \\ &= (x-1)^2 \cdot (x^2 + px + p^2) \cdot (x^3 + p^3 + 1) + 3.\end{aligned}$$

Therefore, the total cost of the final exponentiation is

$$\begin{aligned}&(I_9 + F_3 + M_9) + (2E_{x-1}) + (2E_x + F_1 + F_2 + 2M_9) + (3E_x + F_3 + 2M_9) \\ &+ (2M_9 + S_9) \\ =&I_9 + 23M_9 + 302S_9 + F_1 + F_2 + 2F_3 \\ =&I_9 + 856M_1 + 10872S_1.\end{aligned}$$

BLS family with $k = 12$. The elliptic curve E parametrized as BLS family with embedding degree 12 has the following polynomial parameter:

$$\begin{cases} r(x) = \Phi_{12}(x), \\ p(x) = (x-1)^2 r(x)/3 + x, \\ t(x) = x + 1. \end{cases}$$

The exponent to be computed in final exponentiation of optimal Ate pairings over E is

$$\frac{p^{12} - 1}{r} = (p^6 - 1)(p^2 + 1) \cdot \frac{\Phi_{12}(p)}{r}.$$

The final exponentiation of the BLS family with $k = 12$ is studied in [2,17]. The final exponentiation decomposition in [17] is the same as the decomposition in Theorem 1. The total cost of the final exponentiation is

$$\begin{aligned}&(I_{12} + 2M_{12} + F_2) + (4E_x + E_{x/2} + 8M_{12} + S_{12} + F_1 + F_2 + F_3) \\ =&I_{12} + 20M_{12} + 535S_{12} + F_1 + 2F_2 + F_3 \\ =&I_{12} + 1135M_1 + 28890S_1.\end{aligned}$$

See [2] for the cost of each operation.

Next, we apply Theorem 4 to this BLS family with $k = 12$. Let h_1, h_2, T be

$$\begin{cases} h_1(x) = (x-1)^2/3 \\ h_2(x) = 1 \\ T(x) = x. \end{cases}$$

The exponent $3 \cdot \Phi_{12}(p(x))/r(x)$ of the hard part is

$$\begin{aligned} 3 \cdot \frac{\Phi_{12}(p(x))}{r(x)} &= (x-1)^2 \cdot \Psi_1(x,p)\Psi_2(x,p) \cdot (x^2+p^2-1) + 3 \\ &= (x-1)^2 \cdot (x+p) \cdot (x^2+p^2-1) + 3. \end{aligned}$$

We use the parameter $x = -2^{107} + 2^{84} + 2^{19}$ in [17]. The total cost of the final exponentiation is

$$\begin{aligned} &(I_{12} + F_2 + 2M_{12}) + (4E_x + E_{x/2} + 7M_{12} + S_{12} + F_1 + F_2) \\ =&I_{12} + 19M_{12} + 535S_{12} + F_1 + 2F_2 \\ =&I_{12} + 1066M_1 + 28890S_1. \end{aligned}$$

See [17] for the idea that we need not compute f^{x-1}.

BLS family with $k = 15$. The elliptic curve E parametrized as BLS family with embedding degree 15 has the following polynomial parameter:

$$\begin{cases} r(x) = \Phi_{15}(x), \\ p(x) = (x-1)^2(x^2+x+1)r(x)/3 + x, \\ t(x) = x+1. \end{cases}$$

The exponent to be computed in final exponentiation for optimal Ate pairings over E is

$$\frac{p^{15}-1}{r} = (p^5-1)(p^2+p+1) \cdot \frac{\Phi_{15}(p)}{r}.$$

The final exponentiation of the BLS family with $k = 15$ is studied in [14]. The total cost of the final exponentiation [14] is

$$\begin{aligned} &I_{15} + 529S_{15} + 63M_{15} + 4I_{cyc} + \sum_{i=1}^{9} F_i \\ =&I_{15} + 3632M_1 + 28674S_1. \end{aligned}$$

See [14] for the cost of each operation.

