Des. Codes Cryptogr. (2013) 67:271–292
DOI 10.1007/s10623-011-9605-y

Simple and exact formula for minimum loop length in Ate$_i$ pairing based on Brezing–Weng curves

Hoon Hong · Eunjeong Lee · Hyang-Sook Lee · Cheol-Min Park

Received: 26 January 2011 / Revised: 23 December 2011 / Accepted: 26 December 2011 /
Published online: 22 January 2012

Abstract We provide a *simple* and *exact* formula for the minimum Miller loop length in Ate$_i$ pairing based on Brezing–Weng curves, in terms of the involved parameters, under a mild condition on the parameters. It will also be shown that almost all cryptographically useful/meaningful parameters satisfy the mild condition. Hence the simple and exact formula is valid for them. It will also turn out that the formula depends only on essentially two parameters, providing freedom to choose the other parameters to address the design issues other than minimizing the loop length.

Keywords Pairing-based cryptosystem · Elliptic curves · Miller algorithm

Mathematics Subject Classification (2000) 11T70

Communicated by A. Enge.

H. Hong
Department of Mathematics, North Carolina State University, Raleigh, NC 27695-8205, USA
e-mail: hong@ncsu.edu

E. Lee (✉)
Institute of Mathematical Sciences, Ewha Womans University, Seoul 120-750, South Korea
e-mail: ejlee127@ewha.ac.kr

H.-S. Lee
Department of Mathematics, Ewha Womans University, Seoul 120-750, South Korea
e-mail: hsl@ewha.ac.kr

C.-M. Park
National Institute for Mathematical Sciences, Daejeon 305-811, South Korea
e-mail: mpcm@nims.re.kr

1 Introduction

Pairings play an important role in cryptography because they enable many protocols for security services [3,4,16,20]. During last 10 years, several pairings have been proposed such as Eta, Eta$_T$, Ate, Ate$_i$, R-ate, optimal Ate pairings [2,9,15,17,22,23]. Among them, this paper considers the Ate$_i$ pairing. The pairings are built on elliptic curves. During last 6 years, several methods were developed for constructing elliptic curves that are suitable (friendly) for pairing [5,6,10–12]. Among them, this paper considers the method due to Brezing–Weng [6] which produces a pairing-friendly elliptic curves by simply choosing a few parameter values, such as embedding degree, etc. Hence each choice of the parameter values determines a particular elliptic curve, and in turn, a particular Ate$_i$ pairing.

One important factor to consider while choosing the parameter values is the time taken for computing the resulting pairing. The computation essentially consists of calls to Miller's algorithm [18]. The time-complexity of Miller's algorithm is captured by the number of iterations of a loop in the algorithm, namely "Miller Loop Length". In the context of Ate$_i$ pairing, one chooses the i value so that the Miller loop length is minimal.

Naturally we are interested in determining the minimum loop length for given parameter values. One could, in principle, do this by tracing the Brezing–Weng/Ate$_i$ method (See Notation 1), in brute-force manner. However, it involves long, tedious and complicated computations such as evaluating polynomial functions, polynomial divisions (remaindering), square root operation in a ring of algebraic integers, finding minima over potentially large sets, etc. As a result, it is virtually impossible to do any reasoning on the relation between the minimum loop length and the parameter values, making it quite inconvenient for designing cryptosystems. It would be nice to have a simple formula (in terms of the parameters). Unfortunately, as usual, it seems that there is no simple formula that holds for all values of the parameters. One could, as typically done, carry out an asymptotic analysis (the big-O analysis) where one tries to obtain a simple formula by assuming that the parameter values are "sufficiently" large and by allowing "unknown" constant factors. However, such a result is not so useful for cryptosystem design, because it is not clear how large is sufficient and the unknown constant factor can make significant differences in the practical performance of cryptosystems.

The main contribution of this paper is to provide a *simple* and *exact* formula for the minimum loop length, under a mild condition on the parameters (see Theorem 1). It will be also shown that almost all cryptographically useful parameters satisfy the mild condition (see Remark 2). Hence the simple and exact formula is valid for them. It also turns out that the formula depends only on essentially two parameters, providing freedom to choose the other parameters to address the design issues other than minimizing the loop length (see Remark 1).

In order to obtain the formula, we had to overcome three technical challenges: (a) determining the minimum degree over i of x^i modulo a cyclotomic polynomial $\Phi_n(x)$, (b) finding out when a smaller degree implies a smaller value upon evaluation, and (c) finding out when remaindering commutes with evaluation, that is, polynomial remaindering followed by evaluation gives the same result as evaluation followed by integer remaindering. The problem (a) was challenging because there seemed to be no discernable relationship between the degree of x^i modulo $\Phi_n(x)$ and the parameters (i, n). For the problems (b) and (c), one would try to tackle them by estimating root bounds of involved polynomials, which requires finding (a bound on) the coefficients. Unfortunately, the coefficients of the involved polynomials are very difficult to bound, hence the challenge.

The crucial idea for overcoming the challenges was that the problems become more manageable when they are suitably recast in terms of *inverse* cyclotomic polynomials [19]. Once

so recast, the problem (a) amounts to studying a certain sparsity structure (maximum gap between consecutive exponents) of inverse cyclotomic polynomials (Lemmas 5 and 6), which can be done by direct computation for moderate parameter values, or using the recent theoretic results in [14] for large parameter values. The problems (b) and (c) amount to bounding the coefficients of inverse cyclotomic polynomials (Lemmas 10 and 12), which can be also done by direct computation on moderate parameter values, or using the recent number theoretic results in [7,19] on large parameter values.

One naturally wonders whether similar results could be obtained for more recent and improved pairings such as R-ate [17] and optimal Ate pairings [22]. We have not yet found a way to derive such results, due to various technical challenges (beyond those that we encountered while working on Ate_i). We leave them as open challenges.

The paper is structured as follows. The next section (Sect. 2) gives a brief review of the Brezing–Weng curves, Ate_i pairing and the Miller loop length. The readers who are familiar with them can skip this section, *except* Notation 1 and Assumption 1 in Sect. 2.4. We encourage all the readers to read them carefully, because the notations and the assumptions there will be extensively used throughout the subsequent sections. The following section (Sect. 3) states the main result (Theorem 1) precisely. The subsequent section (Sect. 4) provides a proof of the main result. We tried to make the proof as self-contained as possible. However, it might be helpful if the reader is familiar with the basic notations of Ate_i pairing [23], Brezing–Weng elliptic curves [6], and the basic properties of cyclotomic polynomials. We also suggest that the reader gets familiar with the properties of inverse cyclotomic polynomials given in [19]. The last section (Sect. 5) summarizes the main result and discusses a few open problems.

2 Preliminaries

In this section, we briefly review the Brezing–Weng curves, the Ate_i pairing and the Miller loop length. The readers who are familiar with them can skip this section, *except* Notation 1 and Assumption 1 in Sect. 2.4. We encourage all the readers to read them carefully, because the notations and the assumptions there will be extensively used throughout the subsequent sections.

2.1 Brezing–Weng curves

We recall Brezing–Weng curves [6,11]. Let $\mathbb{F}_q$ be a finite field where $q = p^n$ with prime p and let E be an elliptic curve defined over $\mathbb{F}_q$. Let $r(\neq p)$ be a prime factor of the order of $E(\mathbb{F}_q)$. Let k be the smallest integer such that $r \mid (q^k - 1)$; the integer k is called *the embedding degree* of E with respect to q and r (For the details, see [13]).

To use pairings in cryptosystem, the prime r should be sufficiently large and the embedding degree k should not be too large [11]. There are a number of methods for constructing such pairing-friendly elliptic curves. All these methods essentially consist of the following two steps:

(S1) Choose suitable integers q, r, k, t and d, where q, r, k are as described above and t is the trace and d is the CM-discriminant.
(S2) Find an equation of the elliptic curve such that $\#E(\mathbb{F}_q) = q + 1 - t$ using the Complex Multiplication(CM) method [1].

