Simple and Exact Formula for Minimum Loop Length in Ate$_i$ pairing based on Brezing-Weng curves

Hoon Hong, Eunjeong Lee, Hyang-Sook Lee and Cheol-Min Park

January 21, 2011

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 be also 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 two parameters, providing freedom to choose the other parameters to address the design issues other than minimizing the loop length.

1 Introduction

Pairing plays an important role in cryptography because it enables many protocols for security services [2, 3, 11, 15]. During last 10 years, several pairings have been proposed such as Eta, Eta$_T$, Ate, Ate$_i$, R-ate, optimal Ate pairing [7, 1, 10, 18, 12, 17]. This paper focuses on Ate$_i$ pairing because other pairings such as R-ate, optimal Ate pairing are variants of Ate$_i$. The parings are built on elliptic curves. Brezing-Weng [4] provided a general method for constructing infinitely many "pairing friendly" elliptic curves by simply choosing a few parameter values, such as embedding degree, etc. Hence each choice of the parameter values yields a particular Ate$_i$ pairing.

One important factor to consider while choosing the parameters is the time taken for computing the paring. The computation essentially consists of calls to Miller's algorithm [13]. The time-complexity of Miller's algorithm is captured by the number of iterations in 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 minimum.

Naturally we are interested in determining the minimum loop length for given parameters. 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 minimums over potentially large sets, etc. As the result, it is virtually impossible to do any "reasoning" on the relation between the minimum loop length and the parameters, making it quite inconvenient for designing cryptosystems . It would be nice to have a simple formula (in terms of the parameters). Unfortunately, as usual, there is no simple formula that holds for all values of the parameters. One could, as typically done, carry out 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 enough

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 3). Hence the simple and exact formula is valid for them. It also turns out that the formula depends only on two parameters, providing freedom to choose the other parameters to address the design issues other than minimizing the loop length (See Remark 4).

In order to obtain the formula, we had to overcome several technical challenges: (a) finding out when polynomial remaindering commutes with evaluation, (b) finding out when a smaller degree implies a smaller value upon evaluation, (c) determining the minimum degree over i of x^i modulo a cyclotomic polynomial $\Phi_n(x)$, etc. Usually one would try to tackle the problems (a) and (b) 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 problem (c) 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).

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 [14]. Once so recast, the problems (a) and (b) amounts to bounding the coefficients of inverse cyclotomic polynomials (Lemmas 13 and 11), which can be done by direct computation on moderate parameter values, or using the recent number theoretic results in [14, 5] on large parameter values. The problem (c) amounts to studying a certain sparsity structure (maximum gap between consecutive exponents) of inverse cyclotomic polynomials (Lemmas 6 and 7), which can be done again by direction computation on moderate parameter values, or using the recent number theoretic results in [9] for large parameter values.

The next section (Section 2) state the problem and the main result (Theorem 1) precisely. The following section (Section 3) 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 [18], Brezing-Weng elliptic curves [4], and the basic properties of cyclotomic polynomials. We also suggest that the reader gets familiar with the properties of inverse cyclotomic polynomials given in [14].

2 Main Result

The problem is to find a *simple* and *exact* formula for the minimum Miller loop length in Ate_i pairing based on Brezing-Weng curves, in terms of the Brezing-Weng parameters. We begin by fixing all the notations needed for a precise definition of the minimum Miller loop length. The notations are taken mainly from [8, 18].

Notation 1 (Minimum Miller loop length in Ate_i pairing based on Brezing-Weng curves)**.**

Parameters:

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

Brezing-Weng curves:

$$\begin{aligned}
\Phi_{ak}(x) &= \text{the } ak\text{-th cyclotomic polynomial} \\
\zeta(x) &= x^{a\eta} \bmod \Phi_{ak}(x) \qquad [\ f(x) \bmod g(x) \text{ stands for the remainder of } f(x)/g(x)\ ] \\
t(x) &= \zeta(x) + 1 \\
s(x) &= \text{the representation of } \sqrt{-d} \text{ as an element of } \mathbb{Q}[x]/(\Phi_{ak}(x)) \\
y(x) &= (\zeta(x) - 1)\frac{s(x)}{-d} \bmod \Phi_{ak}(x) \\
Q(x) &= \frac{t(x)^2 + dy(x)^2}{4} \\
r &= \Phi_{ak}(x_0) \\
q &= Q(x_0)
\end{aligned}$$

Ate_i pairing:

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

Minimum Miller loop length:

$$L = \begin{cases} \min\limits_{0<i<k} \log_2 |\mu_i| & \text{if } k \text{ is odd} \\ \min\limits_{0<i<\frac{k}{2}} \log_2 |\mu_i| & \text{if } k \text{ is even} \end{cases}$$

Remark 1. A few remarks on the intended meaning of the notations: The integer r is the size of a large cyclic subgroup of $E(\mathbb{F}_q)$. The integer k is the embedding degree of r and q, that is, the smallest integer such that $r|(q^k - 1)$. The polynomial $\zeta(x)$ represents a k-th primitive root of unity as an element of $\mathbb{Q}[x]/(\Phi_{ak}(x))$. The integer η indicates the particular choice of a k-th primitive root of unity. The integer d is a CM discriminant. The operation smod stands for the *signed* remainder.