We evaluate the complexity of the final exponentiation using the decomposition as in Theorem 1. Let h_1, h_2, T be

$$\begin{cases} h_1(x) = (x-1)^2(x^2+x+1)/3 \\ h_2(x) = 1 \\ T(x) = x. \end{cases}$$

The exponent $3 \cdot \Phi_{15}(p(x))/r(x)$ of the hard part is

$$3 \cdot \frac{\Phi_{15}(p(x))}{r(x)} = (x-1)^2(x^2+x+1)\left(\sum_{i=0}^{7} \lambda_i(x)p(x)^i\right) + 3,$$

where

$$\lambda_7 = 1, \quad \lambda_6 = x\lambda_7 - 1, \quad \lambda_5 = x\lambda_6, \quad \lambda_4 = x\lambda_5 + 1$$
$$\lambda_3 = x\lambda_4 - 1, \quad \lambda_2 = x\lambda_3 + 1, \quad \lambda_1 = x\lambda_2, \quad \lambda_0 = x\lambda_1 - 1.$$

We use the parameter $x = 2^{48} + 2^{41} + 2^9 + 2^8 + 1$ in [14]. The total cost of the final exponentiation is

$$\begin{aligned}
&(I_{15} + F_5 + M_{15}) + (2F_1 + 2M_{15}) + 2E_{x-1} + (2E_x + 2M_{15}) + (7E_x + 3I_{cyc} \\
&+ 5M_{15} + \sum_{i=1}^{7} F_i) + (2M_{15} + S_{15}) \\
=&I_{15} + 54M_{15} + 529S_{15} + 3I_{cyc} + 2F_1 + F_5 + \sum_{i=1}^{7} F_i \\
=&I_{15} + 3133M_1 + 28647S_1.
\end{aligned}$$

BLS family with $k = 24$. The elliptic curve E parametrized as BLS family with embedding degree 24 has the following polynomial parameter:

$$\begin{cases} r(x) = \Phi_{24}(x), \\ p(x) = (x-1)^2 r(x)/3 + x, \\ t(x) = x + 1. \end{cases}$$

The exponent to be computed in final exponentiation for optimal Ate pairings over E is

$$\frac{p^{24} - 1}{r} = (p^{12} - 1)(p^4 + 1) \cdot \frac{\Phi_{24}(p)}{r}.$$

The final exponentiation of the BLS family with $k = 24$ is studied in [2,17]. The total cost of the final exponentiation [17] is

$$\begin{aligned}
&(I_{24} + 2M_{24} + F_4) + (8E_x + E_{x/2} + 10M_{24} + S_{24} + \sum_{i=1}^{7} F_i \\
=&I_{24} + 30M_{24} + 432S_{24} + F_4 + \sum_{i=1}^{7} F_i \\
=&I_{24} + 5220M_1 + 69984S_1.
\end{aligned}$$

See [17] for the cost of each operation.

We apply Theorem 4 to this BLS family with $k = 24$. Let h_1, h_2, T be

$$\begin{cases} h_1(x) = (x-1)^2/3 \\ h_2(x) = 1 \\ T(x) = x. \end{cases}$$

The exponent $3 \cdot \Phi_{24}(p(x))/r(x)$ of the hard part is

$$\begin{aligned} 3 \cdot \frac{\Phi_{24}(p(x))}{r(x)} &= (x-1)^2 \cdot \Psi_1(x,p)\Psi_2(x,p)\Psi_4(x,p) \cdot (x^4+p^4-1)+3 \\ &= (x-1)^2 \cdot (x+p)(x^2+p^2) \cdot (x^4+p^4-1)+3. \end{aligned}$$

We use the parameter $x = 2^{48} - 2^{30} + 2^{26}$ in [17]. The total cost of the final exponentiation is

$$\begin{aligned} &(I_{24} + F_4 + 2M_{24}) + (8E_x + E_{x/2} + 8M_{24} + S_{24} + F_1 + F_2 + F_4) \\ =&I_{24} + 28M_{24} + 432S_{24} + F_1 + F_2 + 2F_4 \\ =&I_{24} + 4716M_1 + 69984S_1. \end{aligned}$$

BLS family with $k = 27$. The elliptic curve E parametrized as BLS family with embedding degree 27 has the following polynomial parameter:

$$\begin{cases} r(x) = \Phi_{27}(x)/3, \\ p(x) = (x-1)^2 r(x) + x, \\ t(x) = x + 1. \end{cases}$$