In [6,11], Brezing and Weng gave a general method for carrying out Step (S1). We summarize it below as Algorithm 1.

Algorithm 1 (Brezing–Weng method)

Input: k, d

Output: r, t, q

(1) Choose an irreducible polynomial $R(x) \in \mathbb{Z}[x]$ and a primitive k-th root of unity ζ_k such that $K \cong \mathbb{Q}[x]/(R(x))$ contains $\sqrt{-d}$ and ζ_k.
(2) Set $t(x) \in \mathbb{Q}[x]$ be the polynomial representing $\zeta_k + 1 \in K$.
(3) Set $y(x) \in \mathbb{Q}[x]$ be the polynomial representing $(\zeta_k - 1)/\sqrt{-d} \in K$.
(4) Set $Q(x) = (t(x)^2 + dy(x)^2)/4$.
(5) Choose $x_0 \in \mathbb{Z}$ be such that $Q(x_0)$ and $R(x_0)$ are primes.
(6) Set $r = R(x_0), t = t(x_0), q = Q(x_0)$.
(7) Output r, t, q.

Note that the outputs r, t, q depend not only on the inputs k, d but also on the choices $R(x), \zeta_k, x_0$ made in Steps (1) and (5). We will make the choices explicit. For this, we recall that the Brezing–Weng method can be specialized into two types depending on the choice of $R(x)$ in Step (1), namely

(T1) $R(x)$ is a cyclotomic polynomial [6].
(T2) $R(x)$ is a non-cyclotomic polynomial, such as an irreducible factor of $\Phi_k(u(x))$ for some $u(x) \in \mathbb{Q}[x]$ [5,12].

In this paper, we deal with the first type. Specifically we set $R(x)$ to be an ak-th cyclotomic polynomial $\Phi_{ak}(x)$ for some integer a. As the result, ζ_k is represented by $x^{a\eta} \bmod \Phi_{ak}(x)$ for some integer η with $\gcd(k, \eta) = 1$. Hence Steps (1) and (5) can be viewed as choosing the values of the parameters a, η, x_0. Thus the outputs r, t, q can be uniquely determined from the parameters k, d, a, η, x_0.

2.2 Ate_i pairing

We recall the Ate_i pairings [15,23]. Let E be an elliptic curve over $\mathbb{F}_q$ and $E[r]$ be the set of all points of order r in E. For every integer a and $P \in E$, let $f_{a,P}$ be a function in $\overline{\mathbb{F}_q}(E)$ with a divisor $\mathrm{div}(f_{a,P}) = a(P) - (aP) - (a-1)(O)$ where O is the point at infinity on E. Let π_q be the Frobenius endomorphism, $\pi_q : E \to E, (x, y) \mapsto (x^q, y^q)$ and

$$G_1 = E[r] \bigcap \mathrm{Ker}(\pi_q - [1])$$

$$G_2 = E[r] \bigcap \mathrm{Ker}(\pi_q - [q])$$

The Ate_i pairings for $P \in G_1, Q \in G_2$ are defined as follows:

$$\mathrm{Ate}_i \text{ pairing}: \ a_i(Q, P) = f_{\mu_i, Q}(P)^{(q^k-1)/r} \text{ for } 0 < i < k$$

where

$$\mu_i = q^i \bmod r \qquad [\, a = b \bmod c \iff c|(a-b) \text{ and } -c/2 < a \le c/2 \,]$$

for

$$i = \begin{cases} 1, \ldots, k-1 & k \text{ is odd} \\ 1, \ldots, \frac{k}{2} - 1 & k \text{ is even} \end{cases}$$

We use 'smod' instead of 'mod' because it is known to be more efficient (one less loop). When k is even, we consider only $i = 1, \ldots, \frac{k}{2} - 1$, because $\mu_{k/2} = -1$ (trivial Ate_i pairing) and $\mu_{i+\frac{k}{2}} = -\mu_i$ (symmetric).

2.3 Minimum Miller loop length

To compute the Ate_i pairings, we use Miller's algorithm [18], which repeats a certain loop for computing additions of points and evaluation at P. The complexity of Miller's algorithm is naturally characterized by the number of iterations of the loop, the so-called loop length. The loop length, in case of the Ate_i pairing, can be easily shown to be $\log_2 |\mu_i|$. Of course, one chooses the value of i so that the loop length is minimum. We will denote the minimum loop length by the symbol L, which is precisely given as

$$L = \log_2 \begin{cases} \min\limits_{1 \le i \le k-1} |\mu_i| & \text{if } k \text{ is odd} \\ \min\limits_{1 \le i \le \frac{k}{2}-1} |\mu_i| & \text{if } k \text{ is even} \end{cases} \tag{1}$$

2.4 Summary

In this subsection, we summarize all the notations and the assumptions introduced in the previous subsections for easy reference. We encourage all the readers to read this subsection carefully, because the notations and the assumptions listed here will be extensively used throughout the subsequent sections. The notations are ordered/structured so as to show explicitly how the minimum loop length L can be determined from the Brezing–Weng parameters k, d, a, η, x_0.

Notation 1 (Minimum Miller loop length in the Ate_i pairing based on Brezing–Weng curves)

Parameters:
k, d, a, η, x_0 : positive integers satisfying the condition given below (Assumption 1)

Brezing–Weng curves:

$$\begin{aligned} \Phi_{ak}(x) &= \text{the } ak\text{-th cyclotomic polynomial} \\ \zeta(x) &= x^{a\eta} \bmod \Phi_{ak}(x) \ i.e.\ \zeta(x) \text{ is a primitive } k\text{-th root of unity in } \mathbb{Q}[x]/(\Phi_{ak}(x)) \\ t(x) &= \zeta(x) + 1 \\ s(x) &= \text{the representation of } \sqrt{-d} \text{ as an element of } \mathbb{Q}[x]/(\Phi_{ak}(x)) \\ y(x) &= (\zeta(x) - 1)\frac{s(x)}{-d} \bmod \Phi_{ak}(x) \\ Q(x) &= \frac{t(x)^2 + d y(x)^2}{4} \\ r &= \Phi_{ak}(x_0) \\ q &= Q(x_0) \end{aligned}$$

Ate_i pairing:
$\mu_i = q^i \bmod r \qquad [\, a = b \bmod c \iff c | (a-b) \text{ and } -c/2 < a \le c/2 \,]$

Minimum Miller loop length:

$$L = \log_2 \begin{cases} \min\limits_{1 \le i \le k-1} |\mu_i| & \text{if } k \text{ is odd} \\ \min\limits_{1 \le i \le \frac{k}{2}-1} |\mu_i| & \text{if } k \text{ is even} \end{cases}$$

□

For the above quantities to be well-defined and meaningful, one needs to impose certain conditions on the parameters such as the following.

Assumption 1 (Global) From now on, *throughout* the paper, we will assume that the parameters k, a, d, η, x_0 satisfy the following conditions. Hence, whenever the above parameters appear in theorems, lemmas and proofs, one must remember that the conditions are *implicitly assumed*.

A1 : $k \geq 3$

A2 : $\gcd(\eta, k) = 1$

A3 : d is squarefree and $\sqrt{-d} \in \mathbb{Q}(\zeta_{ak})$ where ζ_{ak} is a primitive ak-th root of unity.

A4 : r is an odd prime number.

A5 : q is a prime power.

3 Main result

In the previous section (Sect. 2), we recalled how the minimum Miller loop length L in the Ate_i pairing based on Brezing–Weng curves depends on the Brezing–Weng parameters k, d, a, η, x_0. If you have not done so yet, we encourage the readers to skim through the notations and assumptions summarized in Sect. 2.4. Notation 1 shows explicitly the steps to follow to compute L for given k, d, a, η, x_0. One immediately sees that it involves long, tedious and complicated computations such as evaluating polynomial functions, polynomial divisions (remaindering), square root operation in a ring of algebraic integers, finding minima over potentially large sets, etc.

