International Journal of Networking and Computing – www.ijnc.org, ISSN 2185-2847
Volume 12, Number 2, pages 317–338, July 2022

Efficient Final Exponentiation for Cyclotomic Families of Pairing-Friendly Elliptic Curves with Any Prime Embedding Degrees

Yuki Nanjo[†1], Masaaki Shirase[‡], Yuta Kodera[†], Takuya Kusaka[†] and Yasuyuki Nogami[†]

[†]Okayama University, Tsushima–naka 3–1–1, Kita–ku, Okayama 700–8530, Japan.
[‡]Future University Hakodate, Kamedanakano-cho 116–2, Hakodate, Hokkaido 041–8655, Japan.

Received: February 8, 2022
Revised: April 28, 2022
Accepted: May 28, 2022
Communicated by Toru Nakanishi

Abstract

Pairings on elliptic curves consisting of the Miller loop and final exponentiation are used for innovative protocols such as ID-based encryption and group signature authentication. As the recent progress of attacks for the discrete logarithm problem in finite fields in which pairings are defined, the importance of the use of curves with prime embedding degrees k has been increased. In this paper, the authors provide formulas to construct algorithms for computing the final exponentiation for cyclotomic families of curves with any prime k. Since the formulas give rise to one of the same exponents given by a lattice-based method for the small cases of k, it is expected that the proposed algorithms are efficient enough for the cases of any prime k. At least for the curves with $k = 13$ and 19 for the pairing at the 128-bit security level, the proposed algorithms can achieve current state-of-the-art computations.

Keywords: Pairing-based cryptography, elliptic curve, final exponentiation.

1 Introduction

Pairings on elliptic curves enable innovative protocols, e.g., ID-based encryption [7], group signature authentication [5], searchable encryption [6], attribute-based encryption [13], and homomorphic encryption [29]. The security of the pairings is typically based on the difficulties of the discrete logarithm problem (DLP) in the finite field and elliptic curve. In recent years, there have been notable improvements of the tower number field sieve (TNFS) algorithm which is an attack for DLP in a finite field [22]. This motivates researchers working on the review of the security analyses and providing new recommendations of curves in [1, 2, 10, 17, 15, 8, 16]. Interestingly, according to these results, not only the curves with composite embedding degree k but also the curves with prime k are suggested for the pairings. This is because the curves with a prime k have high resistance against the TNFS which leads to an advantage of the use of the small size of the field. In [8], Clarisse et al. focused on this advantage and presented curves with $k = 13$ and 19 that are specifically tailored to be fast over the specific group used for the pairings, however, performances of the pairings are not so good.

In this context, the pairings on elliptic curves are typically carried out by two steps, which are the Miller loop and extra exponentiation in the field to bring the output of the Miller loop to

[1]From April 2022, the affiliation has changed to Toshiba Corporation, 1–1, Shibaura 1–chome, Minato–ku, Tokyo 105–8001, Japan.

Table 1: Properties of previous and proposed methods.

Methods	Based on	Alg. gen.	Applicable for	Effective for
Fuentes-Castaneda et al. [12]	Lattice	Heuristic	Any families	Any families
Kim et al. [23]	Lattice	Heuristic	Any curves	Curves not in families
Hayashida et al. [18]	Formula	Algorithmic	Any families	Specific families, e.g., BLS family
This work	Formula	Algorithmic	Cyclotomic families with any prime k	Cyclotomic families with any prime k

the unique value. This extra exponentiation is called the final exponentiation and that becomes more of a computational bottleneck with the curves with larger k. Since the final exponentiation has the specific exponent corresponding to the families of curves, optimization techniques have been proposed. As one of the typical methods, in [30], Scott et al. proposed to expand the exponent in base a field characteristic to exploit the Frobenius endomorphism with low computational complexity. In [12], Fuentes-Castaneda et al. presented a lattice-based method for determining a multiple of the exponent which results in at least as efficient final exponentiations as ones given by Scott et al. [30]. Later, in [23], Kim et al. also showed that a similar method to [12] for any curves. Especially, the lattice-based method given in [12] might produce one of the most efficient algorithms for computing the final exponentiation for a majority of families of curves. However, the method involves several heuristic processes with a trial-and-error search and thus it requires complicated works for producing one of the best exponents. This might become an obstacle to updating the curves and reproducing the algorithms according to the security analyses in the future.

To overcome the problem, in [18], Hayashida et al. focused on another method for providing the expansion of the exponent by using the structure of pairings given by Zhang et al. in [34] that is only applicable for the BLS family [3] of curves with $k = 27$. They extended [34] for any families of curves to allow us to obtain an algorithm for computing the final exponentiation with a small effort. Their method might provide more efficient algorithms than the lattice-based method [12] for the BLS family of curves with any k of multiple of 3 and 6 except for 18. However, unfortunately, the method by Hayashida et al. [18] might not be effective for the other families of curves. As described in the first paragraph, since the importance of the curves with a prime k has been notably increased, similar methods that are especially effective for these curves are desired. In this paper, the authors try to meet this demand.

Our contribution. The authors focus on the cyclotomic families of curves with prime embedding degree k where the parameterizations are presented in Construction 6.6 of [11] and which can generate the curves with $k = 13$ and 19 given by Clarisse et al. in [8]. For these families of curves with any prime k, the authors propose a new method for constructing an efficient algorithm for computing the final exponentiation. The properties of the previous methods [12, 18, 23] and the proposed one are summarized in Table 1. The details of the contributions are described below.

(i) The authors provide formulas for providing specific multiples of the exponents of the final exponentiation for the cyclotomic families of curves with any prime k. For the cases of $k = 5, 7, 11, 13, 17$, and 19, the authors confirmed that the proposed formulas provide exactly one of the same exponents given by the lattice-based method [12]. Thus, there is a possibility that the proposed formulas result in as efficient algorithms as ones given by [12] for the cases of any prime k.

(ii) According to the proposed formulas, the authors construct algorithms for computing the final exponentiation with fixed calculation costs for the cyclotomic families of curves with any prime k. As a result, it is found that the proposed algorithms have lower computational complexity than that of the method by Hayashida et al. [18] Indeed, although the previous algorithm has $O(n^2)$ complexity, the proposed ones have $O(n)$ complexity, where n is an integer such that $k = 6n \pm 1$.

(iii) The authors estimate the calculation costs of the final exponentiation for the curves with $k = 13$ and 19 at the 128-bit security level by applying the proposed algorithms. The estimation result shows that there are 47.5% and 63.4% reductions of the calculation costs from the previous result [8] based on the method by Kim et al. [23] for the curves with $k = 13$ and 19, respectively. Thus, the proposed algorithms can reach state-of-the-art computations of the final exponentiation at least for those curves.

Differences from CANDAR'21. This paper is an extended version of the authors' previous work [28] published in CANDAR'21. The previous version provided the formula and algorithm for computing the final exponentiation for the cyclotomic family of curves with prime k given by $k = 6n + 1$. Although the previous version does not consider the case of prime k of $k = 6n - 1$, this paper considers the formula and algorithm for such cases. In addition to this, the authors revise the construction of the algorithm and reduce the several numbers of the multiplications and cyclotomic inversions of the final exponentiation of the case of $k = 6n + 1$. Moreover, the authors estimate the calculation costs of the final exponentiation of the pairings on the concrete curves.

Organization. The rest of this paper is organized below. Sect. 2 provides a brief background on pairings. In Sect. 3, the author reviews the structure of the final exponentiation with the previous optimization techniques. Sect. 4 presents the proposed formulas of the final exponentiation for the cyclotomic families of curves with prime embedding degrees. In Sect. 5, the authors apply the formulas and construct the algorithms for computing the final exponentiation. The result of the calculation cost estimations with certain curves is also described. Finally, Sect. 6 draws the conclusion.

2 Background on Pairing

The authors present the fundamentals of pairings on elliptic curves. In the following, for a positive integer i and a prime p, let $\mathbb{F}_q$ be a finite field of order q, where $q = p^i$. Let $\mathbb{F}_q^*$ be a multiplicative group of $\mathbb{F}_q$ and let $\overline{\mathbb{F}}_q$ be an algebraic closure of $\mathbb{F}_q$.

2.1 Elliptic curves

For a prime $p > 3$, an elliptic curve E of Weierstrass form defined over $\mathbb{F}_p$ is given as follows:

$$E/\mathbb{F}_p : y^2 = x^3 + ax + b, \tag{1}$$

where a and b are coefficients in $\mathbb{F}_p$ satisfying $4a^3 + 27b^2 \neq 0$. The j-invariant of E is given by $j(E) = 1728 \cdot 4a^3/(4a^3 + 27b^2)$. A set of rational points is defined by $E(\overline{\mathbb{F}}_p) = \{(x, y) \mid (x, y) \in \overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p, y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$ where $\mathcal{O}$ is a point at infinity on E. The set forms an abelian group of which $\mathcal{O}$ acts as the identity, and which is called a rational point group. For a positive integer s, a point multiplication endomorphism is defined as $[s] : E(\overline{\mathbb{F}}_p) \to E(\overline{\mathbb{F}}_p), P \mapsto P + P + \cdots + P$ which involves $(s - 1)$-times additions. If $E(\overline{\mathbb{F}}_p)$ does not admit a point of order p such that $[p]P = \mathcal{O}$, E is supersingular, otherwise, E is non-supersingular or ordinary.

Let $n = \#E(\mathbb{F}_p)$, which is the number of rational points. Let t be an integer defined by $t = p+1-n$ which is called the Frobenius trace of E. If E is ordinary, there is a square-free integer D such that $DV^2 = 4p - t^2$ with an integer V. Let r be a prime factor of n such that $p \neq r$. Let $E[r]$ be an entire group of order r defined by $E[r] = \{P \mid P \in E(\overline{\mathbb{F}}_p), [r]P = \mathcal{O}\}$ which is called an r-torsion subgroup. Then, the group structure of $E[r]$ is $E[r] \cong \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$, i.e., $\#E[r] = r^2$. This implies that $E[r]$ has $(r + 1)$ different subgroups of order r since the identity $\mathcal{O}$ overlaps into all subgroups of order r. Let k be the smallest integer satisfying $r \mid (p^k - 1)$, i.e., there is a multiplicative subgroup of $\mathbb{F}_{p^k}^*$ of order r. Then, $E[r]$ belongs to the rational point group $E(\mathbb{F}_{p^k})$. The quantity k is called an embedding degree with respect to r.

2.2 Pairings

Let G_1 and G_2 be different subgroups of $E[r] \subset E(\mathbb{F}_{p^k})$ defined by $G_1 = E[r] \cap \ker(\pi_p - [1])$ and $G_2 = E[r] \cap \ker(\pi_p - [p])$, where π_p is Frobenius endomorphism for points of elliptic curve E, i.e., $\pi_p : E(\overline{\mathbb{F}}_p) \to E(\overline{\mathbb{F}}_p), (x, y) \mapsto (x^p, y^p)$. Note that the groups are the eigenspaces of π_p on $E[r]$, i.e., $G_1 \oplus G_2 \cong E[r]$. According to the properties of the subgroups, G_1 and G_2 are named as base-field and trace-zero subgroups, respectively. For two points $P \in G_1$ and $Q \in G_2$, the Tate pairing τ_r, which is non-degenerate and bilinear, is defined as follows:

$$\tau_r : G_1 \times G_2 \to \mathbb{F}^*_{p^k}/(\mathbb{F}^*_{p^k})^r, (P, Q) \mapsto f_{r,P}(Q), \tag{2}$$

where $f_{r,P}$ is a rational function with a divisor $\mathrm{div}(f_{r,P}) = r(P) - r(\mathcal{O})$. The value of $f_{r,P}(Q)$ is computed by Miller's algorithm [25] that is an iterative algorithm with $O(\log_2 r)$.