The exponent to be computed in final exponentiation for optimal Ate pairings over E is

$$\frac{p^{27}-1}{r} = (p^9-1) \cdot \frac{\Phi_{27}(p)}{r}.$$

The final exponentiation of the BLS family with $k = 27$ is studied in [40]. The total cost of the final exponentiation [40] is

$$\begin{aligned} &(I_{27} + F_9 + M_{27}) + 2E_{x-1} + (8E_x + 8M_{27} + \sum_{i=1}^{8} F_i) + (9E_x + F_9 + 2M_{27}) \\ &+ (2M_{27} + S_{27}) \\ =&I_{27} + 91M_{27} + 533S_{27} + 2F_9 + \sum_{i=1}^{8} F_i \\ =&I_{27} + 19884M_1 + 115128S_1. \end{aligned}$$

See [40] for the cost of each operation.

We apply Theorem 3 to this BLS family with $k = 27$. Let h_1, h_2, T be

$$\begin{cases} h_1(x) = (x-1)^2 \\ h_2(x) = 3 \\ T(x) = x. \end{cases}$$

The exponent $\Phi_{27}(p(x))/r(x)$ of the hard part is

$$\begin{aligned} \frac{\Phi_{27}(p(x))}{r(x)} &= (x-1)^2 \cdot \Psi_1(x,p)\Psi_3(x,p)\Psi_9(x,p) \cdot (x^9+p^9+1)+3 \\ &= (x-1)^2 \cdot (x^2+px+p^2)(x^6+p^3x^3+p^6) \cdot (x^9+p^9+1)+3. \end{aligned}$$

We use the parameter $x = 2^{28} + 2^{27} + 2^{25} + 2^8 - 2^3$ in [40]. Then the total cost of the final exponentiation is

$$\begin{aligned}&(I_{27} + F_9 + M_{27}) + 2E_{x-1} + (8E_x + 4M_{27} + F_1 + F_2 + F_3 + F_6) + (9E_x + F_9 \\ &+ 2M_{27}) + (2M_{27} + S_{27}) \\ =&I_{27} + 87M_{27} + 533S_{27} + F_1 + F_2 + F_3 + F_6 + 2F_9 \\ =&I_{27} + 18916M_1 + 115128S_1.\end{aligned}$$

BLS family with $k = 48$. The elliptic curve E parametrized as BLS family with embedding degree 48 has the following polynomial parameter:

$$\begin{cases} r(x) = \Phi_{48}(x), \\ p(x) = (x-1)^2 r(x)/3 + x, \\ t(x) = x + 1. \end{cases}$$

The exponent to be computed in final exponentiation for optimal Ate pairings over E is

$$\frac{p^{48} - 1}{r} = (p^{16} - 1)(p^{16} + p^8 + 1) \cdot \frac{\Phi_{48}(p)}{r}.$$

The final exponentiation of the BLS family with $k = 48$ is studied in [24,28]. The total cost of the final exponentiation [28] is

$$\begin{aligned}&I_{48} + 22M_{48} + 17E_x + S_{48} + F_8 + \sum_{i=1}^{15} F_i \\ =&I_{48} + 73M_{48} + 545S_{48} + F_8 + \sum_{i=1}^{15} F_i \\ =&I_{48} + 36222M_1 + 264870S_1.\end{aligned}$$

See [28] for the cost of each operation.

We apply Theorem 4 to this BLS family with $k = 48$. Let h_1, h_2, T be

$$\begin{cases} h_1(x) = (x-1)^2/3 \\ h_2(x) = 1 \\ T(x) = x. \end{cases}$$

The exponent $3 \cdot \Phi_{48}(p(x))/r(x)$ of the hard part is

$$\begin{aligned}3 \cdot \frac{\Phi_{48}(p(x))}{r(x)} &= (x-1)^2 \cdot \Psi_1(x,p)\Psi_2(x,p)\Psi_4(x,p)\Psi_8(x,p) \cdot (x^8 + p^8 - 1) + 3 \\ &= (x-1)^2 \cdot (x+p)(x^2+p^2)(x^4+p^4) \cdot (x^8 + p^8 - 1) + 3.\end{aligned}$$