Remark 2. In Ate_i pairing, we use 'smod' instead of 'mod' because it is known to be more efficient (one less loop). In Minimum Miller loop length, when k is even we optimize over $0 < i < \frac{k}{2}$ because $\mu_{k/2} = -1$ (trivial Ate_i pairing) and $\mu_{i+\frac{k}{2}} = -\mu_i$ (symmetric).

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 an ak-th primitive root of unity.
- A4 : r is an odd prime number.
- A5 : q is a prime or a power of prime number.

We will also need the following additional notations in order to state the main result.

Notation 2 (Notations used in stating the main result)**.**

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

$$g_n = \begin{cases} g(\Psi_n) & \text{if } n \text{ is odd} \\ g(\Psi_n \bmod x^{n/2}) & \text{if } n \text{ is even} \end{cases}$$

Note that the minimum Miller loop length L could depend on the parameters a, k, d, η, x_0. In order to make this potential dependence explicit, we will sometimes write $L(a, k, d, \eta, x_0)$. Now we are ready to state the main result (Theorem 1).

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

$$\begin{aligned}
\mathsf{C1} \ : & \begin{cases} \varphi(n) - g_n \ \geq \frac{n}{3} & \text{if } n \text{ is odd} \\ \varphi(n) - g_n \ \geq \frac{n}{6} & \text{if } n \text{ is even and } k \neq 4 \\ \varphi(n) \ > \frac{n}{4} & \text{if } n \text{ is even and } k = 4 \end{cases} \\
\mathsf{C2} \ : & \ x_0 \ > \ 2\,H(\Psi_n) + 2 \\
\mathsf{C3} \ : & \ d \ < \ \Phi_n(x_0)
\end{aligned}$$

where $n = ak$, we have

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

Example 1. We will illustrate the above Theorem 1 by applying it on a small example taken from [8] 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 [14], 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 3. We observe that *almost all* cryptographically useful values of a, k, x_0 satisfy the conditions in Theorem 1. Hence the exact formula (1) 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 $2 \cdot 3 \cdot 5 \cdot 13$ [9].

- 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 [14, 5] 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^{160} for security reasons. On the other hand, the CM discriminant d is at most $10^{13} \approx 2^{44}$ for efficiency reasons [16]. Thus we see that $d \ll r$, satisfying the condition C3.

Remark 4. Note that the minimum Miller loop length $L(a, k, d, \eta, x_0)$ does *not* depend on the values of k, d and η as long as they satisfy the conditions in Theorem 1. Hence one can choose the values of k, d, η to address other design issues (other than minimizing the Miller loop length).