As seen in the definition, the standard Tate pairing has an undesirable property that the output lies in an equivalence class, rather than being a unique element. To be suitable in practice, $(p^k - 1)/r$ is raised to the output of the Tate pairing as follows:

$$\hat{\tau}_r : G_1 \times G_2 \to \mu_r, (P, Q) \mapsto f_{r,P}(Q)^{\frac{p^k-1}{r}}, \tag{3}$$

where μ_r is a subgroup of $\mathbb{F}^*_{p^k}$ of order r which consists of r-th roots of identity. The above pairing is called the reduced Tate pairing. The additional exponentiation is called the final exponentiation.

There are several variants of Tate pairings with shorter loop length of Miller's algorithm than typical ones. According to [19], restricting the reduced Tate pairing to swap the arguments as $G_2 \times G_1$ with the above subgroups leads to an ate pairing α_T defined as follows:

$$\alpha_T : G_2 \times G_1 \to \mu_r, (Q, P) \mapsto f_{T,Q}(P)^{\frac{p^k-1}{r}}, \tag{4}$$

where $T = t - 1$ and $f_{T,Q}$ is a rational function with a divisor $\mathrm{div}(f_{T,Q}) = T(Q) - ([T]Q) - (T-1)(\mathcal{O})$, which is computed by Miller's algorithm with $O(\log_2 T)$. Since $\log_2 T < \log_2 r$ is typically satisfied for the curves for practical pairings, the loop length of Miller's algorithm for ate pairing is shorter than that of the typical Tate pairings. The ate pairing is one of the special cases of ate-like pairings introduced in [33] for generating an optimum pairing.

2.3 Pairing-friendly elliptic curves

As seen in the above descriptions, the properties of the elliptic curves are typically specified by integer parameters k, D, p, r, and t. In this paper, elliptic curves having small k, large r, and appropriate ρ-value defined by $\rho = \log_2 p / \log_2 r$ are called pairing-friendly. The concrete properties of the pairing-friendly curves depend on the security level that we would like to guarantee, e.g., for the STNFS secure-pairing at the 128-bit security level, it is suggested to use the curves such that $6 \leq k \leq 16$, $256 \leq \log_2 r$, and $1 \leq \rho \leq 2.6$ in [15]. Note that ρ greater than 2 is currently acceptable, however, it is previously considered that ρ is desired to satisfy $1 \leq \rho \leq 2$.

One of the first suggested methods for constructing ordinary pairing-friendly curves with ρ around 2 was presented in an unpublished manuscript [9] by Cocks and Pinch. The other methods are typically based on an idea of the parameterization of p, r, and t as polynomials $p(x)$, $r(x)$, and $t(x)$ in terms of variable x to make curves to have favorite properties, respectively. In this paper, the parameterized triple $(p(x), r(x), t(x))$ is called a family of elliptic curves, where a curve is generated by finding an integer seed $x = x_0$ making $p(x_0)$ and $r(x_0)$ being primes, and $t(x_0)$ being an integer. Many families of pairing-friendly elliptic curves have been discovered in [26, 3, 4, 20, 11]. Currently, cyclotomic families of pairing-friendly curves, which are introduced in [11] and are involving the BLS family [3], are important for generating not only curves with composite k but also curves with prime k.

3 Review of Final Exponentiation

As described in the previous section, the variants of reduced Tate pairing require the final exponentiation. In this section, the authors review the basic structure of the final exponentiation and

briefly describe the major optimizations techniques given by [30, 12, 18]. Before providing them, the authors firstly describe the cyclotomic polynomial.

3.1 Cyclotomic polynomial

For any positive integer n, Euler's totient function ϕ is given as follows:

$$\phi(n) = \#\{i \in 1, 2, \ldots, n-1 : \gcd(i, n) = 1\}. \tag{5}$$

The n-th cyclotomic polynomial is defined by

$$\Phi_n(x) = \prod_{\substack{1 \le m \le n \\ \gcd(m,n)=1}} (x - e^{2\pi i m/n}), \tag{6}$$

where e is Napier's constant, i is the imaginary unit, and π is a mathematical constant that is approximately equal to 3.14. Although that is not an immediate derivation from the definition, $\Phi_n(x)$ is a monic polynomial with integer coefficients that is the minimal polynomial over the field of the rational numbers of a primitive n-th root of unity. When enumerating the cyclotomic polynomials from the smallest order n, we have the following.

$$\begin{aligned}
&\Phi_1(x) = x - 1, && \Phi_2(x) = x + 1, && \Phi_3(x) = x^2 + x + 1, \\
&\Phi_4(x) = x^2 + 1, && \Phi_5(x) = x^4 + x^3 + x^2 + x + 1, && \Phi_6(x) = x^2 - x + 1, \ldots
\end{aligned}$$

As seen above, the degree of Φ_n is given by $\phi(n)$. A fundamental relation involving cyclotomic polynomials is

$$\prod_{i|n} \Phi_i(x) = x^n - 1. \tag{7}$$

It is important that there are the following relations for any prime l and integer n.

$$\Phi_l(x) = \sum_{i=0}^{l-1} x^i, \tag{8}$$

$$\Phi_{ln}(x) = \Phi_n(x^l)/\Phi_n(x). \tag{9}$$

3.2 The structure of final exponentiation

The final exponentiation is a powering $(p^k - 1)/r$ in $\mathbb{F}_{p^k}^*$. To achieve a fast final exponentiation, the exponent of the final exponentiation is typically decomposed as follows:

$$\frac{p^k - 1}{r} = \left(\frac{p^k - 1}{\Phi_k(p)}\right) \cdot \left(\frac{\Phi_k(p)}{r}\right), \tag{10}$$

where Φ_k is the k-th cyclotomic polynomial. It is possible to represent the first part as $(p^k - 1)/\Phi_k(p) = \sum e_i p_i$ with small integers e_i from the property of the cyclotomic polynomial given in Eq. (7). Thus, the first part can be computed by using several p^i-th power Frobenius endomorphisms, multiplications, squarings, and inversion in $\mathbb{F}_{p^k}^*$. Thus, the first part is called the easy part. After raising to the easy part, we can work on a cyclotomic subgroup $G_{\Phi_k(p)}$ of $\mathbb{F}_{p^k}^*$ of order $\Phi_k(p)$ in which several efficient arithmetics are available corresponding to k. For any k, it is trivial that there are low-cost inversions in $G_{\Phi_k(p)}$. For $2 \mid k$ especially $6 \mid k$, efficient squarings are described in [32, 14, 21]. However, the second part, i.e., $d = \Phi_k(p)/r$, is more difficult to compute than the easy part and is called the hard part. To reduce the computational complexity, certain optimization techniques are typically applied for the hard part.

3.3 The existence optimizations of hard part

For the pairings with a family of pairing-friendly curves, the parameters p, r, and t are specified by polynomials $p(x)$, $r(x)$, and $t(x)$, respectively. Then, the exponent of the final exponentiation is denoted by $(p(x)^k - 1)/r(x)$ where the hard part is also denoted as $d(x) = \Phi_k(p(x))/r(x)$. For such the hard part, there are the following major optimization techniques.

(i) $p(x)$-adic expansion method. In [30], Scott et al. gave a systematic method to reduce the computational complexity of the hard part by representing $d(x)$ to be the polynomial in base $p(x)$ from the observation that $p(x)$-th powering in the finite field is efficiently computed by the Frobenius endomorphism. In the context, $d(x)$ can be represented as $d(x) = d_0(x) + d_1(x)p(x) + \cdots + d_{k'-1}(x)p^{k'-1}(x)$ where k' is the value of Euler's totient function by k, i.e., $k' = \phi(k)$, and $d_i(x)$ for $0 \leq i \leq k' - 1$ are polynomials in base x. Assuming f is an element after raising to the power of the easy part, one can find short vectorial addition chains to compute $f \mapsto f^{d(x)} = f^{d_0(x)} \cdot (f^{d_1(x)})^{p(x)} \cdots (f^{d_{k'-1}(x)})^{p(x)^{k'-1}}$.

(ii) Lattice-based method. In [12], Fuentes-Castaneda et al. proposed to use a multiple $d'(x) = c(x)d(x)$ such that $r(x) \nmid c(x)$ and presented a lattice-based method for determining $d'(x)$ such that $f \mapsto f^{d'(x)}$ can be computed at least as efficiently as $f \mapsto f^{d(x)}$ applied [30]. An efficient $d'(x)$ can be found by constructing a rational matrix M' with dimensions $k' \times (k' \deg p(x))$ given as follows:

$$\begin{bmatrix} d(x) \\ xd(x) \\ \vdots \\ x^{k'-1}d(x) \end{bmatrix} = M' \left(\begin{bmatrix} 1 \\ p(x) \\ \vdots \\ p(x)^{k'-1} \end{bmatrix} \otimes \begin{bmatrix} 1 \\ x \\ \vdots \\ x^{\deg p(x)-1} \end{bmatrix} \right). \tag{11}$$

where $\otimes$ is a Kronecker product. Let us consider the integer matrix M constructed from M' as the unique matrix of which rows are multiples of the rows of M' such that the entries of M are integers, and the greatest common divisor of the set of entries is 1. Applying the LLL algorithm [24] to M, a matrix with small entries can be obtained. Then, small integer linear combinations of the basis of the matrix are heuristically examined with the hope of finding short addition chains with a trial-and-error search. It is considered that the lattice-based method can achieve efficient algorithms for many curves, however, it requires much efforts for finding one of the best choices of $d'(x)$. Note that Kim et al. also presented a similar method for any curves in [23].

(iii) Formula-based method. As one of the algorithmic approaches, in [18], Hayashida et al. provided a representation of $d(x)$ that is applicable for any families of curves by generalizing the method by Zhang et al. [34] For any family of curves given by $p(x)$, $r(x)$, and $T(x)$, they described that one can find polynomials $h_1(x)$, $h_2(x), T(x) \in \mathbb{Q}[x]$ such that

$$\begin{cases} p(x) &= h_1(x)r(x) + T(x), \\ r(x) &= \Phi_k(T(x))/h_2(x), \\ t(x) &= T(x) + 1. \end{cases} \tag{12}$$

This leads to the following formula for representing $d(x) = \Phi_k(p(x))/r(x)$.

$$d(x) = h_1(x) \left(\sum_{i=0}^{k'-1} \lambda_i(x) p(x)^i \right) + h_2(x). \tag{13}$$

Assuming $\Phi_k(x) = \sum_{i=0}^{k'} c_i x^i$ with integers c_i, $\lambda_i(x)$ is denoted as follows:

$$\lambda_i(x) = \begin{cases} c_n & \text{if } i = k' - 1, \\ T(x) \cdot \lambda_{i+1}(x) + c_{i+1} & \text{if } 0 \leq i < k' - 1. \end{cases} \tag{14}$$

Let $\tilde{d}(x) = sd(x)$ be a polynomial with the smallest integer s such that both $sh_1(x)$ and $sh_2(x)$ do not involve denominators. Then, one can construct an algorithm for computing the hard part $f \mapsto f^{\tilde{d}(x)}$ as seen in Algorithm 1. In the following, the details of each step in Algorithm 1 are described with the calculation costs.

Algorithm 1: Hard part computation [18]

Input: $f \in G_{\Phi_k(p)}$
Output: $f \mapsto f^{\tilde{d}(x)} \in \mu_r$
1 $u \leftarrow f^{sh_1(x)}, t \leftarrow f^{sh_2(x)}$;
2 $v_{n-1} = u^{c_n}$;
3 **for** $i = k' - 2$ *downto* 0 **do**
4 $\quad v_i \leftarrow v_{i+1}^{T(x)} \cdot u^{c_{i+1}}$;
5 $w \leftarrow v_0 \cdot t$;
6 **for** $i = 1$ *to* $k' - 1$ **do**
7 $\quad w \leftarrow w \cdot v_i^{p(x)^i}$;
return $w = f^{d'(x)}$;

- Step 1 computes $u = f^{sh_1(x)}$ and $t = f^{sh_2(x)}$, which approximately takes $\max(\deg sh_1, \deg sh_2)$-times exponentiation by x in $\mathbb{F}_{p^k}^*$.
- Steps 2–4 compute $v_i = u^{\lambda_i(x)}$ for $0 \leq i \leq k'-2$, which take $(k'-1)\cdot \deg T$-times exponentiation by x in $\mathbb{F}_{p^k}^*$ with certain number of multiplications and cyclotomic inversions.
- Steps 5 set $w = v_0 \cdot t$ and computes $w = w \cdot \prod_{i=1}^{n-1} {v_i}^{p(x)^i}$, which take n-times multiplications and $p(x)^i$-th power Frobenius endomorphisms for $1 \leq i \leq k' - 1$ in $\mathbb{F}_{p^k}^*$.

