Universally Constructing 12-th Degree Extension Field for Ate Pairing

Masaaki Shirase

School of Systems Information, Future University Hakodate,
116-2 Kamedanakano, Hakodate, Hokkaido 041-8655, Japan
shirase@fun.ac.jp

Abstract. We need to perform arithmetic in $\mathbb{F}_{p(z)^{12}}$ to use Ate pairing on a Barreto-Naehrig (BN) curve, where $p(z)$ is a prime given by $p(z) = 36z^4 + 36z^3 + 24z^2 + 6z + 1$ with an integer z. In many implementations of Ate pairing, $\mathbb{F}_{p(z)^{12}}$ has been regarded as the 6-th extension of $\mathbb{F}_{p(z)^2}$, and it has been constructed as $\mathbb{F}_{p(z)^{12}} = \mathbb{F}_{p(z)^2}[v]/(v^6 - \xi)$ for an element $\xi \in \mathbb{F}_{p(z)^2}$ such that $v^6 - \xi$ is irreducible in $\mathbb{F}_{p(z)^2}[v]$. Such ξ depends on the value of $p(z)$, and we may use mathematic software to find ξ. This paper shows that when $z \equiv 7, 11 \pmod{12}$ we can universally construct $\mathbb{F}_{p(z)^2}$ as $\mathbb{F}_{p(z)^{12}} = \mathbb{F}_{p(z)^2}[v]/(v^6 - u - 1)$, where $\mathbb{F}_{p(z)^2} = \mathbb{F}_{p(z)}[u]/(u^2 + 1)$.

Key words: pairing, Barreto-Naehrig curve, extension field, quadratic residue, cubic residue, Euler's conjecture.

1 Introduction

Many new cryptographic protocols, such as identity-based key agreement [18], identity-based encryption [6], identity-based signature [10], ring signature [20], keyword search encryption [5], efficient broadcast encryption [8], aggregate signature [7], and certificateless public key cryptography [1], can be constructed using pairings. Arithmetic in $\mathbb{F}_p$ and $\mathbb{F}_{p^k}$, which is the k-th extension of $\mathbb{F}_p$, is needed to implement pairing, and $\mathbb{F}_{p^d}$ is also needed when we use twisted pairing, which is suitable for fast implementation, where k and d are integers depending on E and p with $1 < d < k$. It is desirable for the definition polynomials for $\mathbb{F}_{p^k}$ and $\mathbb{F}_{p^d}$ to have fewer terms and smaller coefficients to fast implement pairings. However, the form of these polynomials depends on the prime p in general. Therefore, we have to change these definition polynomials when p is changed each time.

Ate pairing, which this paper targets, is one of the fastest pairings due to fewer loops of Miller's algorithm and the availability of the twist technique. When we implement Ate pairing on a Barreto-Naehrig (BN) curve [3], which is most suitable for 128-bit security, we need to implement finite fields, $\mathbb{F}_p$, $\mathbb{F}_{p^2}$, and $\mathbb{F}_{p^{12}}$. $\mathbb{F}_{p^2}$ can be constructed as $\mathbb{F}_{p^2} = \mathbb{F}_p[u]/(u^2 - \lambda)$ such that λ is quadratic non-residue modulo p. Since $\mathbb{F}_{p^{12}}$ is the 6-th extension of $\mathbb{F}_{p^2}$, $\mathbb{F}_{p^{12}}$ can be constructed as $\mathbb{F}_{p^{12}} = \mathbb{F}_{p^2}[v]/(v^6 - \xi)$ with $\xi \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$, where $v^6 - \xi$ is irreducible in

$\mathbb{F}_{p^2}[v]$. There are specific examples of such ξ's corresponding to some p's [9] or methods constructing such ξ's, which require cubic residue judgment modulo p and depending on p's [3, 4]. However, a method for universally constructing $\mathbb{F}_{p^{12}}$ independent from p is not yet known.