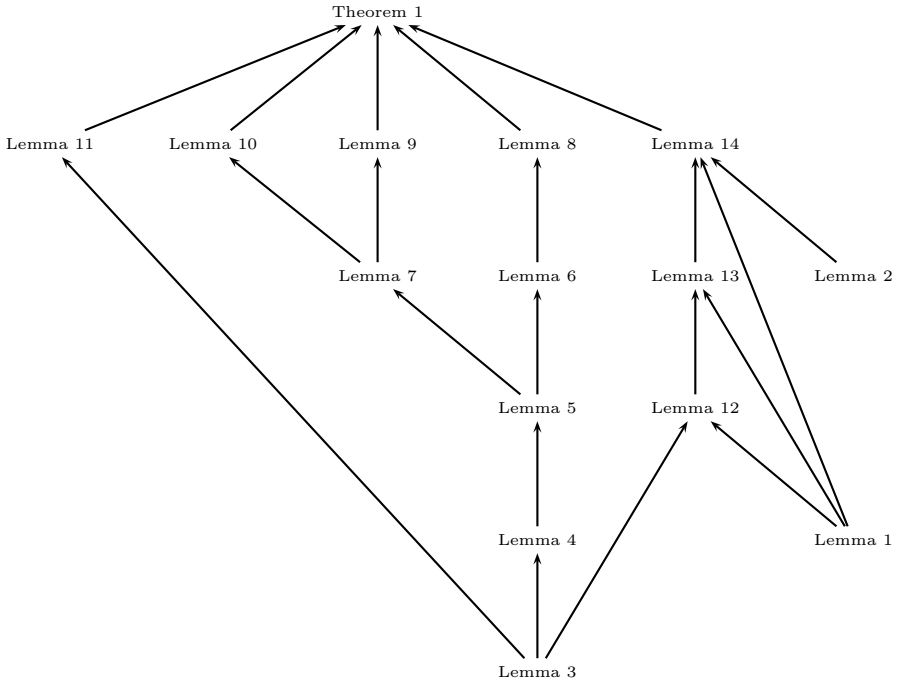

Figure 1: Dependency among Lemmas

3 Proof

In this section, we prove the main theorem given in the previous section. The proof is a bit long and technical. Thus we divided it into many lemmas, that are interesting on their own. For the sake of easy navigation among the lemmas, we provide a dependency diagram among them in Figure 1. 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)**.**

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

Lemma 1. *We have*

- $Q(x)^i \bmod \Phi_{ak}(x) \;=\; x^{a\eta i} \bmod \Phi_{ak}(x)$
- $Q(x)^i \bmod \Phi_{ak}(x) \;\in\; \mathbb{Z}[x]$.

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

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

Hence $Q(x)^i \bmod \Phi_{ak}(x) = x^{a\eta i} \bmod \Phi_{ak}(x)$. Since $x^{a\eta i}, \Phi_{ak}(x) \in \mathbb{Z}[x]$ and $\Phi_{ak}(x)$ is monic, we immediately see that $Q(x)^i \bmod \Phi_{ak}(x) \;\in\; \mathbb{Z}[x]$. □

Lemma 2. *For every η such that $\gcd(\eta, k) = 1$ we have*

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

Proof. Immediate from the fact that the following map is one-to-one and onto.

$$\begin{array}{rcll} \sigma & : & I_k \longrightarrow I_k & \\ & & i \longmapsto \eta i \bmod k & \text{when } k \text{ is odd} \\ & & i \longmapsto \eta i \bmod \dfrac{k}{2} & \text{when } k \text{ is even} \end{array}$$

□

Lemma 3. *Let $\Psi_n = \sum_{j=1}^{t_n} c_{n,j}\, x^{e_{n,j}}$. We have*

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

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

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

□

Lemma 4. *For $0 \le i < n$, 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 3, 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

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

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 5. *For $1 \le j < \; t_n$, we have*

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

Proof. From Lemma 4, we have

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

□

Lemma 6. *We have*

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

Proof. Note

$$\begin{array}{rl} & \exists i \quad [\ \varphi(n) \le i < n \quad \wedge \quad n - e_{n,j+1} \le i < n - e_{n,j}\ ] \\ \iff & \max\{\varphi(n), n - e_{n,j+1}\} < n - e_{n,j} \\ \iff & \max\{n - e_{n,t_n}, n - e_{n,j+1}\} < n - e_{n,j} \\ \iff & n - \min\{e_{n,t_n}, e_{n,j+1}\} < n - e_{n,j} \\ \iff & \min\{e_{n,t_n}, e_{n,j+1}\} > e_{n,j} \\ \iff & 1 \le j < t_n \end{array}$$

From Lemma 5, we have

$$\begin{array}{rcl} \min\limits_{\varphi(n)\le i<n} d_n(i) & = & \min\limits_{1\le j<t_n} \quad \min\limits_{n-e_{n,j+1}\le i<n-e_{n,j}} \quad d_n(i) \\ & = & \min\limits_{1\le j<t_n} \quad \varphi(n) - g_{n,j} \\ & = & \varphi(n) - \max\limits_{1\le j<t_n} \quad g_{n,j} \\ & = & \varphi(n) - g_n \end{array}$$

□

Lemma 7. *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 [14], 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

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

From Lemma 5, we have

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

□

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

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

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

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

Let $i \in I_k = \{1, \ldots, k-1\}$. Assume that $i \neq 1$. 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 6, we have

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

Thus

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

□

Lemma 9. *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 $i \neq \frac{k+1}{2}$. We consider the 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: $\frac{\varphi(ak)}{a} \leq i \leq \frac{k-1}{2}$.
From Lemma 7, 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 7, 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 10. *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 7, we have

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

Thus

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

□

Lemma 11. *For all* (a, k, 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 3, 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 [6], 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 $\text{lc}(S_{\pm}) > 0$, 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

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

□

Lemma 12. *For all* (a, k, 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

$$\begin{aligned} S_{\pm} &= \frac{\Phi_{ak}}{2} \pm \Gamma_i \\ W_{\pm} &= S_{\pm} \cdot \Psi_{ak} \end{aligned}$$