As seen in Algorithm 1, the formula given by Hayashida et al. [18] results in an efficient final exponentiation for the families of curves with $\deg T = 1$, e.g., the BLS family. However, their formula might be not effective for the other families with $\deg T > 1$. The similar results are also found by Shirase and Nanjo in [31].

4 The Proposed Formulas of Final Exponentiation for Curves with Any Prime Embedding Degrees

In this section, the authors propose new formulas for representing the hard part of the final exponentiation for curves with any prime embedding degrees k.

4.1 The cyclotomic families of curves with prime k

The authors construct pairing-friendly curves with prime k by using cyclotomic families of curves with $k \equiv 1, 5 \pmod 6$. According to Construction 6.6 of [11], the families have the specific parameterizations given as follows:

- $k \equiv 1 \pmod 6$

$$\begin{cases} p(x) &= \frac{1}{3}(x+1)^2(x^{2k} - x^k + 1) - x^{2k+1}, \\ r(x) &= \Phi_{6k}(x), \\ t(x) &= -x^{k+1} + x + 1. \end{cases} \tag{15}$$

- $k \equiv 5 \pmod 6$

$$\begin{cases} p(x) &= \frac{1}{3}(x^2 - x + 1)(x^{2k} - x^k + 1) + x^{k+1}, \\ r(x) &= \Phi_{6k}(x), \\ t(x) &= x^{k+1} + 1. \end{cases} \tag{16}$$

Let x_0 be an integer seed making $p(x_0)$ and $r(x_0)$ being primes. Then, there is an elliptic curve E with $\#E(\mathbb{F}_{p(x_0)}) = p(x_0) + 1 - t(x_0)$ which is divisible by $r(x_0)$. Since $r(x_0)$ divides $p(x_0)^k - 1$ with the smallest integer k, E has an embedding degree k with respect to $r(x_0)$. The concrete values of x_0 for generating curves with $k = 13$ and 19 are provided in [8]. Such curves with $k = 13$ and 19 are named `BW13-P310` and `BW19-P286`, respectively.

4.2 The proposed formulas of the hard part for any prime k

For the cyclotomic families of curves with prime k of $k \equiv 1, 5 \pmod 6$, the exponent of the final exponentiation can be written as follows:

$$\frac{p(x)^k - 1}{r(x)} = \left(\frac{p(x)^k - 1}{\Phi_k(p(x))}\right) \cdot \left(\frac{\Phi_k(p(x))}{r(x)}\right) = (p(x) - 1) \cdot \left(\frac{\Phi_k(p(x))}{r(x)}\right), \tag{17}$$

where $p(x) - 1$ and $d(x) = \Phi_k(p(x))/r(x)$ are easy and hard parts, respectively. It is considered that the previous formula given by Hayashida et al. in [18] might not result in efficient algorithms for computing the hard part since the families of curves have the property $\deg T = \deg t > 1$.

To obtain better formulas than [18], the authors apply the lattice-based method [12] and observe results of the representations of the hard part given by $d'(x) = c(x)d(x)$ with a polynomial $c(x)$ for the cases of small prime k. More actually say, the authors suppose that $k' = k-1$, $d(x) = \Phi_k(x)/r(x)$, and M is a matrix with dimensions $k' \times \phi(k) \deg p(x)$ given by

$$\begin{bmatrix} 3d(x) \\ 3xd(x) \\ \vdots \\ 3x^{k'-1}d(x) \end{bmatrix} = M \left(\begin{bmatrix} 1 \\ p(x) \\ \vdots \\ p(x)^{k'-1} \end{bmatrix} \otimes \begin{bmatrix} 1 \\ x \\ \vdots \\ x^{\deg p(x)-1} \end{bmatrix} \right), \tag{18}$$

where 3 is the smallest integer for the coefficient of $x^i d(x)$ such that M has all integer entries and the greatest common divisor of the set of entries is 1. The authors apply the LLL algorithm to M and obtain a matrix. Then, the authors observe the 1st row of the matrix which indicates one of the representations of the hard parts $d'(x) = c(x)d(x)$ for the cases of small primes k. As a result of the observation, the authors find the following new formulas for the hard part of the final exponentiation for the cyclotomic families of curves with any prime k.

Theorem 1. Let n be any positive integer and let $k = 6n+1$. Let $p(x), r(x), t(x)$ be polynomials in $\mathbb{Q}[x]$ where $(p(x), r(x), t(x))$ is the cyclotomic family of pairing-friendly curves with $k \equiv 1 \pmod 6$ given in Eq. (15). Let $d(x) = \Phi_k(p(x))/r(x)$ and $d'(x) = c(x)d(x)$ where $c(x)$ is a polynomial defined as follows:

$$c(x) = (x^{6n} - 1)/\Phi_6(x). \tag{19}$$

If k is a prime, $d'(x)$ is represented as follows:

$$d'(x) = \sum_{i=0}^{6n-1} \left(x^{6n}\Phi_6(x) - 3 + \mu_{6n-1-i}(x)\right) p(x)^i, \tag{20}$$

where $\mu_s(x)$ with $s = 6n - 1 - i$ is a polynomial defined as follows:

$$\mu_s(x) = \begin{cases} -x^s\Phi_6(x) & \text{if } s \equiv 0 \pmod 6, \\ x^{6n+1+s}\Phi_6(x) - x^s\Phi_6(x) - 3x^{s+1} & \text{if } s \equiv 1 \pmod 6, \\ x^{6n+1+s}\Phi_6(x) - 3x^{s+1} & \text{if } s \equiv 2 \pmod 6, \\ x^s\Phi_6(x) & \text{if } s \equiv 3 \pmod 6, \\ -x^{6n+1+s}\Phi_6(x) + x^s\Phi_6(x) + 3x^{s+1} & \text{if } s \equiv 4 \pmod 6, \\ -x^{6n+1+s}\Phi_6(x) + 3x^{s+1} & \text{if } s \equiv 5 \pmod 6. \end{cases} \tag{21}$$

Proof of Theorem 1. Please refer to App. A. □

Theorem 2. Let n be any positive integer and let $k = 6n-1$. Let $p(x), r(x), t(x)$ be polynomials in $\mathbb{Q}[x]$ where $(p(x), r(x), t(x))$ is the cyclotomic family of pairing-friendly curves with $k \equiv 5 \pmod 6$ given in Eq. (16). Let $d(x) = \Phi_k(p(x))/r(x)$ and $d'(x) = c(x)d(x)$ where $c(x)$ is a polynomial defined as follows:

$$c(x) = 3(x^{6n-1} - x^{6n-2} - 1)/\Phi_6(x). \tag{22}$$

If k is a prime, $d'(x)$ is represented as follows:

$$d'(x) = \sum_{i=0}^{6n-3} \left(-x^{6n-2}\Phi_6(x) - 3 + \nu_{6n-3-i}(x)\right) p(x)^i, \tag{23}$$

where $\nu_s(x)$ with $s = 6n-3-i$ is a polynomial defined as follows:

$$\nu_s(x) = \begin{cases} x^{6n-1+s}\Phi_6(x) - x^s\Phi_6(x) + 3x^{s+1} & \text{if } s \equiv 0 \pmod 6, \\ -x^s\Phi_6(x) & \text{if } s \equiv 1 \pmod 6, \\ -x^{6n-1+s}\Phi_6(x) - 3x^{s+1} & \text{if } s \equiv 2 \pmod 6, \\ -x^{6n-1+s}\Phi_6(x) + x^s\Phi_6(x) - 3x^{s+1} & \text{if } s \equiv 3 \pmod 6, \\ x^s\Phi_6(x) & \text{if } s \equiv 4 \pmod 6, \\ x^{6n-1+s}\Phi_6(x) + 3x^{s+1} & \text{if } s \equiv 5 \pmod 6. \end{cases} \tag{24}$$

Proof of Theorem 2. Please refer to App. B. □

4.3 The proposed formulas for small primes k

Theorem 1 and 2 can produce the following specific formulas of the hard part $d'(x) = d(x)c(x)$ for the cyclotomic families of curves with prime k such as $k = 5, 7, 11, 13, 17$, and 19.

Example 1. The cyclotomic family of curves with $k = 5$ has parameterizations given by

$$\begin{cases} p(x) &= \frac{1}{3}(x^2 - x + 1)(x^{10} - x^5 + 1) + x^6, \\ r(x) &= \Phi_{30}(x), \\ t(x) &= x^6 + 1. \end{cases} \tag{25}$$

The formula of the hard part is given by $d'(x) = c(x)\Phi_5(p(x))/r(x) = \sum_{i=0}^{3} d'_i(x)p^i$ where $c(x) = 3(x^3 - x - 1)$ and $d_i(x)$ for $0 \le i \le 3$ are polynomials given as follows:

$$\begin{cases} d'_3(x) &= -x^4\Phi_6(x) - 3 + x^5\Phi_6(x) - \Phi_6(x) + 3x, \\ d'_2(x) &= -x^4\Phi_6(x) - 3 - x\Phi_6(x), \\ d'_1(x) &= -x^4\Phi_6(x) - 3 - x^7\Phi_6(x) - 3x^3, \\ d'_0(x) &= -x^4\Phi_6(x) - 3 - x^8\Phi_6(x) + x^3\Phi_6(x) - 3x^4. \end{cases} \tag{26}$$

Example 2. The cyclotomic family of curves with $k = 7$ has parameterizations given by

$$\begin{cases} p(x) &= \frac{1}{3}(x + 1)^2(x^{14} - x^7 + 1) - x^{15}, \\ r(x) &= \Phi_{42}(x), \\ t(x) &= -x^8 + x + 1. \end{cases} \tag{27}$$

The formula of the hard part is given by $d'(x) = c(x)\Phi_7(p(x))/r(x) = \sum_{i=0}^{5} d'_i(x)p(x)^i$ where $c(x) = 3(x^4 + x^3 - x - 1)$ and $d'_i(x)$ for $0 \le i \le 5$ are polynomials given as follows:

$$\begin{cases} d'_5(x) &= x^6\Phi_6(x) - 3 - \Phi_6(x), \\ d'_4(x) &= x^6\Phi_6(x) - 3 + x^8\Phi_6(x) - x\Phi_6(x) - 3x^2, \\ d'_3(x) &= x^6\Phi_6(x) - 3 + x^9\Phi_6(x) - 3x^3, \\ d'_2(x) &= x^6\Phi_6(x) - 3 + x^3\Phi_6(x), \\ d'_1(x) &= x^6\Phi_6(x) - 3 - x^{11}\Phi_6(x) + x^4\Phi_6(x) + 3x^5, \\ d'_0(x) &= x^6\Phi_6(x) - 3 - x^{12}\Phi_6(x) + 3x^6. \end{cases} \tag{28}$$

Example 3. The cyclotomic family of curves with $k = 11$ has parameterizations given by

$$\begin{cases} p(x) &= \frac{1}{3}(x^2 - x + 1)(x^{22} - x^{11} + 1) + x^{12}, \\ r(x) &= \Phi_{66}(x), \\ t(x) &= x^{12} + 1. \end{cases} \tag{29}$$