A method for universally constructing the 12-th extension field for Ate pairing is proposed. Specifically, this paper shows that if primes are given by $p(z) = 36z^4 + 36z^3 + 24z^2 + 6z + 1$ with $z \equiv 7, 11 \pmod{12}$, $\mathbb{F}_{p(z)^{12}}$ can be universally constructed as $\mathbb{F}_{p(z)^2} = \mathbb{F}_{p(z)}[u]/(u^2+1)$, and $\mathbb{F}_{p(z)^{12}} = \mathbb{F}_{p(z)^2}[v]/(v^6 - \xi)$ ($\xi = u+1$). Such $p(z)$'s are used to generate a BN curve, and such primes are called *BN primes* in this paper. Note that the proposed construction of $\mathbb{F}_{p(z)^{12}}$ is suitable for fast implementation because all coefficients of the definition polynomials are 1 or -1. To prove this, we need Euler's conjecture on cubic residue modulo p. To apply Euler's conjecture to a prime p, we have to represent p as $p = a^2 + 3b^2$ for integers a and b. However, it is generally not easy to find such a and b if p is so large that these integers are used for practical cryptographic applications. However, applying Euler's conjecture to BN primes is easy because each BN prime $p(z)$ is represented as $p(z) = (6z^2 + 3z + 1)^2 + 3z^2$, that is, we can set $a = 6z^2 + 3z + 1$ and $b = z$ for all z's. This representation of $p(z)$ derives the result of this paper.

2 Elliptic Curve and Pairing

This section explains elliptic curve, twist, and pairing.

2.1 Elliptic Curve

Let p be a prime ≥ 5, and let q be the power of p. For an elliptic curve over $\mathbb{F}_q$,

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

the set $E(\mathbb{F}_q)$ of $\mathbb{F}_q$ rational points on E is defined as

$$E(\mathbb{F}_q) = \{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\},$$

where $\mathcal{O}$ is the point at infinity. $E(\mathbb{F}_q)$ forms an additive group with zero $\mathcal{O}$.

The following integer t is called the trace of $E(\mathbb{F}_q)$.

$$t = q + 1 - \#E(\mathbb{F}_q)$$

Let r be the largest prime factor of $\#E(\mathbb{F}_q)$. Then the smallest integer $k \geq 1$ satisfying $r | (q^k - 1)$ is called the embedding degree.

For two elliptic curves E and E' over $\mathbb{F}_q$, E' is called a twist of E of degree d if there exists an isomorphism $\psi_d : E' \to E$ and d is minimal[1]. If there is such a map ψ, d is equal to 1, 2, 3, 4 or 5 [19, Proposition X.5.4]. Table 1 lists the form of twist E' of each degree d of E, the isomorphic map ψ_d, and $\#E(\mathbb{F}_q)$.

[1] E' is often not called the twist if $d = 1$, however, in this paper E' with $d = 1$ is also called the twist.

Table 1. Form of twist E' of E of each degree d, isomorphism ψ_d, and $\#E'(\mathbb{F}_q)$

d	E'	$\psi_d : E' \to E$	$\#E'(\mathbb{F}_q)$	Expression $f$satisfies
2	$y^2 = x^3 + (a/h^2)x + b/h^3$	$(x, y) \to (hx, h^{3/2}y)$	$q + 1 + t$	
3	$y^2 = x^3 + b/h$	$(x, y) \to (h^{1/3}x, h^{1/2}y)$	$q + 1 - (3f - t)/2$	$t^2 - 4q = -3f^2$
			$q + 1 - (-3f - t)/2$	$t^2 - 4q = -3f^2$
4	$y^2 = x^3 + (a/h)x$	$(x, y) \to (h^{1/2}x, h^{3/4}y)$	$q + 1 + f$	$t^2 - 4q = -f^2$
			$q + 1 - f$	$t^2 - 4q = -f^2$
6	$y^2 = x^3 + b/h$	$(x, y) \to (h^{1/3}x, h^{1/2}y)$	$q + 1 - (-3f + t)/2$	$t^2 - 4q = -3f^2$
			$q + 1 - (3f + t)/2$	$t^2 - 4q = -3f^2$

2.2 Pairing

Let r be a prime, G_1 and G_2 be additive groups of r elements, and G_3 be a multiplicative group of r elements. A map $e : G_1 \times G_2 \to G_3$ is called pairing if it is bilinear (e.g., $e(aP, bQ) = e(P, Q)^{ab}$ is satisfied for any $P \in G_1, Q \in G_2$ and a, b are integers) and non-degeneracy (e.g., there exist $P \in G_1$ and $Q \in G_2$ such that $e(P, Q) \neq 1$).