We use the parameter $x = 2^{32} - 2^{18} - 2^{10} - 2^4$ in [28]. Then the total cost of the final exponentiation is

$$\begin{aligned}&(I_{48} + 3M_{48} + F_8) + (16E_x + E_{x/2} + 9M_{48} + S_{48} + F_1 + F_2 + F_4 + F_8) \\ =&I_{48} + 63M_{48} + 544S_{48} + F_1 + F_2 + F_4 + 2F_8 \\ =&I_{48} + 30849M_1 + 264384S_1.\end{aligned}$$

6 Conclusion

In this paper, we presented a new decomposition of hard part in final exponentiation for optimal Ate pairings over families of elliptic curves. The first decomposition method is that we derive the coefficients of base-p expansion of hard part from cyclotomic polynomials for families of elliptic curves with arbitrary embedding degrees. The second decomposition method is that we directly factorize hard part using a new tool, homogeneous cyclotomic polynomials, for families of elliptic curves with specific embedding degrees $k = 2^i$, 3^j and $2^i 3^j$. Both methods are effective for families of elliptic curves with trace $x + 1$, for example BLS families, and our results give faster final exponentiation than the previous state-of-the-art construction on BLS families.

Acknowledgment

This work was supported by the Cabinet Office (CAO), Cross-ministerial Strategic Innovation Promotion Program (SIP), "Cyber Physical Security for IoT Society", JPNP18015 (funding agency: NEDO).

The third author was partially supported by JST CREST Grant Number JPMJCR19F6 and JSPS KAKENHI Grant Number JP19H01109.

References

1. Aranha, D.F., Barreto, P.S.L.M., Longa, P., Ricardini, J.E.: The realm of the pairings. In: SAC 2013 Proceedings. pp. 3–25 (2013)
2. Aranha, D.F., Fuentes-Castañeda, L., Knapp, E., Menezes, A., Rodríguez-Henríquez, F.: Implementing pairings at the 192-bit security level. In: Pairing 2012 Proceedings. pp. 177–195 (2012)
3. Aranha, D.F., Karabina, K., Longa, P., Gebotys, C.H., Hernandez, J.L.: Faster explicit formulas for computing pairings over ordinary curves. In: EUROCRYPT 2011 Proceedings. pp. 48–68 (2011)
4. Aranha, D.F., Knapp, E., Menezes, A., Rodríguez-Henríquez, F.: Parallelizing the Weil and Tate pairings. In: IMACC 2011 Proceedings. pp. 275–295 (2011)
5. Atkin, A.O.L., Morain, F.: Elliptic curves and primality proving. Math. Comput. **61**(203), 29–68 (July 1993)
6. Barbulescu, R., Duquesne, S.: Updating key size estimations for pairings. J. Cryptology **32**(4), 1298–1336 (2019)
7. Barbulescu, R., El Mrabet, N., Ghammam, L.: A taxonomy of pairings, their security, their complexity. Cryptology ePrint Archive, Report 2019/485 (2019), `https://eprint.iacr.org/2019/485`
8. Barreto, P.S.L.M., Lynn, B., Scott, M.: Constructing elliptic curves with prescribed embedding degrees. In: SCN 2002 Proceedings. pp. 257–267 (2002)
9. Barreto, P.S.L.M., Lynn, B., Scott, M.: Efficient implementation of pairing-based cryptosystems. J. Cryptology **17**(4), 321–334 (2004)
10. Beuchat, J., González-Díaz, J.E., Mitsunari, S., Okamoto, E., Rodríguez-Henríquez, F., Teruya, T.: High-speed software implementation of the optimal ate pairing over Barreto–Naehrig curves. In: Pairing 2010 Proceedings. pp. 21–39 (2010)