The formula of the hard part is given as $d'(x) = c(x)d(x) = \sum_{i=0}^{9} d'_i(x)p(x)^i$ where $c(x) = 3(x^9 - x^7 - x^6 + x^4 + x^3 - x - 1)$ and $d'_i(x)$ for $0 \leq i \leq 9$ are polynomials given as follows:

$$\begin{cases} d'_9(x) &= -x^{10}\Phi_6(x) - 3 + x^{11}\Phi_6(x) - \Phi_6(x) + 3x, \\ d'_8(x) &= -x^{10}\Phi_6(x) - 3 - x\Phi_6(x), \\ d'_7(x) &= -x^{10}\Phi_6(x) - 3 - x^{13}\Phi_6(x) - 3x^3, \\ d'_6(x) &= -x^{10}\Phi_6(x) - 3 - x^{14}\Phi_6(x) + x^3\Phi_6(x) - 3x^4, \\ d'_5(x) &= -x^{10}\Phi_6(x) - 3 + x^4\Phi_6(x), \\ d'_4(x) &= -x^{10}\Phi_6(x) - 3 + x^{16}\Phi_6(x) + 3x^6, \\ d'_3(x) &= -x^{10}\Phi_6(x) - 3 + x^{17}\Phi_6(x) - x^6\Phi_6(x) + 3x^7, \\ d'_2(x) &= -x^{10}\Phi_6(x) - 3 - x^7\Phi_6(x), \\ d'_1(x) &= -x^{10}\Phi_6(x) - 3 - x^{19}\Phi_6(x) - 3x^9, \\ d'_0(x) &= -x^{10}\Phi_6(x) - 3 - x^{20}\Phi_6(x) + x^9\Phi_6(x) - 3x^{10}. \end{cases} \tag{30}$$

Example 4. The cyclotomic family of curves with $k = 13$ has parameterizations given by

$$\begin{cases} p(x) &= \frac{1}{3}(x+1)^2(x^{26} - x^{13} + 1) - x^{27}, \\ r(x) &= \Phi_{78}(x), \\ t(x) &= -x^{14} + x + 1. \end{cases} \tag{31}$$

The formula of the hard part is given as $d'(x) = \sum_{i=0}^{11} d'_i(x)p(x)^i$ where $c(x) = 3(x^{10} + x^9 - x^7 - x^6 + x^4 + x^3 - x - 1)$ and $d'_i(x)$ for $0 \leq i \leq 11$ are polynomials given as follows:

$$\begin{cases} d'_{11}(x) &= x^{12}\Phi_6(x) - 3 - \Phi_6(x), \\ d'_{10}(x) &= x^{12}\Phi_6(x) - 3 + x^{14}\Phi_6(x) - x\Phi_6(x) - 3x^2, \\ d'_9(x) &= x^{12}\Phi_6(x) - 3 + x^{15}\Phi_6(x) - 3x^3, \\ d'_8(x) &= x^{12}\Phi_6(x) - 3 + x^3\Phi_6(x), \\ d'_7(x) &= x^{12}\Phi_6(x) - 3 - x^{17}\Phi_6(x) + x^4\Phi_6(x) + 3x^5, \\ d'_6(x) &= x^{12}\Phi_6(x) - 3 - x^{18}\Phi_6(x) + 3x^6, \\ d'_5(x) &= x^{12}\Phi_6(x) - 3 - x^6\Phi_6(x), \\ d'_4(x) &= x^{12}\Phi_6(x) - 3 + x^{20}\Phi_6(x) - x^7\Phi_6(x) - 3x^8, \\ d'_3(x) &= x^{12}\Phi_6(x) - 3 + x^{21}\Phi_6(x) - 3x^9, \\ d'_2(x) &= x^{12}\Phi_6(x) - 3 + x^9\Phi_6(x), \\ d'_1(x) &= x^{12}\Phi_6(x) - 3 - x^{23}\Phi_6(x) + x^{10}\Phi_6(x) + 3x^{11}, \\ d'_0(x) &= x^{12}\Phi_6(x) - 3 - x^{24}\Phi_6(x) + 3x^{12}. \end{cases} \tag{32}$$

Example 5. The cyclotomic family of curves with $k = 17$ has parameterizations given by

$$\begin{cases} p(x) &= \frac{1}{3}(x^2 - x + 1)(x^{34} - x^{17} + 1) + x^{18}, \\ r(x) &= \Phi_{102}(x), \\ t(x) &= x^{18} + 1. \end{cases} \tag{33}$$

The formula of the hard part is given as $d'(x) = \Phi_{17}(p(x))/r(x) = \sum_{i=0}^{15} d'_i(x)p(x)^i$ where $c(x) = 3(x^{15} - x^{13} - x^{12} + x^{10} + x^9 - x^7 - x^6 + x^4 + x^3 - x - 1)$ and $d_i(x)$ for $0 \leq i \leq 15$ are polynomials

given as follows:

$$\begin{cases} d'_{15}(x) &= -x^{16}\Phi_6(x) - 3 + x^{17}\Phi_6(x) - \Phi_6(x) + 3x, \\ d'_{14}(x) &= -x^{16}\Phi_6(x) - 3 - x\Phi_6(x), \\ d'_{13}(x) &= -x^{16}\Phi_6(x) - 3 - x^{19}\Phi_6(x) - 3x^3, \\ d'_{12}(x) &= -x^{16}\Phi_6(x) - 3 - x^{20}\Phi_6(x) + x^3\Phi_6(x) - 3x^4, \\ d'_{11}(x) &= -x^{16}\Phi_6(x) - 3 + x^4\Phi_6(x), \\ d'_{10}(x) &= -x^{16}\Phi_6(x) - 3 + x^{22}\Phi_6(x) + 3x^6, \\ d'_9(x) &= -x^{16}\Phi_6(x) - 3 + x^{23}\Phi_6(x) - x^6\Phi_6(x) + 3x^7, \\ d'_8(x) &= -x^{16}\Phi_6(x) - 3 - x^7\Phi_6(x), \\ d'_7(x) &= -x^{16}\Phi_6(x) - 3 - x^{25}\Phi_6(x) - 3x^9, \\ d'_6(x) &= -x^{16}\Phi_6(x) - 3 - x^{26}\Phi_6(x) + x^9\Phi_6(x) - 3x^{10}, \\ d'_5(x) &= -x^{16}\Phi_6(x) - 3 + x^{10}\Phi_6(x), \\ d'_4(x) &= -x^{16}\Phi_6(x) - 3 + x^{28}\Phi_6(x) + 3x^{12}, \\ d'_3(x) &= -x^{16}\Phi_6(x) - 3 + x^{29}\Phi_6(x) - x^{12}\Phi_6(x) + 3x^{13}, \\ d'_2(x) &= -x^{16}\Phi_6(x) - 3 - x^{13}\Phi_6(x), \\ d'_1(x) &= -x^{16}\Phi_6(x) - 3 - x^{31}\Phi_6(x) - 3x^{15}, \\ d'_0(x) &= -x^{16}\Phi_6(x) - 3 - x^{32}\Phi_6(x) + x^{15}\Phi_6(x) - 3x^{16}. \end{cases} \tag{34}$$

Example 6. The cyclotomic family of curves with $k = 19$ has parameterizations given by

$$\begin{cases} p(x) &= \frac{1}{3}(x+1)^2(x^{38} - x^{19} + 1) - x^{39}, \\ r(x) &= \Phi_{114}(x), \\ t(x) &= -x^{20} + x + 1. \end{cases} \tag{35}$$

The formula of the hard part is given as $d'(x) = \sum_{i=0}^{19} d'(x)p(x)^i$ where $c(x) = 3(x^{16} + x^{15} - x^{13} - x^{12} + x^{10} + x^9 - x^7 - x^6 + x^4 + x^3 - x - 1)$ and $d'_i(x)$ for $0 \leq i \leq 19$ are polynomials given as follows:

$$\begin{cases} d'_{17}(x) &= x^{18}\Phi_6(x) - 3 - \Phi_6(x), \\ d'_{16}(x) &= x^{18}\Phi_6(x) - 3 + x^{20}\Phi_6(x) - x\Phi_6(x) - 3x^2, \\ d'_{15}(x) &= x^{18}\Phi_6(x) - 3 + x^{21}\Phi_6(x) - 3x^3, \\ d'_{14}(x) &= x^{18}\Phi_6(x) - 3 + x^3\Phi_6(x), \\ d'_{13}(x) &= x^{18}\Phi_6(x) - 3 - x^{23}\Phi_6(x) + x^4\Phi_6(x) + 3x^5, \\ d'_{12}(x) &= x^{18}\Phi_6(x) - 3 - x^{24}\Phi_6(x) + 3x^6, \\ d'_{11}(x) &= x^{18}\Phi_6(x) - 3 - x^6\Phi_6(x), \\ d'_{10}(x) &= x^{18}\Phi_6(x) - 3 + x^{26}\Phi_6(x) - x^7\Phi_6(x) - 3x^8, \\ d'_9(x) &= x^{18}\Phi_6(x) - 3 + x^{27}\Phi_6(x) - 3x^9, \\ d'_8(x) &= x^{18}\Phi_6(x) - 3 + x^9\Phi_6(x), \\ d'_7(x) &= x^{18}\Phi_6(x) - 3 - x^{29}\Phi_6(x) + x^{10}\Phi_6(x) + 3x^{11}, \\ d'_6(x) &= x^{18}\Phi_6(x) - 3 - x^{30}\Phi_6(x) + 3x^{12}, \\ d'_5(x) &= x^{18}\Phi_6(x) - 3 - x^{12}\Phi_6(x), \\ d'_4(x) &= x^{18}\Phi_6(x) - 3 + x^{32}\Phi_6(x) - x^{13}\Phi_6(x) - 3x^{14}, \\ d'_3(x) &= x^{18}\Phi_6(x) - 3 + x^{33}\Phi_6(x) - 3x^{15}, \\ d'_2(x) &= x^{18}\Phi_6(x) - 3 + x^{15}\Phi_6(x), \\ d'_1(x) &= x^{18}\Phi_6(x) - 3 - x^{35}\Phi_6(x) + x^{16}\Phi_6(x) + 3x^{17}, \\ d'_0(x) &= x^{18}\Phi_6(x) - 3 - x^{36}\Phi_6(x) + 3x^{18}. \end{cases} \tag{36}$$

As for the above cases of $k = 5, 7, 11, 13, 17$, and 19, the authors confirm that the formulas are exactly one of the same representations of the hard part $d'(x) = c(x)d(x)$ given by the lattice-based method [12]. For the cases of any k, there is a possibility that the proposed formulas give rise to one of the same representations as [12]. This also means that there is a possibility that the proposed formulas lead to as efficient algorithms for computing the hard part as ones given by [12].

5 Applications

According to the formulas of the hard part, the authors construct the algorithm for computing the hard part for the cyclotomic families of curves with any primes k. The authors also provide

the calculation cost estimations of the final exponentiation for the pairings on concrete curves with $k = 13$ and 19. In the following, the calculation costs of the exponentiation by s, multiplication, cubing, p^i-th power Frobenius endomorphism in $\mathbb{F}_{p^k}^*$, and inversion in the cyclotomic subgroup of $\mathbb{F}_{p^k}^*$ of order $\Phi_k(p)$ are denoted as u_k^s, m_k, c_k, f_k^i, and i_{ck}, respectively.

5.1 Algorithms for computing the hard part for any prime k

The authors construct algorithms for computing the hard part based on the formulas given in Theorem 1 and 2. According to the existence curves given in [8], the authors consider the case of negative x in this paper. To reduce the number of multiplications and cyclotomic inversions, the authors adopt the formulas of $d'(x) = c(x)\Phi_k(x)/r(x)$ multiplied by $-(p(x)-1)$. This results in simpler representations of the hard part as given in the following corollaries.