Ate pairing is one of the pairings that have the smallest computational cost, in which G_1 and G_2 are groups based on elliptic curves. When an elliptic curve E over a prime field $\mathbb{F}_p$ has the embedding degree 12 and has the 6-th twist E', where E is regarded as over $\mathbb{F}_{p^2}$ not $\mathbb{F}_p$ (BN curve described in Sec. 2.3 is an example of such a curve), the computational cost of Ate pairing can be additionally reduced using the twist technique [11] and the map $\psi_6 : E' \to E$ explained in Sec. 2.1 and Table 1. In the case where such an elliptic curve is used to define Ate pairing, Ate pairing is a bilinear map given by

$$E(\mathbb{F}_p)[r] \times E'(\mathbb{F}_{p^2})[r] \to \mathbb{F}^*_{p^{12}}, \tag{2}$$

where r is the largest prime factor of $\#E(\mathbb{F}_p)$. Ate pairing is accurately defined as $e(P, Q) = f_{t,Q'}(P)^{(q^k-1)/r} \in \mathbb{F}^*_{p^{12}}$ with the function f whose divisor satisfies $(f_{t,Q'}) = t(Q') - (tQ') - (t - 1)(\mathcal{O})$, where $Q' = \psi_6(Q)$. Therefore, we need to perform arithmetic on $\mathbb{F}_p$, $\mathbb{F}_{p^2}$, and $\mathbb{F}_{p^{12}}$ to implement the Ate pairing of Eq. (2).

2.3 Barreto-Naehrig (BN) Curve

Barreto and Naehrig proposed a method for efficiently constructing elliptic curves with the embedding degree of 12 and a twist of degree of 6 [3].

Let $t(z), n(z), p(z)$ be polynomials in z given by

$$\left.\begin{aligned} t(z) &= 6z^2 + 1, \\ n(z) &= 36z^4 + 36z^3 + 18z^2 + 6z + 1, \\ p(z) &= n(z) + t(z) - 1 \\ &= 36z^4 + 36z^3 + 24z^2 + 6z + 1. \end{aligned}\right\} \tag{3}$$

In this paper primes $p(z)$ with an integer z are called *BN primes*. By fixing a BN prime $p(z)$ and choosing b at random, an elliptic curve,

$$E : y^2 = x^3 + b,$$

always has the embedding degree of 12, and $\#E(\mathbb{F}_q)$ is equal to $n(z)$ with possibility of 1/6. Then, when we would like to construct an elliptic curve over $\mathbb{F}_{p(z)}$ whose order is $n(z)$, we first choose a coefficient b of $E : y^2 = x^3 + b$ at random, next we check whether E is desirable as follows: 1) picking up a point $P \in E(\mathbb{F}_{p(z)})$, 2) computing $n(z)P$, and 3) if it is equal to $\mathcal{O}$, then E is a desirable curve, if not we choose another b.

Although we generally need a high cost process in the complex multiplication (CM) method [2] to construct elliptic curves of desirable order, the process becomes only checking order using a BN curve. Therefore, a BN curve is one of pairing-friendly elliptic curves that are most efficiently constructed. Moreover, the embedding degree of 12 of a BN curve is most suitable for 128-bit, which is expected to become standard security [15], corresponding to 3,072-bit RSA and 256-bit elliptic curve cryptography.

Therefore, a BN curve is easy to construct and has the desirable embedding degree of 12. There are variants of Ate pairing, R-ate [13] and Xate [17], which are defined on only a BN curve and have smaller computational cost than general Ate pairing.

3 Current Construction Methods of 12-th Extension Field

As described in Sec. 2.2, to implement Ate pairing on a BN curve over $\mathbb{F}_p$, we need to perform arithmetic not only on $\mathbb{F}_p$ but also on $\mathbb{F}_{p^2}$ and $\mathbb{F}_{p^{12}}$. We may construct $\mathbb{F}_{p^2}$ as $\mathbb{F}_{p^2} = \mathbb{F}_p[u]/(u^2 - \lambda)$ for quadratic non-residue element λ modulo p. To construct $\mathbb{F}_{p^{12}}$ we have to find $\xi \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ such that $v^6 - \xi$ is irreducible in $\mathbb{F}_{p^2}[v]$. After that, we can construct $\mathbb{F}_{p^2}$ as $\mathbb{F}_{p^{12}} = \mathbb{F}_{p^2}[v]/(v^6 - \xi)$.

Since the computational cost of arithmetic in $\mathbb{F}_{p^2}$ and $\mathbb{F}_{p^{12}}$ greatly depends on λ and ξ, we have to carefully select them. When λ is regarded as an integer, $\lambda = -1$ is one of the best selections possible because its absolute value is the smallest. Similarly, when ξ is represented as $\xi = au + b \in \mathbb{F}_{p^2} (= \mathbb{F}_p[u]/(u^2 - \lambda))$, $\xi = u + 1$ is one of the best selections possible because its coefficients are the smallest.