11. Boneh, D., Gorbunov, S., Wahby, R.S., Wee, H., Zhang, Z.: draft-irtf-cfrg-bls-signature-02. Internet-Draft draft-irtf-cfrg-bls-signature-02, Internet Engineering Task Force (Mar 2020), https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-bls-signature-02, work in Progress
12. El Mrabet, N., Guillevic, A., Ionica, S.: Efficient multiplication in finite field extensions of degree 5. In: AFRICACRYPT 2011 Proceedings. pp. 188–205 (2011)
13. El Mrabet, N., Joye, M. (eds.): Guide to Pairing-Based Cryptography. Chapman and Hall/CRC (2016)
14. Fouotsa, E., El Mrabet, N., Pecha, A.: Computing optimal ate pairings on elliptic curves with embedding degree $9, 15$ and 27. Cryptology ePrint Archive, Report 2016/1187 (2016), https://eprint.iacr.org/2016/1187
15. Freeman, D., Scott, M., Teske, E.: A taxonomy of pairing-friendly elliptic curves. J. Cryptology **23**(2), 224–280 (2010)
16. Fuentes-Castañeda, L., Knapp, E., Rodríguez-Henríquez, F.: Faster hashing to $\mathbb{G}_2$. In: SAC 2011 Proceedings. pp. 412–430 (2011)
17. Ghammam, L., Fouotsa, E.: Improving the computation of the optimal ate pairing for a high security level. J. Appl. Math. Comput. **59**, 21–36 (2019)
18. Groves, M.: MIKEY-SAKKE: Sakai-Kasahara Key Encryption in Multimedia Internet KEYing (MIKEY). RFC 6509 (Feb 2012). https://doi.org/10.17487/RFC6509
19. Guillevic, A.: A short-list of pairing-friendly curves resistant to special TNFS at the 128-bit security level. In: PKC 2020 Proceedings Part II. pp. 535–564 (2020)
20. Hess, F.: Pairing lattices. In: Pairing 2008 Proceedings. pp. 18–38 (2008)
21. Hess, F., Smart, N.P., Vercauteren, F.: The eta pairing revisited. IEEE Trans. Inf. Theory **52**(10), 4595–4602 (2006)
22. Kim, T., Barbulescu, R.: Extended tower number field sieve: A new complexity for the medium prime case. In: CRYPTO 2016 Proceedings Part I. pp. 543–571 (2016)
23. Kim, T., Jeong, J.: Extended tower number field sieve with application to finite fields of arbitrary composite extension degree. In: PKC 2017 Proceedings Part I. pp. 388–408 (2017)
24. Kiyomura, Y., Inoue, A., Kawahara, Y., Yasuda, M., Takagi, T., Kobayashi, T.: Secure and efficient pairing at 256-bit security level. In: ACNS 2017 Proceedings. pp. 59–79 (2017)
25. Knuth, D.E.: The art of computer programming, Volume II: Seminumerical Algorithms. Addison-Wesley, 3rd edn. (1998)
26. Le, D., Tan, C.H.: Speeding up ate pairing computation in affine coordinates. In: ICISC 2012 Proceedings. pp. 262–277 (2012)
27. Lin, X., Zhao, C., Zhang, F., Wang, Y.: Computing the ate pairing on elliptic curves with embedding degree $k = 9$. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **91-A**(9), 2387–2393 (2008)
28. Mbang, N.B., Aranha, D., Fouotsa, E.: Computing the optimal ate pairing over elliptic curves with embedding degrees 54 and 48 at the 256-bit security level. IJACT **4**(1), 45–59 (2020)
29. Menezes, A., Sarkar, P., Singh, S.: Challenges with assessing the impact of NFS advances on the security of pairing-based cryptography. In: Mycrypt 2016 Proceedings. pp. 83–108 (2016)
30. Micheli, G.D., Gaudry, P., Pierrot, C.: Asymptotic complexities of discrete logarithm algorithms in pairing-relevant finite fields. Cryptology ePrint Archive, Report 2020/329 (2020), https://eprint.iacr.org/2020/329
31. Miller, V.S.: The Weil pairing, and its efficient calculation. J. Cryptology **17**(4), 235–261 (2004)