The main result of this paper to provide a *simple* and *exact* formula for L in terms of the parameters k, d, a, η, x_0, under a mild condition. In order to state the main result, we need the following additional notations.

Notation 2 (Notations used in stating the main result)

$$
\begin{aligned}
\varphi(n) &= \text{Euler-phi function, i.e. } \deg(\Phi_n) \\
g(f) &= \text{The maximum of the differences of two consecutive exponents in a polynomial } f,\ g(f) = 0 \text{ when } f \text{ is a monomial} \\
H(f) &= \text{the height of a polynomial } f, \text{ i.e., the maximum of the absolute values of the coefficients} \\
\Psi_n(x) &= \text{the } n\text{-th inverse cyclotomic polynomial, i.e., } \frac{x^n - 1}{\Phi_n(x)} \\
g_n &= \begin{cases} g(\Psi_n) & \text{if } n \text{ is odd} \\ g(\Psi_n \bmod x^{n/2}) & \text{if } n \text{ is even} \end{cases}
\end{aligned}
$$

Now we are ready to state the main result.

Theorem 1 (Main result) *For all* (k, d, a, η, x_0) *satisfying the following conditions*

$$\mathsf{C1}: \begin{cases} \varphi(n) - g_n \geq \dfrac{n}{3} & \text{if } n \text{ is odd} \\ \varphi(n) - g_n \geq \dfrac{n}{6} & \text{if } n \text{ is even and } k \neq 4 \\ \varphi(n) > \dfrac{n}{4} & \text{if } n \text{ is even and } k = 4 \end{cases}$$

$$\mathsf{C2}: x_0 > 2\,H(\Psi_n) + 2$$

$$\mathsf{C3}: d < \Phi_n(x_0)$$

where $n = ak$, *we have*

$$L = \log_2 \begin{cases} x_0^{a/2} - 1 & \text{if } k = 3 \text{ and } a \text{ is even} \\ x_0^{a/2} & \text{if } k > 3 \text{ is odd and } a \text{ is even} \\ x_0^{a} - 1 & \text{if } k = 6 \\ x_0^{a} & \text{else} \end{cases} \tag{2}$$

Remark 1 Note that the minimum Miller loop length L depends only on essentially two parameters x_0 and a as long as they satisfy the conditions in Theorem 1. Hence one can choose the values of the other parameter to address other design issues (other than minimizing the Miller loop length).

Example 1 We will illustrate the above Theorem 1 by applying it to a small example taken from [11] where $a = 4$, $d = 1$ and $k > 3$ is an odd prime. Note $n = 4k$. Note

$$\varphi(n) = \varphi(2^2 \cdot k) = (2^2 - 2)(k - 1) = 2(k - 1)$$

From the basic properties of inverse cyclotomic polynomials [19], we immediately have

$$\Psi_n(x) = x^{2k+2} + x^{2k} - x^2 - 1$$

Since n is even, we inspect $\Psi_n \bmod x^{2k}$, namely $-x^2 - 1$, obtaining $g_n = 2 - 0 = 2$. Note

$$\varphi(n) - g_n = 2(k - 1) - 2 = \frac{4k}{6} + \frac{8(k-3)}{6} \geq \frac{4k}{6} = \frac{n}{6}$$

Thus the condition C1 is satisfied by every odd prime $k > 3$. All the coefficients of Ψ_n are one of $1, 0, -1$ and so $H(\Psi_n) = 1$. We can satisfy C2 by simply choosing $x_0 > 2 \cdot 1 + 2 = 4$. Recall that $\Phi_n(x_0) = r$ is intended to be the size of a large cyclic group. Hence $d = 1 \ll r$. Thus the condition C3 is also satisfied by every "eligible" x_0 value (that makes r a large prime). Then, from Theorem 1, the minimum loop length L is given *exactly* by

$$L = \log_2(x_0^2)$$

Note that L does not depend on the value of k at all. It says the minimum loop length is essentially twice the bit length of x_0.

Remark 2 We observe that *almost all* cryptographically useful values of a, k, x_0 satisfy the conditions in Theorem 1. Hence the exact formula (2) in Theorem 1 applies to them. We elaborate on this observation.

- In cryptography, typically $a \in [1,\ 100]$ and $k \in [3, 100]$. Direct computation shows

$$a \in [1,\ 100] \text{ and } k \in [3, 100] \implies \mathsf{C1}$$

  In fact, it also holds for much larger values of $n = ak$. For instance, it holds for every n which has up to 3 distinct odd prime factors, except when $k = 4$ and the radical of n is $2 \cdot 3 \cdot 5 \cdot 7$, $2 \cdot 3 \cdot 5 \cdot 11$ or $2 \cdot 3 \cdot 5 \cdot 13$ [14].
- Direct computation shows that $H(\Psi_n) \leq 9$ for $n \leq 10^4$. Thus

$$n \leq 10^4 \text{ and } x_0 > 20 \implies \mathsf{C2}$$

  Direct computation also shows that $H(\Psi_n) \leq 1$ for $n \leq 10^4$ and $\varphi(n) \leq 100$. Thus

$$n \leq 10^4 \text{ and } \varphi(n) \leq 100 \text{ and } x_0 > 4 \implies \mathsf{C2}$$

  Typically n is chosen so that $\varphi(n) \leq 100$ for efficiency reason and x_0 is chosen to be much larger than 4, satisfying the condition C2.
  If needed, one can estimate $H(\Psi_n)$ for very large values of n. See [7,19] where an upper bound for $H(\Psi_n)$ is expressed in terms of the prime factors of n.
- The subgroup size $r = \Phi_n(x_0)$ should be at least 2^{256} for security reasons. On the other hand, the CM discriminant d is at most $10^{13} \approx 2^{44}$ for efficiency reasons [21]. Thus we see that $d \ll r$, satisfying the condition C3.

4 Proof

In this section, we prove the main theorem given in the previous section. The proof is a bit long and technical. Thus we divide it into many lemmas. For the sake of easy navigation among the lemmas, we provide a dependency diagram among them in Fig. 1 in Appendix. We begin by listing all the additional notations that will be used throughout the proofs without explicit references.

Notation 3 (Notations used in the proof)

$$\begin{aligned}
\mathrm{lc}(f) &= \text{the leading coefficient of a univariate polynomial } f \\
I_k &= \begin{cases} \{1, \ldots, k-1\} & \text{if } k \text{ is odd} \\ \{1, \ldots, \frac{k}{2} - 1\} & \text{if } k \text{ is even} \end{cases} \\
\psi(n) &= \deg \Psi_n(x) \\
B(f) &= \max_{x \in \mathbb{C}:\, f(x)=0} |x| \\
\Lambda_i(x) &= x^{ai} \bmod \Phi_{ak}(x) \\
d_n(i) &= \deg(x^i \bmod \Phi_n(x)) \\
t_n &= \text{the number of exponents (terms) occurring in } \Psi_n(x). \\
e_{n,j} &= \text{the } j\text{-th smallest exponent occurring in } \Psi_n(x). \\
g_{n,j} &= e_{n,j+1} - e_{n,j}
\end{aligned}$$

The following lemma summarizes a few basic facts about $Q(x)$ defined in Notation 1 (that holds under Assumption 1). It shows that, in order to solve our main problem, we first need to understand the remainder of a monomial modulo a cyclotomic polynomial.