Explicitly finding quadratic non-residue element λ modulo p is easy using the quadratic residue theory [12]. On the other hand, explicitly finding ξ is much more difficult.

Barreto and Naehrig showed that such ξ always existed for BN primes p, and that ξ might be $\xi = (\nu^2\mu^3)^{-1}$, where ν was cubic non-residue modulo p and μ was non-square in $\mathbb{F}_{p^2}$ [3]. However, how to find such μ was not explained, and ξ had to be re-selected when changing p.

Devegili et al. dealt with implementation of pairing using a BN curve and constructed $\mathbb{F}_{p^2} = \mathbb{F}_p[u]/(u^2 + 2), \mathbb{F}_{p^{12}} = \mathbb{F}_{p^2}[v]/(v^6 - \xi)$ with $\xi = -u - 1$ for

a specific p [9]. They described that u^2+2 was always irreducible when $p \equiv 1 \pmod 8$. On the other hand, they described that there only always existed ξ such that $(v^6-\xi)$ was irreducible when $p \equiv 1 \pmod 6$, however, they did not give any method on how to find such ξ.

Benger and Scott proposed methods for construct extension fields for various pairings [4]. For the 12-th extension field for a BN curve, if a^2+b^2 was quadratic non-residue and cubic non-residue modulo p, we could construct $\mathbb{F}_{p^{12}}$ as $\mathbb{F}_{p^{12}} = \mathbb{F}_p(\sqrt{-1}, (a-b\sqrt{-1})^{1/6})$. However, they did not explain when a^2+b^2 was cubic non-residue.

As mentioned above, current methods for constructing $\mathbb{F}_{p^{12}}$ for Ate pairing using BN curve are not universal, that is, these methods require cubic residue judgment modulo each p, and when p is changed we have to reconstruct $\mathbb{F}_{p^{12}}$. Then, we have the following question.

Question 1.
Does there exist a method for universally constructing $\mathbb{F}_{p^{12}}$ independent from p?

The purpose of this paper is to give a solution to Question 1.

4 Preliminary

This section introduces two known theorems needed for solving Question 1. The first is Euler's conjecture[2] on cubic residue [14], and the second is for the irreducibility of binomials [16].

Let p be a prime with $p \equiv 1 \pmod 3$. If $a \in \mathbb{F}_p^*$ is written as $a = b^3$ for some $b \in \mathbb{F}_p^*$, a is called cubic residue modulo p and denoted by

$$\left(\frac{a}{p}\right)_3 = 1.$$

If a is not cubic residue modulo p, a is called cubic non-residue modulo p.

Theorem 1 (Euler's Conjecture).
(a) Let p be a prime with $p \equiv 1 \pmod 3$. Then p can be always written as $p = a^2+3b^2$ with integers a and b. [3]
(b) Let p be a prime, and let a and b be integers as stated in (a). Then

$$\left(\frac{2}{p}\right)_3 = 1 \text{ if and only if } 3|b. \tag{4}$$

Proof) Refer to [14]. □

[2] Although Euler's conjecture is called "conjecture", it has already been proven.
[3] The theorem just states that representation $p = a^2+3b^2$ exists, and it does not give how to find such a and b.

Theorem 2.
Let t be an integer with $t \geq 2$, and let $a \in \mathbb{F}_q^*$. Then a binomial $x^t - a$ is irreducible in $\mathbb{F}_q[x]$ if and only if the following two conditions are satisfied:
(a) each prime factor of t divides the order e of a in $\mathbb{F}_q^*$, but not $(q-1)/e$.
(b) $q \equiv 1 \pmod 4$ if $t \equiv 0 \pmod 4$.

Proof) Refer to [16]. □

5 Proposed Theorem – Constructing 12-th Extension Field of BN Primes

This section proves the following theorem for universally constructing the 12-th extension field for Ate pairing using BN curves.