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 3, 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 [6], 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 13. *For all (a, k, d, η, x_0) satisfying the following conditions:*

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

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 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

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

From Lemma 12 and C2, we have

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

Hence

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

Therefore

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

Finally we have

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

□

Lemma 14. *For all (a, k, d, η, x_0) satisfying the following conditions:*

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

we have

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

Proof. Note

$$\begin{aligned}
L &= \log_2 \min_{i\in I_k} \left|Q(x_0)^i \bmod \Phi_{ak}(x_0)\right| && \text{from Notation 1}\\
&= \log_2 \min_{i\in I_k} \left|\left(Q(x)^i \bmod \Phi_{ak}(x)\right)(x_0)\right| && \text{from C2, C3 and Lemma 13}\\
&= \log_2 \min_{i\in I_k} \left|\left(x^{a\eta i} \bmod \Phi_{ak}(x)\right)(x_0)\right| && \text{from Lemma 1}\\
&= \log_2 \min_{i\in I_k} \left|\left(x^{ai} \bmod \Phi_{ak}(x)\right)(x_0)\right| && \text{from Lemma 2}\\
&= \log_2 \min_{i\in I_k} |\Lambda_i(x_0)| && \text{from Notation 3}
\end{aligned}$$

□

Proof of Theorem 1(Main Result). From C2, C3 and Lemma 14, 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 8, we have

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

From Lemma 11, 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 9, 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 11, 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 10, we have

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

From Lemma 11, 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

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

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

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

Combining related cases, we have

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

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

References

[1] P.S.L.M. Barreto, S. Galbraith, C. Ó hÉigeartaigh and M. Scott, Efficient Pairing Computation on Supersingular Abelian Varieties, Designs, Codes and Cryptography, Vol. 42, No. 3, pp.239-271, (2007)

[2] D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, SIAM J. of Computing, Vol. 32, No. 3, pp. 586-615, (2003)

[3] D. Boneh,. Lynn, H. Shacham, Short signatures from the Weil pairing, Journal of Cryptology, Vol. 17, No 4, pp. 297-319, (2004)

[4] F. Brezing, A. Weng, Elliptic curves suitable for pairing based cryptography, Designs, Codes and Cryptography, Vol. 37, No. 1, pp.133-141 (2005)

[5] B. Bzdęga, On the height of cyclotomic polynomials, arXiv preprint, `arXiv:1012.3897v1`, Dec (2010)

[6] A.L. Cauchy, Exercises de mathematique, Oeuvres (2) Vol. 9, p. 122 (1829)

[7] I. Duursma and H. Lee, Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$, Advances in Cryptography: Proceedings of AsiaCrypt 2003, Lecture Notes in Computer Science, Vol. 2894, pp.111-123, Springer-Verlag, (2003)

[8] D. Freeman, M. Scott, and E. Teske, A taxonomy of pairing-friendly elliptic curves, Journal of Cryptology, Vol. 23, pp.224-280, Springer, (2010)

[9] H. Hong, E. Lee, H.S Lee and C.M Park, Maximum Gap in Inverse Cyclotomic Polynomials, Preprint, arXiv ????????, Jan (2010)

[10] F. Hess, N.P. Smart and F. Vercauteren, The Eta Pairing Revisited, IEEE Trans. Information Theory, Vol 52, pp.4595-4602, (2006)

[11] A. Joux, A one round protocol for tripartite Diffie-Hellman. Journal of Cryptology, Vol. 17, No. 4, pp.263-276, (2004)

[12] E. Lee, H.S Lee, C.M Park. Efficient and Generalized Pairing Computation on Abelian Varieties. IEEE Transactions on Information Theory, Vol. 55, No. 4, pp.1793-1803, (2009)

[13] V. Miller, The Weil pairing and its efficient calculation, Journal of Cryptology, 17, 235-261, (2004)

[14] P. Moree, Inverse cyclotomic polynomials, Journal of Number Theory, 129 Issue 3, pp. 667-680, (2009)

[15] R. Sakai, K. Ohgishi and M. Kasahara, Cryptosystems based on pairing, Proceedings of Symposium on Cryptography and Information Security, SCIS 2000, (2000)

[16] A. V. Sutherland, Computing Hilbert class polynomials with the Chinese remainder theorem, Math. Comp., Vol. 80, pp.501-538, (2011)

[17] F. Vercauteren, Optimal Pairings, IEEE Transactions on Information Theory, Vol. 56, Vo. 1, pp.455-461, (2010).

[18] C. Zhao, F. Zhang and J. Huang, A Note on the Ate Pairing, International Journal of Information Security, Vol. 7, No. 6, Springer, pp.379-382, (2008).