Lemma 1

(i) $Q(x)^i \bmod \Phi_{ak}(x) \;=\; x^{a\eta i} \bmod \Phi_{ak}(x) \quad \textit{for} \;\; i \in I_k$
(ii) $\{\, \left|\left(Q(x)^i \bmod \Phi_{ak}(x)\right)(x_0)\right| : i \in I_k \,\} \;=\; \{\, \left|\left(x^{ai} \bmod \Phi_{ak}(x)\right)(x_0)\right| : i \in I_k \,\}$

Proof (i) From the definition of $Q(x)$ in Notation 1, we have, modulo $\Phi_{ak}(x)$,

$$\begin{aligned} Q(x) &\equiv \frac{(\zeta(x)+1)^2 + d(\zeta(x)-1)^2 s(x)^2 \frac{1}{d^2}}{4} \;\equiv\; \frac{(\zeta(x)+1)^2 - (\zeta(x)-1)^2}{4} \\ &\equiv\; \zeta(x) \;\equiv\; x^{a\eta} \end{aligned}$$

Hence $Q(x)^i \bmod \Phi_{ak}(x) = x^{a\eta i} \bmod \Phi_{ak}(x)$.

(ii) Note, for $i \in I_k$,

$$Q(x)^i \bmod \Phi_{ak}(x) = x^{a\eta i} \bmod \Phi_{ak}(x) = \begin{cases} x^{a\sigma(i)} \bmod \Phi_{ak}(x) & \text{when } k \text{ is odd} \\ -x^{a\sigma(i)} \bmod \Phi_{ak}(x) & \text{when } k \text{ is even} \end{cases}$$

where

$$\begin{aligned} \sigma : I_k &\longrightarrow I_k \\ i &\longmapsto \eta i \bmod k \quad \text{when } k \text{ is odd} \\ i &\longmapsto \eta i \bmod \frac{k}{2} \quad \text{when } k \text{ is even} \end{aligned}$$

From the fact that σ is one-to-one and onto, we have the desired result. □

The following lemma recasts the question on the remainder of a monomial modulo a cyclotomic polynomial to that on the inverse cyclotomic polynomial. This simple recasting will play a crucial role in overcoming many technical challenges.

Lemma 2 *Let* $\Psi_n \;=\; \sum_{j=1}^{t_n} c_{n,j}\, x^{e_{n,j}}$. *We have, for all* i,

$$(x^i \bmod \Phi_n) \cdot \Psi_n \;=\; \sum_{j=1}^{t_n} c_{n,j}\, x^{(i+e_{n,j}) \bmod n}$$

In particular, the set of non-zero coefficients of $(x^i \bmod \Phi_n) \cdot \Psi_n$ *are the same as those of* Ψ_n.

Proof We only need to note, for all i,

$$\begin{aligned} (x^i \bmod \Phi_n) \cdot \Psi_n &= (x^i \cdot \Psi_n) \bmod (\Phi_n \cdot \Psi_n) \\ &= (x^i \cdot \Psi_n) \bmod (x^n - 1) \\ &= \left(x^i \sum_{j=1}^{t_n} c_{n,j}\, x^{e_{n,j}} \right) \bmod (x^n - 1) \\ &= \left(\sum_{j=1}^{t_n} c_{n,j}\, x^{i+e_{n,j}} \right) \bmod (x^n - 1) \end{aligned}$$

$$= \sum_{j=1}^{t_n} c_{n,j}\ x^{(i+e_{n,j}) \bmod n}$$

□

In the introduction (Sect. 1), we mentioned three technical challenges. Lemma 3 through Lemma 6 deal with the first one: (a) determining the minimum degree over i of x^i modulo a cyclotomic polynomial $\Phi_n(x)$. The lemmas crucially exploit the previous lemma (Lemma 2) where the question is recast in terms of inverse cyclotomic polynomials. Once so recast, the problem (a) amounts to studying a certain sparsity structure (maximum gap between consecutive exponents) of inverse cyclotomic polynomials (Lemmas 5 and 6).

Lemma 3 *For* $0 \leq i < n$, *we have*

$$d_n(i) = i - \psi(n) + \max_{e_{n,j} < n-i} e_{n,j}$$

Proof Let

$$h_i \ = \ (x^i \bmod \Phi_n) \cdot \Psi_n$$

Then we have

$$\deg(h_i) = d_n(i) + \psi(n)$$

Thus we can determine $d_n(i)$ from $\deg(h_i)$. So we try to determine $\deg(h_i)$.

From Lemma 2, we have

$$h_i \ = \ \sum_{j=1}^{t_n} c_{n,j}\ x^{(i+e_{n,j}) \bmod n}$$

Since $i < n$, we have

$$i + e_{n,j} < 2n$$

Thus

$$h_i \ = \ \sum_{i+e_{n,j} < n} c_{n,j}\ x^{i+e_{n,j}} \ + \ \sum_{n \leq i+e_{n,j} < 2n} c_{n,j}\ x^{i+e_{n,j}-n} \tag{3}$$

The first sum is a non-zero polynomial, since it contains the term $c_{n,1}x^i$ due to the fact that $e_{n,1} = 0$. Note that every exponent in the first sum is at least i. Note also that every exponent in the second sum is at most $i - 1$, since $e_{n,j} < n$. Hence

$$\deg(h_i) = \deg\left(\sum_{i+e_{n,j} < n} c_{n,j}\ x^{i+e_{n,j}} \right) = \max_{i+e_{n,j} < n} i + e_{n,j} = i + \max_{e_{n,j} < n-i} e_{n,j}$$

Thus

$$d_n(i) = \deg(h_i) - \psi(n) = i - \psi(n) + \max_{i+e_{n,j} < n} e_{n,j}$$

□

Lemma 4 *For* $1 \leq j < t_n$, *we have*

$$\min_{n-e_{n,j+1} \leq i < n-e_{n,j}} d_n(i) \ = \ \varphi(n) - g_{n,j}$$

Proof From Lemma 3, we have

$$\begin{aligned}\min_{n-e_{n,j+1}\le i<n-e_{n,j}} d_n(i) &= \min_{n-e_{n,j+1}\le i<n-e_{n,j}} \left(i-\psi(n)+\max_{e_{n,\ell}<n-i} e_{n,\ell}\right)\\ &= \min_{n-e_{n,j+1}\le i<n-e_{n,j}} \left(i-\psi(n)+e_{n,j}\right)\\ &= n-e_{n,j+1}+e_{n,j}-\psi(n)\\ &= \varphi(n)-e_{n,j+1}+e_{n,j}\\ &= \varphi(n)-g_{n,j}\end{aligned}$$

□

Lemma 5 *Let n be an odd number. Then we have*

$$\min_{\varphi(n)\le i<n} d_n(i) = \varphi(n)-g_n$$

Proof Note

$$\begin{aligned}&\exists i \quad \left[\ \varphi(n)\le i<n \quad \text{and} \quad n-e_{n,j+1}\le i<n-e_{n,j}\ \right]\\ \Longleftrightarrow\ &\varphi(n)<n-e_{n,j}\\ \Longleftrightarrow\ &n-e_{n,t_n}<n-e_{n,j}\\ \Longleftrightarrow\ &e_{n,t_n}>e_{n,j}\\ \Longleftrightarrow\ &1\le j<t_n\end{aligned}$$

From Lemma 4, we have

$$\begin{aligned}\min_{\varphi(n)\le i<n} d_n(i) &= \min_{1\le j<t_n} \ \min_{n-e_{n,j+1}\le i<n-e_{n,j}} d_n(i)\\ &= \min_{1\le j<t_n} \left(\varphi(n)-g_{n,j}\right)\\ &= \varphi(n)-\max_{1\le j<t_n} g_{n,j}\\ &= \varphi(n)-g_n\end{aligned}$$

□

Lemma 6 *Let n be an even number such that $\varphi(n)<n/2$. Then we have*

$$\min_{\varphi(n)\le i<n/2} d_n(i) = \varphi(n)-g_n$$

Proof Since n is an even number, we have $n=2^{\alpha}\cdot s$ where $\alpha\ge 1$ and $2\nmid s$. Since $\varphi(n)<n/2$, we have $s\ge 3$. From the basic properties of inverse cyclotomic polynomials [19], we have

$$\Psi_n(x) \ = \ \Psi_s(-x^{2^{\alpha-1}}) \ - \ x^{n/2}\Psi_s(-x^{2^{\alpha-1}})$$

and there will be no accumulation/cancellation of terms across the first part and the second part.