Theorem 3 (Proposed Theorem).
Let $p(z) = 36z^4 + 36z^3 + 24z^2 + 6z + 1$ be a BN prime with $z \equiv 7, 11 \pmod{12}$. Then $\mathbb{F}_{p^{12}}$ can be constructed as follows:

$$\mathbb{F}_{p(z)^2} = \mathbb{F}_{p(z)}[u]/(u^2+1),$$
$$\mathbb{F}_{p(z)^{12}} = \mathbb{F}_{p(z)^2}[v]/(v^6 - u - 1).$$

□

Theorem 3 states that $\mathbb{F}_{p(z)^{12}}$ can be universally constructed for all BN primes $p(z)$ with $z \equiv 7, 11 \pmod{12}$, and gives a solution to Question 1. Moreover, in the proposed construction of $\mathbb{F}_{p(z)^{12}}$, all coefficients of the definition polynomials (e.g., u^2+1 and v^2-u-1) are ± 1, then the construction of $\mathbb{F}_{p(z)^{12}}$ is suitable for efficient implementation of Ate pairing. Sections 5.1 and 5.2 give lemmas needed to prove Theorem 3, and Sec. 5.3 completes the proving of Theorem 3.

5.1 Irreducibility of $v^6 - \xi$

When $\mathbb{F}_{p^{12}}$ is constructed as $\mathbb{F}_{p^{12}} = \mathbb{F}_{p^2}[v]/(v^6 - \xi)$ as Theorem 3, $v^6 - \xi$ has to be irreducible in $\mathbb{F}_{p^2}[v]$. The following lemma deduced from Theorem 2 shows that irreducibility judgment of $v^6 - \xi$ is reduced to quadratic and cubic residue judgments.

Lemma 1.
Let $p(z)$ be a BN prime and let $\xi \in \mathbb{F}_{p(z)^2} \setminus \mathbb{F}_{p(z)}$ be not square and not cube in $\mathbb{F}_{p(z)^2}$. Then the polynomial $v^6 - \xi$ is irreducible in $\mathbb{F}_{p(z)^2}[v]$.

(Proof) We apply Theorem 2 to the case of $t = 6$. Let α be a generator of $\mathbb{F}_{p(z)^2}^*$. It is seen that $p(z)^2 \equiv 1 \pmod{12}$ for any integer z; therefore, we write $p(z)^2 - 1 = 12\mathcal{Q}$ ($\mathcal{Q}$ is an integer.) Since ξ is neither square nor cube in $\mathbb{F}_{p(z)^2}$, we may write $\xi = \alpha^{6s+1}$ or $\xi = \alpha^{6s+5}$ for some integer s.

Suppose $\xi = \alpha^{6s+1}$. Let $\mathcal{R}$ be an integer defined as

$$\mathcal{R} = gcd(6s+1, p(z)^2 - 1(= 12\mathcal{Q})).$$

Then $\mathcal{R}$ is neither a multiple of 2 nor 3, and the order of ξ in $\mathbb{F}^*_{p(z)^2}$ is written as $\frac{12Q}{R}$. Note that $\mathcal{R}|12Q$ from the definition of $\mathcal{R}$, then $\frac{12Q}{R}$ is a multiple of 6. Therefore, ξ satisfies the first condition of Theorem 2-(a). It is seen that ξ also satisfies the second condition because

$$\frac{p(z)^2 - 1}{\text{the order of } \xi \text{ in } \mathbb{F}_{p(z)^2}} = \frac{12\mathcal{Q}}{\frac{12Q}{\mathcal{R}}} = \mathcal{R},$$

and $\mathcal{R}$ is not a multiple of 2 nor 3. Therefore, $v^6 - \xi$ is irreducible in $\mathbb{F}_{p(z)^2}[v]$ due to Theorem 2.

For $\xi = \alpha^{6s+5}$, we can similarly show that $v^6 - \xi$ is irreducible in $\mathbb{F}_{p(z)^2}[v]$. □

The following lemma shows that square and cube judgments of an element in $\mathbb{F}_{p^2}$ are reduced to quadratic and cubic residue judgments modulo p.

Lemma 2.
Let p be a prime with

$$p \equiv 3 \pmod 8, \text{ and } (p+1)/4 \not\equiv 0 \pmod 3, \tag{5}$$

which means that $2p' + 1 \not\equiv 0 \pmod 3$ is satisfied when p is written as $p = 8p' + 3$. And let $\mathbb{F}_{p^2}$ be constructed as $\mathbb{F}_{p^2} = \mathbb{F}_p[u]/(u^2+1)$. (Note that such construction of $\mathbb{F}_{p^2}$ is possible if $p \equiv 3 \pmod 4$.) Then the following statements are satisfied.
(a) The order of $u+1$ in $\mathbb{F}^*_p$ is equal to 4 times the order of -4 in $\mathbb{F}^*_p$.
(b) $u+1$ is a square in $\mathbb{F}_{p^2}$ if and only if -1 is quadratic residue modulo p.
(c) $u+1$ is a cube in $\mathbb{F}_{p^2}$ if and only if 2 is cubic residue modulo p.