32. Rubin, K., Silverberg, A.: Choosing the correct elliptic curve in the CM method. Math. Comput. **79**(269), 545–561 (2010)
33. Sakemi, Y., Kobayashi, T., Saito, T., Wahby, R.S.: Pairing-Friendly Curves. Internet-Draft draft-irtf-cfrg-pairing-friendly-curves-07, Internet Engineering Task Force (Jun 2020), work in Progress
34. Sarkar, P., Singh, S.: A general polynomial selection method and new asymptotic complexities for the tower number field sieve algorithm. In: ASIACRYPT 2016 Proceedings Part I. pp. 37–62 (2016)
35. Scott, M., Benger, N., Charlemagne, M., Perez, L.J.D., Kachisa, E.J.: On the final exponentiation for calculating pairings on ordinary elliptic curves. In: Pairing 2009 Proceedings. pp. 78–88 (2009)
36. Teruya, T., Saito, K., Kanayama, N., Kawahara, Y., Kobayashi, T., Okamoto, E.: Constructing symmetric pairings over supersingular elliptic curves with embedding degree three. In: Pairing 2013 Proceedings. pp. 97–112 (2013)
37. Trusted Computing Group: TPM 2.0 library specification. `https://trustedcomputinggroup.org/resource/tpm-library-specification/` (2019)
38. Vercauteren, F.: Optimal pairings. IEEE Trans. Inf. Theory **56**(1), 455–461 (2010)
39. Zavattoni, E., Perez, L.J.D., Mitsunari, S., Sánchez-Ramírez, A.H., Teruya, T., Rodríguez-Henríquez, F.: Software implementation of an attribute-based encryption scheme. IEEE Trans. Computers **64**(5), 1429–1441 (2015)
40. Zhang, X., Lin, D.: Analysis of optimum pairing products at high security levels. In: INDOCRYPT 2012 Proceedings. pp. 412–430 (2012)

A BLS Elliptic Curve

In this section, we briefly describe the Barreto–Lynn–Scott (BLS) families proposed by Barreto et al. [8], and their elliptic curve search method with general embedding degree and general CM discriminant [8].

Family in Particular Case. The BLS families [8] are defined as the four polynomial parameterized quintuples with fixed CM discriminant $D = 3$ and specific embedding degrees, as described in Fig. 1.

Arbitrary Case. Barreto et al. [8] considered how to obtain elliptic curves with arbitrary CM discriminant and arbitrary embedding degree suitable for pairing-based cryptography. Given CM discriminant D and embedding degree k, their search procedure seeks an integer z and an appropriate quintuple (k, D, p, r, t) satisfying $t = z + 1$, $r = \Phi_k(z)$, $p = mr + z$, where m is an integer. See [8] for details.

B Proofs of Theorems

B.1 Proof of Theorem 1

Set $\Phi_k(x) = \sum_{i=0}^{d} c_i x^i$. For the polynomials $r(x)$, $p(x)$ as in (1), we consider a decomposition of $\Phi_k(p(x))/r(x)$. As Zhang and Lin state in [40], we extract the factor $r(x)$ from the polynomial $\Phi_k(p(x))$ using a recurrent formula $p^m =$

(a) BLS family with $k = 3^i$, where $i > 0$

$$\begin{aligned} t(x) &= x + 1, \\ r(x) &= \Phi_k(x)/3, \\ p(x) &= (x-1)^2 r(x) + x. \end{aligned}$$

(b) BLS family with $k = 2^j 3$, where $j > 0$

$$\begin{aligned} t(x) &= x + 1, \\ r(x) &= \Phi_k(x), \\ p(x) &= \frac{(x-1)^2 r(x)}{3} + x. \end{aligned}$$

(c) BLS family with $k = 3^i q^s$, where $i, s > 0$ are integers, and $q > 3$ is a prime number

$$\begin{aligned} t(x) &= x + 1, \\ r(x) &= \Phi_k(x), \\ y(x) &= 2x^{3^{i-1}q^{s-1}} + 1, \\ m(x) &= 3\left(\frac{x-1}{6}\right)^2 (y(x)^2 + 3), \\ p(x) &= m(x)r(x) + x. \end{aligned}$$