Corollary 1. For the cyclotomic families of curves with any prime $k = 6n+1$, let $p(x), d'(x), \mu(x)$ be a polynomial as defined in Theorem 1. Then, $\tilde{d}(x) = -(p(x)-1)d'(x)$ is denoted as follows:

$$\tilde{d}(x) = (-x^{6n}\Phi_6(x)+3)(p(x)^{6n}-1) - \sum_{i=0}^{6n-1} \mu_{6n-1-i}(x)p(x)^i(p(x)-1). \tag{37}$$

Corollary 2. For the cyclotomic families of curves with any prime $k = 6n-1$, let $p(x), d'(x), \nu(x)$ be a polynomial as defined in Theorem 2. Then, $\tilde{d}(x) = -(p(x)-1)d'(x)$ is denoted as follows:

$$\tilde{d}(x) = (x^{6n-2}\Phi_6(x)+3)(p(x)^{6n-2}-1) - \sum_{i=0}^{6n-3} \nu_{6n-3-i}(x)p(x)^i(p(x)-1). \tag{38}$$

The formulas of $\tilde{d}(x) = -(p(x)-1)d'(x)$ lead to algorithms for computing $f \mapsto f^{d\tilde{(x)}}$ for the cyclotomic families of curves with any prime k of $k = 6n+1$ and $k = 6n-1$ as in Algorithms 2 and 3, respectively. In the following, the details of each step in the proposed algorithms are described with the calculation costs.

- Algorithm 2 for computing the hard part for the cases of any prime $k = 6n+1$:
  - Steps 1–3 compute $f_i \leftarrow f^{(-x)^i}$ for $1 \le i \le 6n$, which take $6nu_k^{-x}$.
  - Steps 4–6 compute $g_i \leftarrow f^{(-x)^{6i+j}\Phi_6(x)}$ where $j \in \{0,1,3,4\}$ for $0 \le i \le n-1$, which take $6nm_k$.
  - Steps 7–9 compute $g_i \leftarrow f^{(-x)^{6n-2+i}\Phi_6(x)}$ for $1 \le i \le 6n+2$, which take $(6n+2)u_k^{-x}$.
  - Step 10 computes $t \leftarrow f^{(-x^{6n}\Phi_6(x)+3)(p(x)^{6n}-1)}$, which takes $2m_k + c_k + 2i_{ck} + f_k^6$.
  - Steps 11–17 compute $v_{6i+j} \leftarrow f^{-\mu_{6i+j}(x)}$ where $j = \{0,1,2,3,4,5\}$ for $0 \le i \le n-1$, which take $n(6m_k + 4c_k + 4i_{ck})$.
  - Steps 18–20 compute $w \leftarrow \prod_{i=0}^{6n-1} v_{6n-1-i}^{p(x)^i}$, which take $(6n-1)m_k + \sum_{i=1}^{6n-1} f_k^i$.
  - Step 21 computes $w \leftarrow t \cdot w^{p(x)-1}$, which takes $2m_k + i_{ck} + f_k^1$.

  The calculation cost of the hard part is given by $(12n+2)u_k^{-x} + (18n+3)m_k + (4n+1)c_k + (4n+3)i_{ck} + \sum_{i=1}^{6n-1} f_k^i + f_k^{6n} + f_k^1$.

- Algorithm 3 for computing the hard part for the cases of any prime $k = 6n-1$:
  - Steps 1–3 compute $f_i \leftarrow f^{(-x)^i}$ for $1 \le i \le 6n-2$, which take $(6n-2)u_k^{-x}$.
  - Steps 4–8 compute $g_j \leftarrow f^{(-x)^j\Phi_6(x)}$ where $j \in \{0,1\}$, $g_i \leftarrow f^{(-x)^{6i+j}\Phi_6(x)}$ where $j \in \{0,1,3,4\}$ for $1 \le i \le n-1$, and $g_{6n-4} \leftarrow f^{x^{6n-4}\Phi_6(x)}$, which take $5m_k + (n-1)6m_k = (6n-1)m_k$.
  - Steps 9–10 compute $g_i \leftarrow f^{(-x)^{6n-4+i}\Phi_6(x)}$ for $1 \le i \le 6n$, which take $6nu_k^{-x}$.
  - Step 11 computes $t \leftarrow f^{(x^{6n-2}\Phi_6(x)+3)(p(x)^{6n-2}-1)}$, which takes $2m_k + c_k + i_{ck} + f_k^{6n-2}$.

Algorithm 2: Proposed hard part computation for curves with any prime k of $k = 6n+1$.

Input: $f \in G_{\Phi_k(p)}$
Output: $f^{\tilde{d}(x)} = f^{-(p(x)-1)d'(x)} \in \mu_r$

1 $f_0 \leftarrow f$;
2 **for** $i = 1$ *to* $6n$; **do**
3 $\quad f_i \leftarrow f_{i-1}^{-x}$; $\quad //u_k^{-x}$
4 **for** $i = 0$ *to* $n-1$; **do**
5 $\quad t \leftarrow f_{6i+2} \cdot f_{6i+1}$, $g_{6i} \leftarrow t \cdot f_{6i}$, $g_{6i+1} \leftarrow t \cdot f_{6i+3}$; $\quad //3m_k$
6 $\quad t \leftarrow f_{6i+5} \cdot f_{6i+4}$, $g_{6i+3} \leftarrow t \cdot f_{6i+3}$, $g_{6i+4} \leftarrow t \cdot f_{6i+6}$; $\quad //3m_k$
7 $g_{6n-1} \leftarrow g_{6n}^{-x}$, $g_{6n} \leftarrow g_{6n-1}^{-x}$; $\quad //2u_k^{-x}$
8 **for** $i = 1$ *to* $6n$; **do**
9 $\quad g_{6n+i} \leftarrow g_{6n+i-1}^{-x}$; $\quad //u_k^{-x}$
10 $t \leftarrow g_{6n}^{-1} \cdot f^3$, $t \leftarrow t^{p(x)^6} \cdot t^{-1}$; $\quad //2m_k + c_k + 2i_{ck} + f_k^6$
11 **for** $i = 0$ *to* $n-1$; **do**
12 $\quad v_{6i} \leftarrow g_{6i}$; $\quad //0$
13 $\quad v_{6i+1} \leftarrow (g_{6n+6i+2} \cdot g_{6i+1})^{-1} \cdot f_{6i+2}^3$; $\quad //2m_k + c_k + i_{ck}$
14 $\quad v_{6i+2} \leftarrow g_{6n+6i+3} \cdot f_{6i+3}^{-3}$; $\quad //m_k + c_k + i_{ck}$
15 $\quad v_{6i+3} \leftarrow g_{6i+3}$; $\quad //0$
16 $\quad v_{6i+4} \leftarrow (g_{6n+6i+5} \cdot g_{6i+4})^{-1} \cdot f_{6i+5}^3$; $\quad //2m_k + c_k + i_{ck}$
17 $\quad v_{6i+5} \leftarrow g_{6n+6i+6} \cdot f_{6i+6}^{-3}$; $\quad //m_k + c_k + i_{ck}$
18 $w \leftarrow v_{6n-1}$;
19 **for** $i = 1$ *to* $6n-1$; **do**
20 $\quad w \leftarrow w \cdot v_{6n-1-i}^{p(x)^i}$; $\quad //m_k + f_k^i$
21 $w \leftarrow t \cdot w^{p(x)} \cdot w^{-1}$; $\quad //2m_k + i_{ck} + f_k^1$
Return w;

- Steps 12–20 compute $v_j \leftarrow f^{-\nu_j(x)}$ where $j = \{0,1,2,3\}$ and $v_{6i+j} \leftarrow f^{-\nu_{6i+j}(x)}$ where $j = \{-2,-1,0,1,2,3\}$ for $0 \le i \le n-1$, which take $5m_k + 3c_k + 2i_{ck} + (n-1)(6m_k + 4c_k + 4i_{ck}) = (6n-1)m_k + (4n-1)c_k + (4n-2)i_{ck}$.
- Steps 21–23 compute $w \leftarrow \prod_{i=0}^{6n-3} v_{6n-3-i}^{p(x)^i}$, which take $(6n-3)m_k + \sum_{i=1}^{6n-3} f_k^i$.
- Step 24 computes $w \leftarrow t \cdot w^{p(x)-1}$, which takes $2m_k + i_{ck} + f_k^1$.

The calculation costs of the hard part is given by $(12n-2)u_k^{-x} + (18n-1)m_k + 4nc_k + 4ni_{ck} + \sum_{i=1}^{6n-3} f_k^i + f_k^{6n-2} + f_k^1$.

On the other hand, as described in Sect. 3.3, Algorithm 1 for computing the hard part given by the formula [18] takes at least $(k'-1)\deg Tu_k^x$ for any family of curves with a certain k. Note that k' is the value of Euler's totient function by k. For the cyclotomic family of curves with a prime $k = 6n+1$, since $k' = 6n$ and $T(x) = -x^{6n+2} + x$, it requires at least $(6n-1)(6n+2)u_k^x = (36n^2 + 6n - 2)u_k^x$ for computing the hard part. Similarly for the case of a prime $k = 6n-1$, since $k' = 6n-2$ and $T(x) = x^{6n}$, it requires at least $(6n-3)(6n)u_k^x = (36n^2 - 18n)u_k^x$. Since $u_k^x \approx u_k^{-x}$, this means that the previous algorithm has $O(n^2)$ complexity, but the proposed ones have $O(n)$. Therefore, the proposed algorithms would be better choices than the previous ones for the families of curves with prime k.

5.2 Calculation cost estimations for curves with $k = 13$ and 19

The authors estimate the calculation costs of the final exponentiation of the pairings on concrete curves in the cyclotomic families of curves with primes k. In this paper, the authors employ the seeds $x = x_0$ for generating concrete curves with $k = 13$ and 19 which are suggested for the pairing

Algorithm 3: Proposed hard part computation for curves with any prime k of $k = 6n-1$.

Input: $f \in G_{\Phi_k(p)}$
Output: $f^{\tilde{d}(x)} = f^{-(p(x)-1)d'(x)} \in \mu_r$

$f_0 \leftarrow f$;
for $i = 1$ *to* $6n-2$*;* **do**
  $f_i \leftarrow f_{i-1}^{-x}$; $//u_k^{-x}$
$t \leftarrow f_2 \cdot f_1$, $g_0 \leftarrow t \cdot f_0$, $g_1 \leftarrow t \cdot f_3$; $//3m_k$
for $i = 1$ *to* $n-1$*;* **do**
  $t \leftarrow f_{6i-2} \cdot f_{6i-3}$, $g_{6i-3} \leftarrow t \cdot f_{6i-1}$, $g_{6i-4} \leftarrow t \cdot f_{6i-4}$; $//3m_k$
  $t \leftarrow f_{6i+2} \cdot f_{6i+1}$, $g_{6i+1} \leftarrow t \cdot f_{6i+3}$, $g_{6i} \leftarrow t \cdot f_{6i}$; $//3m_k$
$g_{6n-4} \leftarrow f_{6n-2} \cdot f_{6n-3} \cdot f_{6n-4}$; $//2m_k$
for $i = 1$ *to* $6n$*;* **do**
  $g_{6n-4+i} \leftarrow g_{6n-5+i}^{-x}$; $//u_k^{-x}$
$t \leftarrow g_{6n-2} \cdot f^3$, $t \leftarrow t^{p(x)^{6n-2}} \cdot t^{-1}$; $//2m_k + c_k + i_{ck} + f_k^{6n-2}$
$v_0 \leftarrow g_0 \cdot g_{6n-1} \cdot f_1^3$, $v_1 \leftarrow g_1^{-1}$; $//2m_k + c_k + i_{ck}$
$v_2 \leftarrow (g_{6n+1} \cdot f_3^3)^{-1}$, $v_3 \leftarrow g_{6n+2} \cdot g_3 \cdot f_4^3$; $//3m_k + 2c_k + i_{ck}$
for $i = 1$ *to* $n-1$*;* **do**
  $v_{6i-2} \leftarrow g_{6i-2}^{-1}$; $//i_{ck}$
  $v_{6i-1} \leftarrow (g_{6n+6i-2} \cdot f_{6i}^3)^{-1}$; $//m_k + c_k + i_{ck}$
  $v_{6i} \leftarrow g_{6n-1+6i} \cdot g_{6i} \cdot f_{6i+1}^3$; $//2m_k + c_k$
  $v_{6i+1} \leftarrow g_{6i+1}^{-1}$; $//i_{ck}$
  $v_{6i+2} \leftarrow (g_{6n+6i+1} \cdot f_{6i+3}^3)^{-1}$; $//m_k + c_k + i_{ck}$
  $v_{6i+3} \leftarrow g_{6n+6i+2} \cdot g_{6i+3} \cdot f_{6i+4}^3$; $//2m_k + c_k$
$w \leftarrow v_{6n-3}$;
for $i = 1$ *to* $6n-3$*;* **do**
  $w \leftarrow w \cdot v_{6n-3-i}^{p(x)^i}$; $//m_k + f_k^i$
$w \leftarrow t \cdot w^{p(x)} \cdot w^{-1}$; $//2m_k + i_{ck} + f_k^1$
Return w;

at the 128-bit security level by Clarisse et al. in [8] and which are called `BW13-P310` and `BW19-P286`, respectively. The details of the parameters are presented in Table 2. According to [8], it could not be found seeds for generating curves with $k = 11$ and 17 for the pairings at the 128-bit security level.