Note

$$\begin{aligned}
&\exists i \quad \left[\, \varphi(n) \le i < n/2 \quad \text{and} \quad n - e_{n,j+1} \le i < n - e_{n,j} \,\right] \\
\iff & \max\{\varphi(n), n - e_{n,j+1}\} < \min\{n/2, n - e_{n,j}\} \\
\iff & \max\{n - e_{n,t_n}, n - e_{n,j+1}\} < \min\{n - e_{n,t_s+1}, n - e_{n,j}\} \\
\iff & n - \min\{e_{n,t_n}, e_{n,j+1}\} < n - \max\{e_{n,t_s+1}, e_{n,j}\} \\
\iff & \min\{e_{n,t_n}, e_{n,j+1}\} > \max\{e_{n,t_s+1}, e_{n,j}\} \\
\iff & t_s + 1 \le j < t_n
\end{aligned}$$

From Lemma 4, we have

$$\begin{aligned}
\min_{\varphi(n) \le i < n/2} d_n(i) &= \min_{t_s+1 \le j < t_n} \quad \min_{n - e_{n,j+1} \le i < n - e_{n,j}} \quad d_n(i) \\
&= \min_{t_s+1 \le j < t_n} \quad \varphi(n) - g_{n,j} \\
&= \varphi(n) - \max_{t_s+1 \le j < t_n} \quad g_{n,j} \\
&= \varphi(n) - \max_{\frac{t_n}{2}+1 \le j < t_n} \quad g_{n,j} \\
&= \varphi(n) - g_n \qquad \text{by the symmetry of } \Psi_n
\end{aligned}$$

□

Lemma 7 through Lemma 9 determine when $\Lambda_i = x^{ai} \bmod \Phi_{ak}(x)$ for $i \in I_k$ has the minimum degree. They can be viewed as applications of Lemma 5 and Lemma 6.

Lemma 7 *Let a be odd and k be odd such that $\varphi(ak) - g_{ak} > a$. Then*

- $\Lambda_1 = x^a$
- $\forall i \in I_k \;\; i \ne 1 \Longrightarrow \deg(\Lambda_i) > \deg(\Lambda_1)$

Proof Since $\varphi(ak) > a$, we have

$$\Lambda_1 = x^a \bmod \Phi_{ak}(x) = x^a$$

Let $i \in I_k = \{1, \ldots, k-1\}$. Assume that $i \ne 1$. We consider the two cases:

Case 1: $2 \le i < \frac{\varphi(ak)}{a}$.
We obviously have

$$\deg(\Lambda_i) \;=\; \deg\left(x^{ai} \bmod \Phi_{ak}(x)\right) \;=\; \deg(x^{ai}) \;=\; ai \;>\; a \;=\; \deg(\Lambda_1)$$

Case 2: $\frac{\varphi(ak)}{a} \le i \le k-1$.
From Lemma 5, we have

$$\deg(\Lambda_i) \;\ge\; \varphi(ak) - g_{ak} \;>\; a \;=\; \deg(\Lambda_1)$$

Thus

$$\forall i \in I_k \;\; i \ne 1 \Longrightarrow \deg(\Lambda_i) > \deg(\Lambda_1)$$

□

Lemma 8 *Let a be even and k be odd such that $\varphi(ak) - g_{ak} > \frac{a}{2}$. Then*

- $\Lambda_{\frac{k+1}{2}} = -x^{\frac{a}{2}}$
- $\forall i \in I_k \;\; i \neq \frac{k+1}{2} \Longrightarrow \deg(\Lambda_i) > \deg(\Lambda_{\frac{k+1}{2}})$

Proof Since $\varphi(ak) > \frac{a}{2}$, we have

$$\Lambda_{\frac{k+1}{2}} \;=\; x^{a\frac{k+1}{2}} \bmod \Phi_{ak}(x) \;=\; x^{\frac{ak}{2}} x^{\frac{a}{2}} \bmod \Phi_{ak}(x) \;=\; -x^{\frac{a}{2}} \bmod \Phi_{ak}(x) \;=\; -x^{\frac{a}{2}}$$

Let $i \in I_k = \{1, \ldots, k-1\}$. Assume that $i \neq \frac{k+1}{2}$. Since a is even, we have $\varphi(ak) < ak/2$ and in turn $\frac{\varphi(ak)}{a} < \frac{k}{2}$. Thus we consider the following three cases.

Case 1: $1 \leq i < \frac{\varphi(ak)}{a}$.
We obviously have

$$\deg(\Lambda_i) = \deg\left(x^{ai} \bmod \Phi_{ak}(x)\right) = \deg(x^{ai}) = ai > \frac{a}{2} = \deg(\Lambda_{\frac{k+1}{2}})$$

Case 2: $\frac{\varphi(ak)}{a} \leq i < \frac{k}{2}$.
From Lemma 6, we have

$$\deg(\Lambda_i) \;\geq\; \varphi(ak) - g_{ak} \;>\; \frac{a}{2} \;= \deg(\Lambda_{\frac{k+1}{2}})$$

Case 3: $\frac{k+3}{2} \leq i \leq k-1$.
From Lemma 6, we have

$$\begin{aligned}
\deg(\Lambda_i) &= \deg(x^{ai} \bmod \Phi_{ak}(x)) \\
&= \deg(x^{\frac{ak}{2}} x^{ai-\frac{ak}{2}} \bmod \Phi_{ak}(x)) \\
&= \deg(-x^{ai-\frac{ak}{2}} \bmod \Phi_{ak}(x)) \\
&\geq \min\{\frac{3a}{2},\; \varphi(ak) - g_{ak}\} \\
&> \frac{a}{2} \\
&= \deg(\Lambda_{\frac{k+1}{2}})
\end{aligned}$$

Thus

$$\forall i \in I_k \;\; i \neq \frac{k+1}{2} \Longrightarrow \deg(\Lambda_i) > \deg(\Lambda_{\frac{k+1}{2}})$$

□

Lemma 9 *Let k be even such that $\varphi(ak) - g_{ak} > a$. Then*

- $\Lambda_1 = x^a$
- $\forall i \in I_k \;\; i \neq 1 \Longrightarrow \deg(\Lambda_i) > \deg(\Lambda_1)$

Proof Since $\varphi(ak) > a$, we have

$$\Lambda_1 = x^a \bmod \Phi_{ak}(x) = x^a$$

Let $i \in I_k = \{1, \ldots, \frac{k}{2} - 1\}$. Assume that $i \neq 1$. We consider the two cases:

Case 1: $2 \leq i < \frac{\varphi(ak)}{a}$.
We obviously have

$$\deg(\Lambda_i) \;=\; \deg\left(x^{ai} \bmod \Phi_{ak}(x)\right) \;=\; \deg(x^{ai}) \;= ai \;>\; a \;=\; \deg(\Lambda_1)$$

Case 2: $\frac{\varphi(ak)}{a} \leq i \leq \frac{k}{2} - 1$.
From Lemma 6, we have

$$\deg(\Lambda_i) \;\geq\; \varphi(ak) - g_{ak} \;>\; a \;=\; \deg(\Lambda_1)$$

Thus

$$\forall i \in I_k \;\; i \neq 1 \Longrightarrow \deg(\Lambda_i) > \deg(\Lambda_1)$$

□

In the introduction (Sect. 1), we mentioned three technical challenges. Lemma 10 deals with the second one: (b) finding out when a smaller degree implies a smaller value upon evaluation. The crucial idea is again to recast the problem in terms of *inverse* cyclotomic polynomials. Once so recast, the problem (b) amounts to bounding the coefficients of inverse cyclotomic polynomials.