(d) BLS family with $k = 3^i 2^j q^s$, where $i, j, s > 0$ are integers, and $q > 3$ is a prime number

$$\begin{aligned} t(x) &= x + 1, \\ r(x) &= \Phi_k(x), \\ y(x) &= 2x^{3^{i-1}2^{j-1}q^{s-1}} - 1, \\ m(x) &= 3\left(\frac{x-1}{6}\right)^2 (y(x)^2 + 3), \\ p(x) &= m(x)r(x) + x. \end{aligned}$$

Fig. 1: BLS families with $D = 3$

$h_1 r p^{m-1} + T p^{m-1}$. Reducing the degree of p using the above recurrent formula, we obtain that:

$$\begin{aligned} p^m &= h_1 r p^{m-1} + T p^{m-1} \\ &= h_1 r p^{m-1} + T(h_1 r p^{m-2} + T p^{m-2}) \\ &= h_1 r p^{m-1} + h_1 r T p^{m-2} + T^2(h_1 r p^{m-3} + T p^{m-3}) \\ &\cdots \\ &= h_1 r p^{m-1} + h_1 r T p^{m-2} + h_1 r T^2 p^{m-3} + \cdots + T^{m-1}(h_1 r p^0 + T p^0) \\ &= h_1 r (T^0 p^{m-1} + T^1 p^{m-2} + \cdots + T^{m-1} p^0) + T^m \\ &= h_1 r \cdot g_{m-1} + T^m, \end{aligned} \tag{3}$$

where

$$g_{m-1}(x) = \sum_{i=0}^{m-1} T(x)^i p(x)^{m-1-i}. \tag{4}$$

Second, we apply the equation (3) to each $p(x)^i$ $(0 < i \leq d)$ of $\Phi_k(p(x))$. Then:

$$\begin{aligned}
\Phi_k((p(x)) &= \sum_{i=0}^{d} c_i p(x)^i = \sum_{i=1}^{d} c_i (h_1(x) r(x) \cdot g_{i-1}(x) + T(x)^i) + c_0 \\
&= h_1(x) r(x) \left(\sum_{i=1}^{d} c_i g_{i-1}(x) \right) + \left(\sum_{i=1}^{d} c_i T(x)^i \right) + c_0 \\
&= h_1(x) r(x) \left(\sum_{i=1}^{d} c_i g_{i-1}(x) \right) + \Phi_k(T(x)) \\
&= h_1(x) r(x) \left(\sum_{i=1}^{d} c_i g_{i-1}(x) \right) + r(x) h_2(x).
\end{aligned}$$

Hence, we obtain:

$$\Phi_k(p(x))/r(x) = h_1(x) \left(\sum_{i=1}^{d} c_i g_{i-1}(x) \right) + h_2(x).$$

Therefore, it is enough to prove that

$$\sum_{i=1}^{d} c_i g_{i-1}(x) = \sum_{i=0}^{d-1} \lambda_i(x) p(x)^i.$$

Substituting the equation (4) into $g_{i-1}(x)$ on the left side:

$$\sum_{i=1}^{d} c_i g_{i-1}(x) = \sum_{i=1}^{d} \left(c_i \sum_{j=0}^{i-1} T(x)^{i-1-j} p(x)^j \right).$$

Exchanging the sums, we obtain that:

$$\sum_{i=1}^{d} c_i g_{i-1}(x) = \sum_{j=0}^{d-1} \left(\left(\sum_{i=j+1}^{d} c_i T(x)^{i-1-j} \right) p(x)^j \right).$$

We represent the coefficient $\sum_{i=j+1}^{d} c_i T(x)^{i-1-j}$ of $p(x)^j$ by $\Lambda_j(x)$. Using $\ell = d-j-1$:

$$\begin{aligned}
\Lambda_j(x) &= (c_d, c_{d-1}, \ldots, c_{d-\ell}) \begin{pmatrix} T(x)^{\ell} \\ T(x)^{\ell-1} \\ \vdots \\ T(x)^0 \end{pmatrix} \\
&= (c_d, c_{d-1}, \ldots, c_{d-(\ell-1)}) \begin{pmatrix} T(x)^{\ell} \\ T(x)^{\ell-1} \\ \vdots \\ T(x)^1 \end{pmatrix} + c_{d-\ell} T(x)^0 \\
&= (c_d, c_{d-1}, \ldots, c_{d-(\ell-1)}) \begin{pmatrix} T(x)^{\ell-1} \\ T(x)^{\ell} \\ \vdots \\ T(x)^0 \end{pmatrix} \cdot T(x) + c_{d-\ell} \\
&= T(x)\Lambda_{j+1}(x) + c_{j+1}.
\end{aligned} \tag{5}$$