Proof) (a) In $\mathbb{F}_{p^2} = \mathbb{F}_p[u]/(u^2+1)$, $u^2 + 1 = 0$ is held, then we have

$$(u+1)^2 = 2u,\ (u+1)^3 = 2u - 2,\ (u+1)^4 = -4. \tag{6}$$

Therefore, let t be the order of -4 in $\mathbb{F}^*_p$, then $(u+1)^{4t} = 1$ is held. This means the order of $u+1$ in $\mathbb{F}_{p^2}$ is a divisor of $4t$. To show that the order of $u+1$ in $\mathbb{F}_{p^2}$ is equal to $4t$, it is enough to show $(u+1)^s \neq 1$ for any s with $1 \leq s < 4t$.

Let $s' = \lfloor s/4 \rfloor$ for $1 \leq s < 4t$. Then $(u+1)^s$ is written as follows due to Eq. (6).

$$(u+1)^s = \begin{cases} (-4)^{s'} & \text{if } s \equiv 0 \pmod 4 \\ (-4)^{s'} \cdot (u+1) & \text{if } s \equiv 1 \pmod 4 \\ (-4)^{s'} \cdot 2u & \text{if } s \equiv 2 \pmod 4 \\ (-4)^{s'} \cdot (2u-2) & \text{if } s \equiv 3 \pmod 4 \end{cases}$$

Due to definitions of t and s', we have $(-4)^{s'} \neq 1$, and since $u, 2u, 2u-2 \notin \mathbb{F}_p$, each of them is never the inverse of $(-4)^{s'} \in \mathbb{F}_p$. We then have $(-4)^{s'} \cdot (u+1) \neq$

1, $(-4)^{s'} \cdot 2u \neq 1$, and $(-4)^{s'} \cdot (2u-2) \neq 1$. Therefore, we have $(u+1)^s \neq 1$, which completes the proving that the order of $(u+1)$ in $\mathbb{F}_{p^2}^*$ is equal to $4t$.
(b) The order of each element $a \in \mathbb{F}_p^*$ is a divisor of $p-1$ since a satisfies $a^{p-1} = 1$. Let $(p-1)/w$ be the order of -4 in $\mathbb{F}_p^*$ for an integer w. Then the order of $(u+1)$ in $\mathbb{F}_{p^2}^*$ is written as $4(p-1)/w$ due to (a), and then we have

$$\begin{aligned} u+1 \text{ is a square in } \mathbb{F}_{p^2} &\Leftrightarrow (p^2-1)/2 \text{ is a multiple of } 4(p-1)/w \\ &\Leftrightarrow (p^2-1)/2 \div 4(p-1)/w \text{ is an integer} \\ &\Leftrightarrow w(2p'+1)/2 \text{ is an integer} \\ &\Leftrightarrow w/2 \text{ is an integer (i.e., } w \text{ is even)} \\ &\Leftrightarrow -4 \text{ is quadratic residue modulo } p \\ &\Leftrightarrow -1 \text{ is quadratic residue modulo } p. \end{aligned}$$

Therefore, (b) is shown.
(c) Let $(p-1)/w$ be the order of -4 in $\mathbb{F}_p^*$ as well as the proof of (b). Then the order of $(u+1) \in \mathbb{F}_{p^2}^*$ is written as $4(p-1)/w$, and then we have

$$\begin{aligned} u+1 \text{ is a cube in } \mathbb{F}_{p^2} &\Leftrightarrow (p^2-1)/3 \text{ is a multiple of } 4(p-1)/w \\ &\Leftrightarrow (p^2-1)/3 \div 4(p-1)/w \text{ is an integer} \\ &\Leftrightarrow w(2p'+1)/3 \text{ is an integer} \\ &\Leftrightarrow w/3 \text{ is an integer} \\ &\quad \text{(since } 2p'+1 \text{ is not a multiple of 3} \\ &\quad \text{due to the assumption)} \\ &\Leftrightarrow -4 \text{ is cubic residue modulo } p \\ &\Leftrightarrow 2 \text{ is cubic residue modulo } p. \end{aligned}$$

Therefore, (c) is shown. □

Any BN prime $p(z)$ satisfies the condition (5) of Lemma 2 if $z \equiv 7, 11 \pmod{12}$. Then Lemmas 1 and 2 reduce the irreducibility judgment of $v^6 - \xi$ with $\xi = u+1$ in $\mathbb{F}_{p(z)^2}[v]$ to square residue judgment of -1 and cubic residue judgment of 2 modulo $p(z)$.