Lemma 10 *For all* (k, a, x_0) *satisfying the following condition:*

$$\mathsf{C2} : x_0 \;>\; 2\,H(\Psi_{ak}) + 2$$

we have

$$\deg(\Lambda_j) > \deg(\Lambda_i) \;\Longrightarrow\; |\Lambda_j(x_0)| \;>\; |\Lambda_i(x_0)|$$

Proof Let

$$S_\pm \;=\; \sigma_j \Lambda_j \pm \Lambda_i$$

where $\sigma_j = \text{sign}(\text{lc}(\Lambda_j))$. Let

$$W_\pm \;=\; S_\pm \cdot \Psi_{ak}$$

Note that $\text{lc}(S_\pm) \geq 1$ and $\text{lc}(\Psi_{ak}) = 1$. Thus we have

$$\text{lc}(W_\pm) \;\geq 1$$

Note

$$W_\pm \;=\; \sigma_j \Lambda_j \cdot \Psi_{ak} \pm \Lambda_i \cdot \Psi_{ak}$$

From Lemma 2, we have

$$H(W_\pm) \;\leq\; H(\Lambda_j \cdot \Psi_{ak}) + H(\Lambda_i \cdot \Psi_{ak}) \;=\; 2H(\Psi_{ak})$$

By applying Cauchy's root bound formula [8], we have

$$B(W_\pm) \;\leq\; \frac{H(W_\pm)}{|\text{lc}(W_\pm)|} + 1 \;\leq\; \frac{2H(\Psi_{ak})}{1} + 1 \;=\; 2H(\Psi_{ak}) + 1$$

Since $B(S_\pm) \leq B(W_\pm)$, we have

$$B(S_\pm) \;\leq\; 2H(\Psi_{ak}) + 1$$

Assume that $x_0 > 2H(\Psi_{ak}) + 1$. Since $\mathrm{lc}(S_\pm) > 0$, we have $S_\pm(x_0) > 0$, that is,

$$\sigma_j \Lambda_j(x_0) > \Lambda_i(x_0) > -\sigma_j \Lambda_j(x_0)$$

Hence

$$|\Lambda_j(x_0)| > |\Lambda_i(x_0)|$$

□

In the introduction (Sect. 1), we mentioned three technical challenges. Lemma 11 and Lemma 12 deal with the last one: (c) finding out when remaindering commutes with evaluation, that is, polynomial remaindering followed by evaluation gives the same result as evaluation followed by integer remaindering. The crucial idea is once again to recast the problem in terms of *inverse* cyclotomic polynomials. Once so recast, the problem (c) amounts to bounding the coefficients of inverse cyclotomic polynomials.

Lemma 11 *For all* (k, a, x_0) *satisfying the following condition:*

$$\mathsf{C2} : x_0 > 2H(\Psi_{ak}(x)) + 2$$

we have

$$\frac{\Phi_{ak}(x_0)}{2} > |\Gamma_i(x_0)|$$

where

$$\Gamma_i(x) = Q(x)^i \bmod \Phi_{ak}(x)$$

Proof Let

$$S_\pm = \frac{\Phi_{ak}}{2} \pm \Gamma_i$$
$$W_\pm = S_\pm \cdot \Psi_{ak}$$

Note that $\mathrm{lc}(S_\pm) = 1/2$ and $\mathrm{lc}(\Psi_{ak}) = 1$. Thus we have

$$\mathrm{lc}(W_\pm) = 1/2$$

Note

$$W_\pm = \frac{\Phi_{ak}}{2} \cdot \Psi_{ak} \pm \Gamma_i \cdot \Psi_{ak} = \frac{x^{ak} - 1}{2} \pm \Gamma_i \cdot \Psi_{ak}$$

Thus

$$H(W_\pm) \leq 1/2 + H(\Gamma_i \cdot \Psi_{ak})$$

From Lemmas 1 and 2, we have

$$H(\Gamma_i \cdot \Psi_{ak}) = H(\Psi_{ak})$$

Thus

$$H(W_\pm) \leq 1/2 + H(\Psi_{ak})$$

By applying Cauchy's root bound formula [8], we have

$$B(W_\pm) \leq \frac{H(W_\pm)}{|\mathrm{lc}(W_\pm)|} + 1 \leq \frac{1/2 + H(\Psi_{ak})}{1/2} + 1 = 2H(\Psi_{ak}) + 2$$

Since $B(S_\pm) \leq B(W_\pm)$, we have

$$B(S_\pm) \leq 2H(\Psi_{ak}) + 2$$

Assume that $x_0 > 2H(\Psi_{ak}) + 2$. Since $\mathrm{lc}(S_\pm) > 0$, we have $S_\pm(x_0) > 0$, that is,

$$\frac{\Phi_{ak}(x_0)}{2} > \Gamma_i(x_0) > -\frac{\Phi_{ak}(x_0)}{2}$$

Hence

$$\frac{\Phi_{ak}(x_0)}{2} > |\Gamma_i(x_0)|$$

□

Lemma 12 *For all* (k, d, a, η, x_0) *satisfying the following conditions:*

$$\mathsf{C2} : x_0 > 2\,H(\Psi_{ak}(x)) + 2$$
$$\mathsf{C3} : d < \Phi_{ak}(x_0)$$

we have

$$Q(x_0)^i \bmod \Phi_{ak}(x_0) = \left(Q(x)^i \bmod \Phi_{ak}(x)\right)(x_0)$$

Proof Let $\Gamma_i(x) = Q(x)^i \bmod \Phi_{ak}(x)$. Then we have for some $P(x) \in \mathbb{Q}[x]$

$$Q(x)^i = P(x)\Phi_{ak}(x) + \Gamma_i(x)$$

Thus we have

$$Q(x_0)^i = P(x_0)\Phi_{ak}(x_0) + \Gamma_i(x_0)$$

We claim that $Q(x_0)$, $P(x_0)$, $\Phi_{ak}(x_0)$ and $\Gamma_i(x_0)$ are all integers. First, $Q(x_0)$ is an integer due to A5 in Assumption 1. Second, $\Phi_{ak}(x_0)$ is an integer because $\Phi_{ak}(x) \in \mathbb{Z}[x]$. Third, $\Gamma_i(x_0)$ is an integer due to Lemma 1. It remains to show that $P(x_0)$ is an integer. We will do so by contradiction. Assume $P(x_0)$ is *not* an integer. Since $\Phi_{ak}(x) \in \mathbb{Z}[x]$ and monic, obviously $\zeta(x), t(x), s(x) \in \mathbb{Z}[x]$ and thus

$$Q(x)^i = \tilde{Q}(x)^i/(4d)^i$$

for some $\tilde{Q}(x) \in \mathbb{Z}[x]$. Since $\Phi_{ak}(x)$ is monic, we have

$$P(x) = \tilde{P}(x)/(4d)^i$$

for some $\tilde{P}(x) \in \mathbb{Z}[x]$. Hence

$$P(x_0) = \tilde{p}/(4d)^i$$

for some $\tilde{p} \in \mathbb{Z}$. Note that $P(x_0)\Phi_{ak}(x_0)$ is an integer. Thus the denominator of $P(x_0)$ should be a factor of $\Phi_{ak}(x_0)$. Note that the denominator of $P(x_0)$ is a factor of $(4d)^i$. Hence $(4d)^i$ and $\Phi_{ak}(x_0)$ should have a common factor. According to Assumption 1, $r = \Phi_{ak}(x_0)$ is an odd prime. This means that $\Phi_{ak}(x_0) \mid d$, contradicting C3. So we have shown that $P(x_0)$ is an integer.