The calculation costs of the arithmetics operations in $\mathbb{F}_{p^k}$ for $k = 13$ and 19 can be replaced with the cost of the multiplication in $\mathbb{F}_p$ which is denoted as m in Table 3. Note that the authors refer to [8, 15, 16, 27] and obtain Table 3. Then, the calculation costs of the proposed final exponentiation for `BW13-P310` and `BW19-P286` are estimated as follows:

- Calculation cost of the final exponentiation for `BW13-P310`: Since the seed is given by $x = x_0 = -2224 = -(2^{11} + 2^7 + 2^5 + 2^4)$, the calculation cost of the exponentiation by $-x$ can be considered as $u_{13}^{-x} = 3m_{13} + 11s_{13} = 3(59m) + 11(59m) = 826m$. According to Sect. 5.1, it is found that the hard part takes the calculation costs $26u_{13}^{-x} + 39m_{13} + 9c_{13} + 11i_{c13} + 13f_k^i = 26(826m) + 39(59m) + 9(118m) + 11(438m) + 13(12m) = 29813m$. Adding the calculation cost of the easy part $m_{13} + i_{13} + f_{13}^1 = (59m) + (489m) + (12m) = 560m$, the cost of the final exponentiation is obtained as $30373m$.

- Calculation cost of the final exponentiation for `BW19-P286`: Since $x = x_0 = -145 = -(2^7 + 2^4 + 2^0)$, the calculation cost of the exponentiation by $-x$ is given by $u_{19}^{-x} = 2m_{19} + 7s_{19} = 2(107m) + 7(107m) = 963m$. Similarly, the hard part requires the calculation costs $38u_{19}^{-x} + 57m_{19} + 13c_{19} + 15i_{c19} + 19f_{19}^i = 38(963m) + 57(107m) + 13(214m) + 15(1143m) + 19(18m) = 62962m$. Adding the calculation cost of the easy part $m_{19} + i_{19} + f_{19}^1 = (107m) + (1206m) + (18m) = 1331m$, the cost of the final exponentiation is obtained as $64293m$.

Table 2: Curves with $k = 13$ and 19 for the pairing at the 128-bit security level.

Curves (k, D, ρ)	Seed $x = x_0$	$\log_2 p(x_0)$	$\log_2 p(x_0)^k$	$\log_2 r(x_0)$
`BW13-P310` $(13, 3, 1.167)$	-2224	310	4027	267
`BW19-P286` $(19, 3, 1.111)$	-145	286	5427	259

Table 3: Calculation costs of the arithmetic operations in $\mathbb{F}_{p^k}^*$.

k	m_k	s_k	i_k	c_k	i_{ck}	f_k^i
13	$59m$	$59m$	$489m$	$118m$	$438m$	$12m$
19	$107m$	$107m$	$1206m$	$214m$	$1143m$	$18m$

Table 4: Calculation costs for the final exponentiation of the pairings at the 128-bit security level.

Curves	Clarisse et al. [8]	This work	Reductions [%]
`BW13-P310`	$57827m$	$30373m$	47.5
`BW19-P286`	$175746m$	$64293m$	63.4

Table 4 summarizes the results of the calculation cost estimations given by Clarisse et al. [8] and this work. Note that [8] refer to the method by Kim et al. [23] and estimated the calculation costs as $53834m + 9i_{13}$ and $160824 + 13i_{19}$ for `BW13-P310` and `BW19-P286`, respectively. Since the cyclotomic inversions are available during hard part computation, the authors revise the costs as $53834m+i_{13}+8i_{c13} = 53834m+(489m)+8(438m) = 57827m$ and $160824m+i_{19}+12i_{c19} = 160824m+(1206m) + 12(1143m) = 175746m$ for `BW13-P310` and `BW19-P286`, respectively. The estimation result shows that there are 47.5% and 63.4% reduction of the calculation costs for `BW13-P310` and `BW19-P286`, respectively. Thus, the proposed algorithms are considered to provide state-of-the-art computations for these curves. It is also expected that the performances of the pairings on these curves are significantly faster than previously considered.

6 Conclusion

In this paper, the authors presented formulas for generating the hard part representations of the final exponentiation for the cyclotomic family of curves with any prime k. For the small cases of k, the formulas give rise to one of the same hard part representations given by the lattice-based method [12]. The authors also constructed algorithms for computing the hard part which can be applied for any case of prime k. The algorithms have significantly lower complexity than ones given by Hayashida et al. [18] for any families of curves. At least for `BW13-P310` and `BW19-P286` for the pairing at the 128-bit security level, the proposed algorithms can achieve current state-of-the-art computations. As one of the future works, the authors would like to obtain similar results for the other families of curves.

Acknowledgment

This research was supported by JSPS KAKENHI Grant Numbers 19J2108613 and 19K11966.

References

[1] Razvan Barbulescu and Sylvain Duquesne. Updating key size estimations for pairings. *Journal of cryptology*, 32(4):1298–1336, 2019.

[2] Razvan Barbulescu, Nadia El Mrabet, and Loubna Ghammam. A taxonomy of pairings, their security, their complexity. Cryptology ePrint archive, report 2019/485, 2019. https://eprint.iacr.org/2019/485.

[3] Paulo SLM Barreto, Ben Lynn, and Michael Scott. Constructing elliptic curves with prescribed embedding degrees. In *International conference on security in communication networks*, pages 257–267. Springer, 2002.

[4] Paulo SLM Barreto and Michael Naehrig. Pairing-friendly elliptic curves of prime order. In *International workshop on selected areas in cryptography*, pages 319–331. Springer, 2005.

[5] Dan Boneh and Xavier Boyen. Short signatures without random oracles. In *International conference on the theory and applications of cryptographic techniques*, pages 56–73. Springer, 2004.

[6] Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano. Public key encryption with keyword search. In *International conference on the theory and applications of cryptographic techniques*, pages 506–522. Springer, 2004.

[7] Dan Boneh and Matt Franklin. Identity-based encryption from the weil pairing. In *Annual international cryptology conference*, pages 213–229. Springer, 2001.

[8] Rémi Clarisse, Sylvain Duquesne, and Olivier Sanders. Curves with fast computations in the first pairing group. In *International Conference on Cryptology and Network Security*, pages 280–298. Springer, 2020.

[9] Clifford Cocks and Richard G.E. Pinch. Identity-based cryptosystems based on the weil pairing. *Unpublished manuscript*, 2001.

[10] Emmanuel Fouotsa, Nadia El Mrabet, and Aminatou Pecha. Optimal ate pairing on elliptic curves with embedding degree $9, 15$ and 27. *Journal of groups, complexity, cryptology*, 12, issue 1, 2020. https://arxiv.org/abs/2002.11920v2.

[11] David Freeman, Michael Scott, and Edlyn Teske. A taxonomy of pairing-friendly elliptic curves. *Journal of cryptology*, 23(2):224–280, 2010.

[12] Laura Fuentes-Castaneda, Edward Knapp, and Francisco Rodríguez-Henríquez. Faster hashing to $\mathbb{G}_2$. In *International workshop on selected areas in cryptography*, pages 412–430. Springer, 2011.

[13] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *ACM conference on computer and communications security*, pages 89–98. Acm, 2006.

[14] Robert Granger and Michael Scott. Faster squaring in the cyclotomic subgroup of sixth degree extensions. In *International Workshop on Public Key Cryptography*, pages 209–223. Springer, 2010.

[15] Aurore Guillevic. A short-list of pairing-friendly curves resistant to special TNFS at the 128-bit security level. In *IACR international conference on public-key cryptography*, pages 535–564. Springer, 2020.

[16] Aurore Guillevic, Simon Masson, and Emmanuel Thomé. Cocks–Pinch curves of embedding degrees five to eight and optimal ate pairing computation. *Designs, Codes and Cryptography*, pages 1–35, 2020.

[17] Aurore Guillevic and Shashank Singh. On the alpha value of polynomials in the tower number field sieve algorithm. Cryptology ePrint archive, report 2019/885, 2019. https://eprint.iacr.org/2019/885.

[18] Daiki Hayashida, Kenichiro Hayasaka, and Tadanori Teruya. Efficient final exponentiation via cyclotomic structure for pairings over families of elliptic curves. Cryptology ePrint archive, report 2020/875, 2020. https://eprint.iacr.org/2020/875.

[19] Florian Hess, Nigel P Smart, and Frederik Vercauteren. The eta pairing revisited. *IEEE transactions on information theory*, 52(10):4595–4602, 2006.

[20] Ezekiel J Kachisa, Edward F Schaefer, and Michael Scott. Constructing brezing-weng pairing-friendly elliptic curves using elements in the cyclotomic field. In *International conference on pairing-based cryptography*, pages 126–135. Springer, 2008.

[21] Koray Karabina. Squaring in cyclotomic subgroups. *Mathematics of Computation*, 82(281):555–579, 2013.

[22] Taechan Kim and Razvan Barbulescu. Extended tower number field sieve: A new complexity for the medium prime case. In *Annual international cryptology conference*, pages 543–571. Springer, 2016.

[23] Taechan Kim, Sungwook Kim, and Jung Hee Cheon. On the final exponentiation in tate pairing computations. *IEEE Transactions on Information Theory*, 59(6):4033–4041, 2013.

[24] Hendrik Willem Lenstra, Arjen K Lenstra, L Lovfiasz, et al. Factoring polynomials with rational coeficients. 1982.

[25] Victor S Miller. The weil pairing, and its efficient calculation. *Journal of cryptology*, 17(4):235–261, 2004.

[26] Atsuko Miyaji, Masaki Nakabayashi, and Shunzou Takano. New explicit conditions of elliptic curve traces for FR-reduction. *IEICE transactions on fundamentals of electronics, communications and computer sciences*, 84(5):1234–1243, 2001.

[27] Yuki Nanjo, Masaaki Shirase, Yuta Kodera, Takuya Kusaka, and Yasuyuki Nogami. Calculation costs estimations of final exponentiation for pairing-friendly elliptic curves resistant to special TNFS. In *The 36th International Technical Conference on Circuits/ Systems, Computers, and Communications*, pages 229–232, 2021.

[28] Yuki Nanjo, Masaaki Shirase, Yuta Kodera, Takuya Kusaka, and Yasuyuki Nogami. A construction method of final exponentiation for a specific cyclotomic family of pairing-friendly elliptic curves with prime embedding degrees. In *2021 Ninth International Symposium on Computing and Networking (CANDAR)*, pages 148–154. IEEE, 2021.

[29] Tatsuaki Okamoto and Katsuyuki Takashima. Homomorphic encryption and signatures from vector decomposition. In *International conference on pairing-based cryptography*, pages 57–74. Springer, 2008.