5.2 Square and Cubic Residue Modulo BN Prime

BN primes have a special property, making applying Theorem 1 easy. We have to find integers a and b such that $p = a^2 + 3b^2$ for a prime p when we apply Theorem 1 to p, this task is generally difficult. On the other hand, any BN prime $p(z) = 36z^4 + 36z^3 + 24z + 6z + 1$ is written as

$$p(z) = (6z^2 + 3z + 1)^2 + 3z^2,$$

then we set $a = 6z^2 + 3z + 1, b = z$. This fact derives the following lemma.

Lemma 3.
For any BN prime $p(z) = 36z^4 + 36z^3 + 24z + 6z + 1$, the following (a) and (b)

are satisfied:
(a) **Quadratic Residue of −1:**

$$\left(\frac{-1}{p(z)}\right) = \begin{cases} 1 & \text{if } z \text{ is even} \\ -1 & \text{if } z \text{ is odd,} \end{cases}$$

where $(-)$ *is the Legendre symbol.*
(b) **Cubic Residue of 2:**

$$\left(\frac{2}{p(z)}\right)_3 \begin{cases} = 1 & \text{if } z \equiv 0 \pmod 3 \\ \neq 1 & \text{if } z \equiv 1, 2 \pmod 3. \end{cases}$$

(Proof) (a) If z is even, we have $\left(\frac{-1}{p(z)}\right) = 1$ since $p(z) \equiv 1 \pmod 4$ for any integer z. If z is odd, we have $\left(\frac{-1}{p(z)}\right) = -1$ since $p(z) \equiv 3 \pmod 4$ for any integer z.
(b) For any BN prime $p(z)$ is written as $p(z) = (6z^2 + 3z + 1)^2 + 3z^2$. Then we can set $a = 6z^2 + 3z + 1, b = z$ at Theorem 2. Due to Theorem 2, we have

$$\begin{aligned} \left(\frac{2}{p(z)}\right)_3 = 1 &\Leftrightarrow 3|z \qquad \text{(due to Theorem 2-(b) and Eq. (7))} \\ &\Leftrightarrow z \equiv 0 \pmod 3 \end{aligned}$$

□

5.3 Proof of Theorem 3

Since z is odd, -1 is quadratic non-residue modulo $p(z)$ due to Lemma 3-(a); therefore, $\mathbb{F}_{p(z)^2}$ is written as $\mathbb{F}_{p(z)^2} = \mathbb{F}_{p(z)}[u]/(u^2 + 1)$.

For construction of $\mathbb{F}_{p(z)^{12}}$, first consider the case of $z \equiv 7 \pmod{12}$. Let z be $z = 12z' + 7$. Then we have $p(12z' + 7) \equiv 3 \pmod 8$ since $p(12z' + 7) = 8(93312z'^4 + 225504z'^3 + 204552z'^2 + 82539z' + 12500) + 3$. In addition, we have $(p(12z' + 7) + 1)/4 \not\equiv 0 \pmod 3$ since $(p(12z' + 7) + 1)/4 = 3(62208z'^4 + 150336z'^3 + 136368z'^2 + 55026z' + 8333) + 2$. We then can apply Lemma 2 to $p(12z' + 7)$. We know that -1 is quadratic non-residue modulo $p(z)$ due to Lemma 3-(a), then $u + 1$ is non-square in $\mathbb{F}_{p(z)^2}$ due to Lemma 2-(b). We also know that 2 is cubic non-residue module $p(z)$ due to Lemma 3-(b), then $u + 1$ is non-cube in $\mathbb{F}_{p(z)^2}$ due to Lemma 2-(c). Therefore, $v^6 - (u + 1)$ is irreducible in $\mathbb{F}_{p(z)^2}[v]$ due to Lemma 1.