Since $Q(x_0)$, $P(x_0)$, $\Phi_{ak}(x_0)$ and $\Gamma_i(x_0)$ are all integers, we have

$$Q(x_0)^i \bmod \Phi_{ak}(x_0) = \Gamma_i(x_0) \bmod \Phi_{ak}(x_0)$$

From Lemma 11 and C2, we have

$$\frac{\Phi_{ak}(x_0)}{2} \;>\; |\Gamma_i(x_0)|$$

Hence

$$\Gamma_i(x_0) \bmod \Phi_{ak}(x_0) \;=\; \Gamma_i(x_0)$$

Therefore

$$Q(x_0)^i \bmod \Phi_{ak}(x_0) \;=\; \Gamma_i(x_0)$$

Finally we have

$$Q(x_0)^i \bmod \Phi_{ak}(x_0) \;=\; \left(Q(x)^i \bmod \Phi_{ak}(x)\right)(x_0)$$

□

Lemma 13 uses the previous lemma (Lemma 12) to express the minimum Miller loop length L in terms of $\Lambda_i(x_0)$.

Lemma 13 *For all* (k, d, a, η, x_0) *satisfying the following conditions:*

$$\mathsf{C2} : x_0 \;>\; 2\,H(\Psi_{ak}(x)) + 2$$
$$\mathsf{C3} : d \;<\; \Phi_n(x_0)$$

we have

$$L = \log_2 \min_{i \in I_k} |\Lambda_i(x_0)|$$

Proof Note

$$\begin{aligned}
L &= \log_2 \min_{i \in I_k} \left|Q(x_0)^i \bmod \Phi_{ak}(x_0)\right| && \text{from Notation 1}\\
&= \log_2 \min_{i \in I_k} \left|\left(Q(x)^i \bmod \Phi_{ak}(x)\right)(x_0)\right| && \text{from C2, C3 and Lemma 12}\\
&= \log_2 \min_{i \in I_k} \left|\left(x^{ai} \bmod \Phi_{ak}(x)\right)(x_0)\right| && \text{from Lemma 1}\\
&= \log_2 \min_{i \in I_k} |\Lambda_i(x_0)| && \text{from Notation 3}
\end{aligned}$$

□

Now, we are ready to prove Theorem 1 (Main Result). We will begin with Lemma 13. For the minimum degree of Λ_i, we will use Lemma 7 through Lemma 9 and, for the minimum value, we will use Lemma 10.

Proof of Theorem 1(Main Result) From C2, C3 and Lemma 13, we have

$$L = \log_2 \min_{i \in I_k} |\Lambda_i(x_0)|$$

We consider several cases.

Case 1: a is odd, $k > 3$ is odd. From C1 we have

$$\varphi(ak) - g_{ak} \geq \frac{ak}{3} > \frac{ak}{k} = a$$

From Lemma 7, we have

- $\Lambda_1 = x^a$
- $\forall i \in I_k \;\; i \neq 1 \Longrightarrow \deg(\Lambda_i) > \deg(\Lambda_1)$

From Lemma 10, we have

$$L = \log_2 (x_0^a)$$

Case 2: a is even, $k > 3$ is odd. From C1 we have

$$\varphi(ak) - g_{ak} \geq \frac{ak}{6} > \frac{ak}{2k} = \frac{a}{2}$$

From Lemma 8, we have

- $\Lambda_{\frac{k+1}{2}} = -x^{\frac{a}{2}}$
- $\forall i \in I_k \;\; i \neq \frac{k+1}{2} \Longrightarrow \deg(\Lambda_i) > \deg(\Lambda_{\frac{k+1}{2}})$

From Lemma 10, we have

$$L = \log_2 (x_0^{a/2})$$

Case 3: a is odd, $k > 6$ is even. From C1 we have

$$\varphi(ak) - g_{ak} \geq \frac{ak}{6} > \frac{ak}{k} = a$$

From Lemma 9, we have

- $\Lambda_1 = x^a$
- $\forall i \in I_k \;\; i \neq 1 \Longrightarrow \deg(\Lambda_i) > \deg(\Lambda_1)$

From Lemma 10, we have

$$L = \log_2 (x_0^a)$$

Case 4: a is even, $k > 6$ is even. Using the same reasoning as in Case 3, we have

$$L = \log_2 (x_0^a)$$

Case 5: a is odd, $k = 3$. From C1 we have

$$\varphi(a \cdot 3) - g_{a \cdot 3} \geq \frac{a \cdot 3}{3} = a$$

Since $g_{a \cdot 3} \geq 1$, we have $\varphi(a \cdot 3) > a$. Note

$$\Phi_{a \cdot 3}(x) \;\; | \;\; \Phi_3(x^{a \cdot 3/3}) = x^{2a} + x^a + 1$$

Thus

- $\Lambda_1(x) = x^{a \cdot 1} \bmod \Phi_{a \cdot 3}(x) = x^a$

- $\Lambda_2(x) = x^{a\cdot 2} \bmod \Phi_{a\cdot 3}(x) = (-x^a - 1) \bmod \Phi_{a\cdot 3}(x) = -x^a - 1$

Hence we have

$$L = \log_2 (x_0^a)$$

Case 6: a is even, $k = 3$. From C1 we have

$$\varphi(a \cdot 3) - g_{a\cdot 3} \geq \frac{a \cdot 3}{6} = \frac{a}{2}$$

Since $g_{a\cdot 3} \geq 1$, we have $\varphi(a \cdot 3) > \frac{a}{2}$. Since a is even, we have

$$\Phi_{a\cdot 3}(x) \quad | \quad \Phi_{2\cdot 3}(x^{a\cdot 3/(2\cdot 3)}) = x^a - x^{a/2} + 1$$

Thus

- $\Lambda_1(x) = x^{a\cdot 1} \bmod \Phi_{a\cdot 3}(x) = (x^{a/2} - 1) \bmod \Phi_{a\cdot 3}(x) = x^{a/2} - 1$
- $\Lambda_2(x) = x^{a\cdot 2} \bmod \Phi_{a\cdot 3}(x) = (x^{a/2} - 1)^2 \bmod \Phi_{a\cdot 3}(x) = -x^{a/2}$

Hence we have

$$L = \log_2 (x_0^{a/2} - 1)$$

Case 7: a is odd, $k = 4$. From C1 we have

$$\varphi(ak) > \frac{ak}{4} = a$$

Thus

- $\Lambda_1 = x^a$

Hence we have

$$L = \log_2 (x_0^a)$$

Case 8: a is even, $k = 4$. Using the same reasoning as in Case 7, we have

$$L = \log_2 (x_0^a)$$

Case 9: a is odd, $k = 6$. From C1 we have

$$\varphi(a \cdot 6) - g_{a\cdot 6} \geq \frac{a \cdot 6}{6} = a$$

Since $g_{a\cdot 6} \geq 1$, we have $\varphi(a \cdot 6) > a$. Note

$$\Phi_{a\cdot 6}(x) \quad | \quad \Phi_6(x^{a\cdot 6/6}) = x^{2a} - x^a + 1$$

Thus

- $\Lambda_1(x) = x^{a\cdot 1} \bmod \Phi_{a\cdot 6}(x) = x^a$
- $\Lambda_2(x) = x^{a\cdot 2} \bmod \Phi_{a\cdot 6}(x) = (x^a - 1) \bmod \Phi_{a\cdot 6}(x) = x^a - 1$

Hence we have

$$L = \log_2 (x_0^a - 1)$$

Case 10: a is even, $k = 6$. Using the same reasoning as in Case 9, we have

$$L = \log_2 (x_0^a - 1)$$

Summarizing the cases above, we have

$$L = \log_2 \begin{cases} x_0^a & \text{if } a \text{ is odd and } k > 3 \text{ is odd.} \\ x_0^{a/2} & \text{if } a \text{ is even and } k > 3 \text{ is odd.} \\ x_0^a & \text{if } a \text{ is odd and } k > 6 \text{ is even.} \\ x_0^a & \text{if } a \text{ is even and } k > 6 \text{ is even.} \\ x_0^a & \text{if } a \text{ is odd and } k = 3. \\ x_0^{a/2} - 1 & \text{if } a \text{ is even and } k = 3. \\ x_0^a & \text{if } a \text{ is odd and } k = 4. \\ x_0^a & \text{if } a \text{ is even and } k = 4. \\ x_0^a - 1 & \text{if } a \text{ is odd and } k = 6. \\ x_0^a - 1 & \text{if } a \text{ is even and } k = 6. \end{cases}$$

Combining related cases, we have

$$L = \log_2 \begin{cases} x_0^{a/2} - 1 & \text{if } k = 3 \text{ and } a \text{ is even} \\ x_0^{a/2} & \text{if } k > 3 \text{ is odd and } a \text{ is even} \\ x_0^a - 1 & \text{if } k = 6 \\ x_0^a & \text{else} \end{cases}$$

Finally Theorem 1 (Main Result) has been proved. □

5 Conclusion

In this paper, we provided a *simple* and *exact* formula for the minimum Miller loop length in Ate$_i$ pairing based on Brezing–Weng curves (using cyclotomic polynomials), in terms of the involved parameters, under a mild condition on the parameters. We have also shown that almost all cryptographically useful/meaningful parameters satisfy the mild condition.