[30] Michael Scott, Naomi Benger, Manuel Charlemagne, Luis J Dominguez Perez, and Ezekiel J Kachisa. On the final exponentiation for calculating pairings on ordinary elliptic curves. In *International conference on pairing-based cryptography*, pages 78–88. Springer, 2009.

[31] Masaaki Shirase and Yuki Nanjo. Generalization of the hard part computation of final exponentiation for arbitrary BLS curves (Japanese). *Technical committee on information security*, 2020(29):1–6, 2020.

[32] Martijn Stam and Arjen K Lenstra. Efficient subgroup exponentiation in quadratic and sixth degree extensions. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 318–332. Springer, 2002.

[33] Frederik Vercauteren. Optimal pairings. *IEEE Transactions on Information Theory*, 56(1):455–461, 2009.

[34] Xusheng Zhang and Dongdai Lin. Analysis of optimum pairing products at high security levels. In *International Conference on Cryptology in India*, pages 412–430. Springer, 2012.

A Proof of Theorem 1

The authors describe the proof of Theorem 1. In this context, the authors start to modify $d'(x) = c(x)d(x)$ where $d(x) = \Phi_k(p(x))/r(x)$ by using the expansion of Eq. (13) given by Hayashida et al. in [18]. In this case of the cyclotomic family for a prime $k = 6n+1$, one can determine the polynomials $h_1(x), h_2(x), T(x) \in \mathbb{Q}[x]$ from the properties of the cyclotomic polynomial in Eqs. (8) and (9) and definition of $(p(x), r(x), t(x))$ in Eq. (15) as follows:

$$\begin{cases} h_1(x) &= \Phi_6(x)^2/3, \\ h_2(x) &= \sum_{i=0}^{6n} T(x)^i/r(x), \\ T(x) &= -x^{6n+2} + x. \end{cases} \tag{39}$$

Since the value of Euler's totient function is $k' = k - 1 = 6n$ and the k-th cyclotomic polynomial is given by $\Phi_k(X) = \sum_{i=0}^{6n} X^i$, $d'(x)$ can be denoted as follows:

$$d'(x) = \underbrace{c(x)h_1(x)\left(\sum_{i=0}^{6n-1}\sum_{j=0}^{6n-1-i} T(x)^j p(x)^i\right)}_{=A(x)} + \underbrace{c(x)h_2(x)}_{=B(x)}. \tag{40}$$

where the first and second terms are referred to as $A(x)$ and $B(x)$, respectively.

(i) Modification of $A(x)$. For a non-negative integer s, let $m_s(x)$ be a polynomial defined by $m_s(x) = c(x)h_1(x)\sum_{j=0}^{s} T(x)^j$. For $s = 0$, since $c(x) = (x^{6n} - 1)/\Phi_6(x)$, it is clear that $m_0(x) = x^{6n}\Phi_6(x) - \Phi_6(x)$. In fact, for $s > 0$, $m_s(x)$ is denoted as follows:

$$m_s(x) = -3\sum_{i=0}^{s-1} T(x)^i p(x) - \Phi_6(x)T(x)^s + x^{6n}\Phi_6(x) + 3\sum_{i=1}^{s} T(x)^i. \tag{41}$$

which can be easily proven by the injection of s. The above formulas provide the following modification of $A(x)$.

$$\begin{aligned} A(x) &= \sum_{i=0}^{6n-1} m_{6n-1-i}(x)p(x)^i \\ &= (x^{6n}\Phi_6(x) - \Phi_6(x))p(x)^{6n-1} \\ &\quad + (-3p(x) - \Phi_6(x)T(x) + x^{6n}\Phi_6(x) + 3T(x))p(x)^{6n-2} \\ &\quad + (-3(T(x)+1)p(x) - \Phi_6(x)T(x)^2 + x^{6n}\Phi_6(x) + 3(T(x)^2 + T(x)))p(x)^{6n-3} + \cdots \\ &\quad + \left(-3\sum_{i=0}^{6n-2} T(x)^i p(x) - \Phi_6(x)T(x)^{6n-1} + x^{6n}\Phi_6(x) + 3\sum_{i=1}^{6n-1} T(x)^i\right)p(x)^0 \\ &= (x^{6n}\Phi_6(x) - 3 - \Phi_6(x))p(x)^{6n-1} \\ &\quad + (x^{6n}\Phi_6(x) - 3 - \Phi_6(x)T(x))p(x)^{6n-2} \\ &\quad + (x^{6n}\Phi_6(x) - 3 - \Phi_6(x)T(x)^2)p(x)^{6n-3} + \cdots \\ &\quad + (x^{6n}\Phi_6(x) - 3 - \Phi_6(x)T(x)^{6n-1})p(x)^0 + 3\sum_{i=0}^{6n-1} T(x)^i \\ &= \underbrace{\left(\sum_{i=0}^{6n-1}(x^{6n}\Phi_6(x) - 3)p(x)^i\right)}_{=A_1(x)} - \underbrace{\left(\Phi_6(x)\sum_{i=0}^{6n-1} T(x)^{6n-1-i}p(x)^i\right)}_{=A_2(x)} + \underbrace{3\sum_{i=0}^{6n-1} T(x)^i}_{=A_3(x)}, \end{aligned} \tag{42}$$

where the first, second, and third terms are referred to as $A_1(x), A_2(x)$, and $A_3(x)$, respectively.

(ii) Modification of $A_2(x)$. For a non-negative integer s, let $n_s(x)$ be a polynomial defined by $n_s(x) = \Phi_6(x)T(x)^s$. For $s \geq 0$, it is possible to denote $n_s(x)$ as follows:

$$n_s(x) = \alpha_s(x)p(x) + \beta_s(x) - \alpha_s(x)T(x), \tag{43}$$

where $\alpha_s(x)$ and $\beta_s(x)$ are polynomials in $\mathbb{Q}[x]$ defined as follows: Note that a polynomial $\gamma_s(x)$ is defined for representing $\alpha_s(x)$.

$$\alpha_s(x) = \begin{cases} 0 & \text{if } s = 0, \\ \alpha_{s-1}(x)T(x) + \gamma_s(x) & \text{if } s > 0, \end{cases} \tag{44}$$

$$\beta_s(x) = \begin{cases} x^s\Phi_6(x) & \text{if } s \equiv 0 \pmod 6, \\ -x^{6n+1+s}\Phi_6(x) + x^s\Phi_6(x) & \text{if } s \equiv 1 \pmod 6, \\ -x^{6n+1+s}\Phi_6(x) & \text{if } s \equiv 2 \pmod 6, \\ -x^s\Phi_6(x) & \text{if } s \equiv 3 \pmod 6, \\ x^{6n+1+s}\Phi_6(x) - x^s\Phi_6(x) & \text{if } s \equiv 4 \pmod 6, \\ x^{6n+1+s}\Phi_6(x) & \text{if } s \equiv 5 \pmod 6, \end{cases} \tag{45}$$

$$\gamma_s(x) = \begin{cases} 0 & \text{if } s \equiv 1, 4 \pmod 6, \\ 3x^s & \text{if } s \equiv 2, 3 \pmod 6, \\ -3x^s & \text{if } s \equiv 0, 5 \pmod 6. \end{cases} \tag{46}$$

The correctness of the above equation can be proven by induction on $s' \geq 0$ such that $s = 6s' + i > 0$ for $i \in \{1, 2, 3, 4, 5, 6\}$, however, that is omitted in this paper. The important fact is that $\beta_s(x) + \gamma_{s+1}(x) = -\mu_s(x)$ for $s \geq 0$, which can be easily confirmed from the definition. Then, $A_2(x)$ is represented as follows:

$$\begin{aligned} A_2(x) &= \sum_{i=0}^{6n-1} n_{6n-1-i}(x)p(x)^i \\ &= (\alpha_0(x)p(x) + \beta_0(x) - \alpha_0(x)T(x))p(x)^{6n-1} \\ &\quad + (\alpha_1(x)p(x) + \beta_1(x) - \alpha_1(x)T(x))p(x)^{6n-2} \\ &\quad + (\alpha_2(x)p(x) + \beta_2(x) - \alpha_2(x)T(x))p(x)^{6n-3} + \cdots \\ &\quad + (\alpha_{6n-1}(x)p(x) + \beta_{6n-1}(x) - \alpha_{6n-1}(x)T(x))p(x)^0 \\ &= (\beta_0(x) - \alpha_0(x)T(x) + \alpha_1(x))p(x)^{6n-1} \\ &\quad + (\beta_1(x) - \alpha_1(x)T(x) + \alpha_2(x))p(x)^{6n-2} \\ &\quad + (\beta_2(x) - \alpha_2(x)T(x) + \alpha_3(x))p(x)^{6n-3} + \cdots \\ &\quad + (\beta_{6n-1}(x) - \alpha_{6n-1}(x)T(x) + \alpha_{6n}(x))p(x)^0 \\ &\quad - \alpha_{6n}(x) \\ &= (\beta_0(x) + \gamma_1(x))p(x)^{6n-1} \\ &\quad + (\beta_1(x) + \gamma_2(x))p(x)^{6n-2} \\ &\quad + (\beta_2(x) + \gamma_3(x))p(x)^{6n-3} + \cdots \\ &\quad + (\beta_{6n-1}(x) + \gamma_{6n}(x))p(x)^0 \\ &\quad - ((\alpha_0(x) + \gamma_1(x))T(x)^{6n-1} + \cdots + \gamma_{6n-1}T(x) + \gamma_{6n}(x)) \\ &= \underbrace{-\left(\sum_{i=0}^{6n-1} \mu_{6n-1-i}(x)p(x)^i\right)}_{A_{21}(x)} \underbrace{-\left(\sum_{i=0}^{6n-1} \gamma_{6n-i}(x)T(x)^i\right)}_{A_{22}(x)}, \end{aligned} \tag{47}$$

where the first and second terms are referred to as $A_{21}(x)$ and $A_{22}(x)$, respectively.

(iii) Modification of $B(x)$. The polynomial $B(x)$ can be modified as follows:

$$B(x) = c(x)h_2(x)$$

$$
\begin{aligned}
&= \frac{c(x)T(x)\sum_{i=0}^{6n-1} T(x)^i + c(x)}{r(x)} \\
&= \frac{(-3r(x) + x^2c(x) + 3)\sum_{i=0}^{6n-1} T(x)^i + c(x)}{r(x)} \\
&= \underbrace{-\left(3\sum_{i=0}^{6n-1} T(x)^i\right)}_{=B_1(x)} + \underbrace{\frac{\Phi_6(x)(x^2c(x)+3)\sum_{i=0}^{6n-1} T(x)^i + c(x)}{\Phi_6(x^{6n+1})}}_{B_2(x)}, \qquad (48)
\end{aligned}
$$

where the first and second terms to as $B_1(x)$ and $B_2(x)$, respectively.