From the equation (5), we get $\Lambda_{d-1}(x) = c_d$. This completes the proof. □

B.2 Proof of Theorem 2

The k-th cyclotomic polynomial is of the form $\Phi_k(x) = x^{k/2} + 1$ for $k = 2^n$. Since we have $p^m = h_1 r p^{m-1} + T p^m$ from the equation (1), we can sequentially reduce the polynomial $\Phi_k(p)$ as:

$$\begin{aligned}
\Phi_k(p) &= p^{k/2} + 1 \\
&= h_1 r(T^{k/2-1} + pT^{k/2-2} + \cdots + p^{k/2-2}T + p^{k/2-1}) + T^{k/2} + 1 \\
&= h_1 r(T^{k/2-1} + pT^{k/2-2} + \cdots + p^{k/2-2}T + p^{k/2-1}) + h_2 r.
\end{aligned}$$

Applying Lemma 1 to this polynomial completes the proof. □

B.3 Proof of Theorem 3

The k-th cyclotomic polynomial is of the form $\Phi_k(x) = x^{2\cdot k/3} + x^{k/3} + 1$ for $k = 3^n$. Since we have $p^m = h_1 r p^{m-1} + T p^m$ from the equation (1), we can sequentially reduce the polynomial $\Phi_k(p)$ as:

$$\begin{aligned}
\Phi_k(p) &= p^{2\cdot k/3} + p^{k/3} + 1 \\
&= h_1 r\{p^{2\cdot k/3-1} + Tp^{2\cdot k/3-2} + \cdots + T^{k/3-1}p^{k/3} \\
&\quad + (T^{k/3}+1)p^{k/3-1} + \cdots + T^{k/3-1}(T^{k/3}+1)\} + T^{2\cdot k/3} + T^{k/3} + 1 \\
&= h_1 r\{p^{k/3}(p^{k/3-1} + Tp^{k/3-2} + \cdots + T^{k/3-1}) \\
&\quad + (T^{k/3}+1)(p^{k/3-1} + Tp^{k/3-2} + \cdots + T^{k/3-1})\} + h_2 r \\
&= h_1 r(p^{k/3-1} + Tp^{k/3-2} + \cdots + T^{k/3-1})(T^{k/3} + p^{k/3} + 1) + h_2 r.
\end{aligned}$$

Applying Lemma 1 to this polynomial completes the proof. □

B.4 Proof of Theorem 4

The k-th cyclotomic polynomial is of the form $\Phi_k(x) = x^{2\cdot k/6} - x^{k/6} + 1$ for $k = 2^m 3^n$. Since we have $p^m = h_1 r p^{m-1} + T p^m$ from the equation (1), we can sequentially reduce the polynomial $\Phi_k(p)$ as:

$$\begin{aligned}
\Phi_k(p) &= p^{2\cdot k/6} + p^{k/6} + 1 \\
&= h_1 r\{p^{2\cdot k/6-1} + Tp^{2\cdot k/6-2} + \cdots + T^{k/6-1}p^{k/6} \\
&\quad + (T^{k/6} - 1)p^{k/6-1} + \cdots + T^{k/6-1}(T^{k/6} - 1)\} + T^{2\cdot k/6} + T^{k/6} + 1 \\
&= h_1 r\{p^{k/6}(p^{k/6-1} + Tp^{k/6-2} + \cdots + T^{k/6-1}) \\
&\quad + (T^{k/6} - 1)(p^{k/6-1} + Tp^{k/6-2} + \cdots + T^{k/6-1})\} + h_2 r \\
&= h_1 r(p^{k/6-1} + Tp^{k/6-2} + \cdots + T^{k/6-1})(T^{k/6} + p^{k/6} - 1) + h_2 r.
\end{aligned}$$

Applying Lemma 1 to this polynomial completes the proof. □