Next, consider the case of $z \equiv 11 \pmod{12}$. Let z be $z = 12z' + 11$. Then we have $p(12z' + 11) \equiv 3 \pmod 8$ since $p(12z' + 11) = 8(93312z'^4 + 349920z'^3 + 492264z'^2 + 307899z' + 72245) + 3$. In addition, we have $(p(12z' + 7) + 11)/4 \not\equiv 0 \pmod 3$ since $(p(12z' + 11) + 1)/4 = 3(62208z'^4 + 233280z'^3 + 328176z'^2 + 205266z' + 48163) + 2$, then we can apply Lemma 2 to $p(12z' + 11)$. The remainder of the proof is the same as the case of $z \equiv 7 \pmod{12}$. □

6 Conclusion

This paper has shown that the 12-th extension field for each BN prime $p(z)$ with $z \equiv 7, 11 \pmod{12}$ has been universally constructed as

$$\mathbb{F}_{p(z)^2} = \mathbb{F}_{p(z)}[u]/(u^2 + 1),$$

$$\mathbb{F}_{p(z)^{12}} = \mathbb{F}_{p(z)^2}[v]/(v^6 - \xi) \quad (\xi = u + 1).$$

In the current construction of $\mathbb{F}_{p^{12}}$, we have to change the definition polynomials when p is changed each time, and need cubic residue judgment, which is non-trivial. Then Question 1 of Sec. 3 is posed. On the other hand, with the proposed construction of $\mathbb{F}_{p(z)^{12}}$, we can fix the definition polynomials for $p(z)$ with $z \equiv 7, 11 \pmod{12}$, which gives a solution to Question 1. Moreover, all their coefficients are ± 1, which is suitable for efficient implementation of Ate pairing.

References

1. S. Al-Riyami and K. Peterson, "Certificateless public key cryptography," *ASIACRYPT 2003*, LNCS 2894, pp. 452-474, 2003.
2. A. Atkin and F. Morain, "Elliptic Curves and Primality Proving," *Math. Comp.* Vol. 61, No. 203, pp. 29-68, 1993.
3. P. Barreto and M. Naehrig, "Pairing-friendly elliptic curves of prime," *SAC 2005*, LNCS 3897, pp.319-331, 2006.
4. N. Benger and M. Scott, "Constructing Tower Extensions for the implementation of Pairing-Based Cryptography," Cryptology ePrint Archive, Report 2009/556, 2009.
5. D. Boneh, G. Crescenzo, R. Ostrovsky, and G. Persiano, Public Key Encryption with Keyword Search *EUROCRYPT 2004*, LNCS 3027, pp. 506-522, 2004.
6. D. Boneh and M. Franklin, "Identity based encryption from the Weil pairing," *SIAM Journal of Computing*, Vol. 32, No. 3, pp. 586-615, 2003.
7. D. Boneh, C. Gentry, B. Lynn, and H. Shacham, H, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," *EUROCRYPT 2003*, LNCS 2656, pp. 416-432, 2003.
8. D. Boneh, G. Gentry, and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys", *CRYPTO 2005*, LNCS 3621, pp. 258-275, 2005.
9. A. Devegili, M. Scott and R. Dahab, "Implementing Cryptographic Pairings over Barreto-Naehrig Curves," *Pairing 2007*, LNCS 4575, pp. 197-207, 2007.
10. F. Hess, "Exponent group signature schemes and efficient identity based signature schemes based on pairings", *SAC 2002*, LNCS 2595, pp. 310-324, 2002.
11. F. Hess, N. P. Smart, and F. Vercauteren, "The Eta pairing revisited", *IEEE Transactions on Information Theory*, Vol. 52, pp. 4595-4602, 2006.
12. N. Koblitz, *A course in number theory and cryptography*, Springer–Verlag, 1994.
13. E. Lee, H. Lee, and C. Park, "Efficient and generalized pairing computation on abelian varieties," IEEE Transactions of Information Theory, Vol.55, No.4, pp. 1793-1803, 2009.

14. F. Lemmermeyer, *Reciprocity laws*, Springer–Verlag, 1991.
15. A. Lenstra, "Selecting Cryptographic Key Sizes," Journal of Cryptology, Vol. 14, No. 4, pp. 255-293, 2001.
16. R. Lidl and H. Niederriter, *Introduction to finite fields and their applications*, Cambridge press, 1986.
17. Y. Nogami, M. Akane, Y. Sakemi, H. Kato, and Y. Morikawa, "Integer variable χ-based Ate pairing," *Pairing 2008*, LNCS 5209, pp. 178-191, 2008.
18. R. Sakai, K. Ohgishi, and M. Kasahara, "Cryptosystems based on pairing," In *SCIS 2000*, Japan.
19. J. Silverman, *The arithmetic of elliptic curves*, Springer–Verlag, 1986.
20. F. Zhang and K. Kim, "ID-Based Blind Signature and Ring Signature from Pairings," *ASIACRYPT 2002*, LNCS 2501, pp. 629-637, 2002.