According to the modifications (i), (ii), and (iii), it is found that $d'(x)$ is denoted as

$$
\begin{aligned}
d(x) &= A(x) + B(x) = A_1(x) - (-A_{21}(x) - A_{22}(x)) + A_3(x) - B_1(x) + B_2(x) \\
&= A_1(x) + A_{21}(x) + A_{22}(x) + B_2(x) \\
&= \sum_{i=0}^{6n-1} \left(x^{6n}\Phi_6(x) - 3 + \mu_{6n-1-i}(x)\right) p(x)^i + A_{22}(x) + B_2(x). \qquad (49)
\end{aligned}
$$

Thus, it is enough to show that $A_{22}(x) + B_2(x) = 0$ is true. Since $B_2(x)$ involves denominator $\Phi_6(x^{6n+1})$, it is enough to show that $t_1(x) = \Phi_6(x^{6n+1})B_2(x) = \Phi_6(x)((x^2c(x)+3)\sum_{i=0}^{6n-1} T(x)^i + c(x))$ and $t_2(x) = -\Phi_6(x^{6n+1})\sum_{i=0}^{6n-1}\gamma_{6n-i}(x)T(x)^i$ are the same. Although the authors do not show the details in this paper, it is confirmed that $t_1(x) = 3(x^{6n} - T(x)^{6n}) = t_2(x)$. Thus, Theorem 1 is true. □

B Proof of Theorem 2

In the following, the authors describe proof of Theorem 2. Similar to proof of Theorem 1, the authors modify $d'(x) = c(x)d(x)$ where $d(x) = \Phi_k(p(x))/r(x)$ is given by Eq. (13). For the case of the family of curves with a prime $k = 6n-1$, one can determine the polynomials $h_1(x), h_2(x), T(x) \in \mathbb{Q}[x]$ from Eqs. (8), (9), and (16) as follows:

$$
\begin{cases}
h_1(x) &= \Phi_6(x)^2/3, \\
h_2(x) &= \sum_{i=0}^{6n-2} T(x)^i / r(x), \\
T(x) &= x^{6n}.
\end{cases} \qquad (50)
$$

Since the value of Euler's totient function is $k' = k-1 = 6n-2$ and the k-th cyclotomic polynomial is given by $\Phi_k(X) = \sum_{i=0}^{6n-2} X^i$, $d'(x)$ can be denoted as follows:

$$
d'(x) = \underbrace{c(x)h_1(x)\sum_{i=0}^{6n-3}\sum_{j=0}^{6n-3-i} T(x)^j p(x)^i}_{=A(x)} + \underbrace{c(x)h_2(x)}_{=B(x)}, \qquad (51)
$$

where the first and second parts are referred to as $A(x)$ and $B(x)$, respectively.

(i) Modification of $A(x)$. For a non-negative integer s, let $m_s(x)$ be a polynomial defined by $m_s(x) = c(x)h_1(x)\sum_{i=0}^{s} T(x)^i$. Then, for $s = 0$, it is clear that $m_0(x) = x^{6n-1}\Phi_6(x) - x^{6n-2}\Phi_6(x) - \Phi_6(x)$. For $s > 0$, $m_s(x)$ is written as follows:

$$
m_s(x) = 3\left(xT(x)^{s-1} - \sum_{i=0}^{s-1} T(x)^i\right) p(x) - xT(x)^{s-1}\Phi_6(x) - x^{6n-2}\Phi_6(x) - 3\left(xT(x)^s - \sum_{i=1}^{s} T(x)^i\right). \qquad (52)
$$

which can be easily proven by the injection of s. This leads to the following modification of $A(x)$.

$$
A(x) = \sum_{i=0}^{6n-3} m_{6n-3-i}(x)p(x)^i
$$

$$
\begin{aligned}
&= (x^{6n-1}\Phi_6(x) - x^{6n-2}\Phi_6(x) - \Phi_6(x))p(x)^{6n-3} \\
&\quad + (3(x-1)p(x) - x\Phi_6(x) - x^{6n-2}\Phi_6(x) - 3(xT(x) - T(x))p(x)^{6n-4} \\
&\quad + (3(xT(x) - T(x) - 1)p(x) - xT(x)\Phi_6(x) - x^{6n-2}\Phi_6(x) \\
&\qquad - 3(xT(x)^2 - T(x)^2 - T(x)))p(x)^{6n-5} + \cdots \\
&\quad + \left(3\left(xT(x)^{6n-4} - \sum_{i=0}^{6n-4} T(x)^i\right)p(x) - xT(x)^{6n-4}\Phi_6(x)\right. \\
&\qquad \left. -x^{6n-2}\Phi_6(x) - 3\left(xT(x)^{6n-3} - \sum_{i=1}^{6n-3} T(x)^i\right)\right)p(x)^0 \\
&= (-x^{6n-2}\Phi_6(x) - 3 + x^{6n-1}\Phi_6(x) - \Phi_6(x) + 3x)p(x)^{6n-3} \\
&\quad + (-x^{6n-2}\Phi_6(x) - 3 - x\Phi_6(x))p(x)^{6n-4} \\
&\quad + (-x^{6n-2}\Phi_6(x) - 3 - xT(x)\Phi_6(x))p(x)^{6n-5} + \cdots \\
&\quad + \left(-x^{6n-2}\Phi_6(x) - 3 - xT(x)^{6n-4}\Phi_6(x)\right)p(x)^0 - 3\left(xT(x)^{6n-3} - \sum_{i=0}^{6n-3} T(x)^i\right) \\
&= \underbrace{\left(\sum_{i=0}^{6n-3}(-x^{6n-2}\Phi_6(x) - 3)p(x)^i\right)}_{=A_1(x)} + \underbrace{\left(\nu_0(x)p(x)^{6n-3} - \sum_{i=0}^{6n-4} x\Phi_6(x)T(x)^{6n-4-i}p(x)^i\right)}_{=A_2(x)} \\
&\quad + \underbrace{3\left(\sum_{i=0}^{6n-3} T(x)^i - xT(x)^{6n-3}\right)}_{=A_3(x)}. \qquad (53)
\end{aligned}
$$

where the first, second, and third terms are referred to as $A_1(x), A_2(x)$, and $A_3(x)$, respectively.

(ii) Modification of $A_2(x)$. For a non-negative integer s, let $n_s(x)$ be a polynomial defined by $n_s(x) = \sum_{i=0}^{s} x\Phi_6(x)T(x)^s$. Then, $n_s(x)$ can be denoted as follows:

$$n_s(x) = \alpha_s(x)p(x) + \beta_s(x) - \alpha_s(x)T(x), \qquad (54)$$

where $\alpha_s(x)$ and $\beta_s(x)$ are defined as follows: The authors also define $\gamma_s(x)$ for representing $\alpha_s(x)$.

$$\alpha_s(x) = \begin{cases} 0 & \text{if } s = 0, \\ \alpha_{s-1}(x)T(x) + \gamma_s(x) & \text{if } s > 0, \end{cases} \qquad (55)$$

$$\beta_s(x) = \begin{cases} x^{s+1}\Phi_6(x) & \text{if } s \equiv 0 \pmod 6, \\ x^{6n+s}\Phi_6(x) & \text{if } s \equiv 1 \pmod 6, \\ x^{6n+s}\Phi_6(x) - x^{s+1}\Phi_6(x) & \text{if } s \equiv 2 \pmod 6, \\ -x^{s+1}\Phi_6(x) & \text{if } s \equiv 3 \pmod 6, \\ -x^{6n+s}\Phi_6(x) & \text{if } s \equiv 4 \pmod 6, \\ -x^{6n+s}\Phi_6(x) + x^{s+1}\Phi_6(x) & \text{if } s \equiv 5 \pmod 6, \end{cases} \qquad (56)$$

$$\gamma_s(x) = \begin{cases} 0 & \text{if } s \equiv 1, 4 \pmod 6, \\ 3x^{s+1} & \text{if } s \equiv 2, 3 \pmod 6, \\ -3x^{s+1} & \text{if } s \equiv 0, 5 \pmod 6. \end{cases} \qquad (57)$$

This can be proven by induction on $s' \geq 0$ such that $s = 6s' + i > 0$ for $i \in \{1, 2, 3, 4, 5, 6\}$. Note that there is a relation $\beta_s(x) + \gamma_{s+1}(x) = -\nu_{s+1}(x)$ for $s \geq 0$. Then, $A_2(x)$ can be modified as follows:

$$
\begin{aligned}
A_2(x) &= \nu_0(x)p(x)^{6n-3} - \sum_{i=0}^{6n-4} n_{6n-4-i}(x)p(x)^i \\
&= \nu_0(x)p(x)^{6n-3}
\end{aligned}
$$

$$
\begin{aligned}
&- (\alpha_0(x)p(x) + \beta_0(x) - \alpha_0(x)T(x))p(x)^{6n-4} \\
&- (\alpha_1(x)p(x) + \beta_1(x) - \alpha_1(x)T(x))p(x)^{6n-3} \\
&- (\alpha_2(x)p(x) + \beta_2(x) - \alpha_2(x)T(x))p(x)^{6n-2} - \cdots \\
&- (\alpha_{6n-4}(x)p(x) + \beta_{6n-4}(x) - \alpha_{6n-4}(x)T(x))p(x)^0 \\
&= \nu_0(x)p(x)^{6n-3} \\
&- (\beta_0(x) - \alpha_0(x)T(x) + \alpha_1(x))p(x)^{6n-4} \\
&- (\beta_1(x) - \alpha_1(x)T(x) + \alpha_2(x))p(x)^{6n-3} \\
&- (\beta_2(x) - \alpha_2(x)T(x) + \alpha_3(x))p(x)^{6n-2} - \cdots \\
&- (\beta_{6n-4}(x) - \alpha_{6n-4}(x)T(x) + \alpha_{6n-3}(x))p(x)^0 \\
&+ \alpha_{6n-3}(x) \\
&= \nu_0(x)p(x)^{6n-3} \\
&- (\beta_0(x) + \gamma_1(x))p(x)^{6n-4} \\
&- (\beta_1(x) + \gamma_2(x))p(x)^{6n-3} \\
&- (\beta_2(x) + \gamma_3(x))p(x)^{6n-2} - \cdots \\
&- (\beta_{6n-4}(x) + \gamma_{6n-3}(x))p(x)^0 \\
&+ ((\alpha_0(x)T(x) + \gamma_1(x))T(x)^{6n-4} + \cdots + \gamma_{6n-4}(x)T(x) + \gamma_{6n-3}(x)) \\
&= \underbrace{\left(\sum_{i=0}^{6n-3} \nu_{6n-3-i}(x)p(x)^i\right)}_{=A_{21}(x)} + \underbrace{\left(\sum_{i=0}^{6n-4} \gamma_{6n-3-i}(x)T(x)^i\right)}_{=A_{22}(x)}, \qquad (58)
\end{aligned}
$$

where the first and second terms are referred to as $A_{21}(x)$ and $A_{22}(x)$, respectively.

(iii) Modification of $B(x)$. The polynomial $B(x)$ can be modified as follows:

$$
B(x) = c(x)h_2(x) = \frac{c(x)\Phi_6(x)\sum_{i=0}^{6n-2} T(x)^i}{r(x)\Phi_6(x)} = \frac{3(x^{6n-1} - x^{6n-2} - 1)\sum_{i=0}^{6n-2} T(x)^i}{\Phi_6(x^{6n-1})}. \qquad (59)
$$

According to the modifications (i), (ii), and (iii), it is found that

$$
\begin{aligned}
d'(x) &= A(x) + B(x) = A_1(x) + (A_{21}(x) + A_{22}(x)) + A_3(x) + B(x) \\
&= \sum_{i=0}^{6n-3} (-x^{6n-2} - 3 + \nu_{6n-3-i}(x))p(x)^i + A_{22}(x) + A_3(x) + B(x). \qquad (60)
\end{aligned}
$$

Thus, it is enough to show $A_{22}(x) + A_3(x) + B(x) = 0$. Since $B(x)$ is denoted as Eq. (59), it is equivalent to show $-\Phi_6(x^{6n-1})(A_{22}(x) + A_3(x)) = 3(x^{6n-1} - x^{6n-2} - 1)\sum_{i=0}^{6n-2} T(x)^i$. Although the authors do not present the details, it is obtained that $-\Phi_6(x^{6n-1})A_{22}(x) = -\Phi_6(x^{6n-1}) \cdot \sum_{i=0}^{6n-4} \gamma_{6n-3-i}(x)T(x)^i = -3(xT(x)^{6n-3} + x^{6n-2})$ and $-\Phi_6(x^{6n-1})A_3(x) = -\Phi_6(x^{6n-1})\sum_{i=0}^{6n-3} T(x)^i - xT(x)^{6n-3} = 3(x^{6n-1} - x^{6n-2} - 1)\sum_{i=0}^{6n-2} T(x)^i + 3(xT(x)^{6n-3} + x^{6n-2})$, which indicate that the equation is held. Thus, Theorem 2 is true. □