One naturally wonders whether similar results could be obtained for more recent and improved pairings such as R-ate [17] and optimal Ate pairings [22]. We have not yet found a way to derive similar results, mainly because the expressions for the pairings are much more complex than that of the Ate$_i$ pairing. One also wonders whether the results given here could be adapted to the Brezing–Weng curves where the polynomial $R(x)$ is chosen to be

a non-cyclotomic polynomial as in (T2) of Sect. 2.1. Again we have not yet found a way to adapt the results, mainly because it is not clear what new object could play, in that case, the crucial role that the *inverse*-cyclotomic polynomials play in this paper. We leave both problems as open challenges.

Acknowledgement Eunjeong Lee was supported by the Priority Research Centers Program through the National Research Foundation of Korea (NRF) grant funded by the Ministry of Education, Science and Technology (No. 2009-0093827). Hyang-Sook Lee and Cheol-Min Park were supported by the National Research Foundation of Korea (NRF) grant funded by the Ministry of Education, Science and Technology. (No.2010-0000402). We would like to thank the anonymous referees for their insightful and helpful suggestions.

Appendix

See Fig. 1.

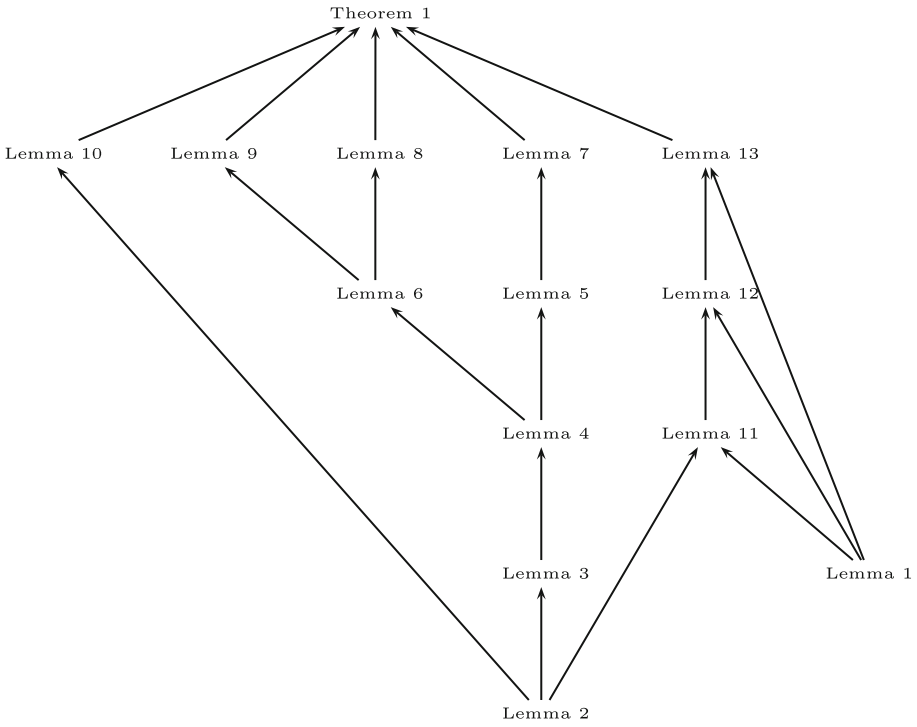

Fig. 1 Dependency among Lemmas

References

1. Atkin A., Morain F.: Elliptic curves and primality proving. Math. Comput. **61**, 29–68 (1993).
2. Barreto P.S.L.M., Galbraith S., Ó hÉigeartaigh C., Scott M.: Efficient pairing computation on supersingular abelian varieties. Des. Codes Cryptogr. **42**(3), 239–271 (2007).

3. Boneh D., Franklin M.: Identity-based encryption from the Weil pairing. SIAM J. Comput. **32**(3), 586–615 (2003).
4. Boneh D., Lynn B., Shacham H.: Short signatures from the Weil pairing. J. Cryptol. **17**(4), 297–319 (2004).
5. Barreto P.S.L.M., Naehrig M.: Pairing-friendly elliptic curves of prime order. In: Preneel B., Tavares S. (eds.) SAC 2005. LNCS, vol. 3897, pp. 319–331. Springer, Heidelberg (2006).
6. Brezing F., Weng A.: Elliptic curves suitable for pairing based cryptography. Des. Codes Cryptogr. **37**(1), 133–141 (2005).
7. Bzdęga B.: On the height of cyclotomic polynomials. arXiv preprint, arXiv:1012.3897v1, Dec (2010).
8. Cauchy A.L.: Exercises de mathematique. Oeuvres **9**(2), 122 (1829).
9. Duursma I., Lee H.: Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$. In: Advances in Cryptography: Proceedings of AsiaCrypt 2003, Lecture Notes in Computer Science, vol. 2894, pp. 111–123. Springer, New York (2003).
10. Freeman D.: Constructing pairing-friendly elliptic curves with embedding degree 10. In: Hess F., Pauli S., Pohst M. (eds.) ANTS 2006. LNCS, vol. 4076, pp. 452–465. Springer, Heidelberg (2006).
11. Freeman D., Scott M., Teske E.: A taxonomy of pairing-friendly elliptic curves. J. Cryptol. **23**, 224–280 (2010).
12. Galbraith S., McKee J., Valenca P.: Ordinary abelian varieties having small embedding degree. Finite Fields Appl. **13**, 800–814 (2007).
13. Hitt L.: On the minimal embedding field. In: Proceedings of Pairing 2007, LNCS 4575, vol. 294–301 (2007).
14. Hong H., Lee E., Lee H.S., Park C.M: Maximum gap in inverse cyclotomic polynomials. arXiv Preprint, arXiv 1101.4255, Jan (2011).
15. Hess F., Smart N.P., Vercauteren F. (2006) The eta pairing revisited. IEEE Trans. Inform. Theory **52**, pp. 4595–4602
16. Joux A.: A one round protocol for tripartite Diffie-Hellman. J. Cryptol. **17**(4), 263–276 (2004).
17. Lee E., Lee H.S, Park C.M: Efficient and generalized pairing computation on Abelian varieties. IEEE Trans. Inform. Theory **55**(4), 1793–1803 (2009).
18. Mille V.: The Weil pairing and its efficient calculation. J. Cryptol. 17:235–261 (2004).
19. Moree P.: Inverse cyclotomic polynomials. J. Numb. Theory **129**(3), 667–680 (2009).
20. Sakai R., Ohgishi K., Kasahara M.: Cryptosystems based on pairing. In: Proceedings of Symposium on Cryptography and Information Security, SCIS 2000 (2000).
21. Sutherland A.V.: Computing Hilbert class polynomials with the Chinese remainder theorem. Math. Comp. **80**, 501–538 (2011).
22. Vercauteren F.: Optimal pairings. IEEE Trans. Inform. Theory **56**(1), 455–461 (2010).
23. Zhao C., Zhang F., Huang J.: A note on the ate pairing. Int. J. Inform. Secur. **7**(6), 379–382 (2008).