








Efficient Ate-Based Pairing over the Attractive Classes of BN Curves

Yuki Nanjo¹(✉) , Md. Al-Amin Khandaker¹ , Masaaki Shirase² ,
Takuya Kusaka¹ , and Yasuyuki Nogami¹ 

¹ Graduate School of Natural Science and Technology,
Okayama University, Okayama, Japan
{yuki.nanjo,khandaker}@s.okayama-u.ac.jp
{kusaka-t,yasuyuki.nogami}@okayama-u.ac.jp

² Future University Hakodate, Hakodate, Hokkaido, Japan
shirase@fun.ac.jp

Abstract. This paper proposes two attractive classes of Barreto-Naehrig curve for ate-based pairing by imposing certain condition $\chi \equiv 7, 11 \pmod{12}$ on the integer χ that parameterizes the curve settings. The restriction results in an unparalleled way to determine a BN curve, its twisted curve coefficients, and obvious generator points. The proposed $\chi \equiv 11 \pmod{12}$ are found to be more efficient than $\chi \equiv 7 \pmod{12}$ together with pseudo 8-sparse multiplication in Miller's algorithm. The authors also provide comparative implementations for the proposal.

Keywords: Pairing · Tower of extension field · Barreto-Naehrig curve

1 Introduction

Pairing-Based Cryptography (PBC) provides several innovative protocols, e.g. ID-based encryption [6] and BLS short signatures [5] making it an inseparable tool of modern cryptography. The prerequisites for PBC are a pairing-friendly elliptic curve [9] and an efficient pairing algorithm. Over the years, several variants of Weil's pairing i.e. ate [7], χ -ate [15], optimal-ate [17] pairings have been evolved. However, to find a suitable pairing-friendly curve is a nontrivial task. In 2005 Barreto et al. [4] made a major breakthrough introducing parameterized pairing-friendly curve named as Barreto-Naehrig (BN) curve given as polynomial formulas of an integer. This work especially focuses on pairing in BN curve. A bilinear-pairing is an efficiently computable non-degenerate map $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_3$. Typically, \mathbb{G}_1 and \mathbb{G}_2 are additive cyclic sub-groups of order r defined over a finite extension field \mathbb{F}_{p^k} and \mathbb{G}_3 is a multiplicative cyclic sub-group of order r in $\mathbb{F}_{p^k}^*$. The embedding degree k ($k = 12$ for BN) is the smallest positive integer such that $r | (p^k - 1)$, where prime p and order r is given by polynomial formulas of integer χ .

When considering the pairing over BN curves, suitable parameter χ have to be found for which both p and r become an odd prime number. Then it comes to determining an elliptic curve $E : y^2 = x^3 + b$ to be a BN curve over the prime field \mathbb{F}_p . The probabilistic way to prove curve coefficient b is to choose a random b and check the group order until $\#E(\mathbb{F}_p) = r$. Moreover, a sextic twisted curve $E'(\mathbb{F}_{p^{12/d}})$ ($d = 6$) also have to be determined, since the Miller's algorithm for pairing in BN curve is calculated over E' . However, E' could not be determined immediately since there exist two possible types of the twisted curve with $d = 6$. As noted above, these initial settings require time-consuming computation. In addition to this, when selecting the parameters, the following cautions are considered for an efficient implementation of pairing. The Parameters have an effect on efficient towering; another prerequisite of efficient finite field arithmetic; one of the pivotal factors of efficient pairing implementation. Also, the parameters with a small Hamming weight result in reducing calculation amount of the Miller's algorithm and final exponentiation. Moreover, the authors found that not all parameters end up efficient line evaluation of Miller's algorithm due to the type of twisted curve E' . However, the conditions of suitable parameters have not clearly given at this point. This paper overcomes the aforementioned challenges of efficient pairing in BN curve by restricting parameter as mentioned below.

Our Contribution: The major contribution of this paper can be summarized as (i) offering two attractive classes of BN curves by restricting integer χ as $\chi \equiv 7, 11 \pmod{12}$. (ii) The restriction also results in an efficient tower of extension field construction given in [1]. (iii) Instantaneously determining the coefficient b in BN curve and resulting obvious rational points overcomes the probabilistic approach. (iv) The twisted curve and its coefficients can also be determined easily from the condition on χ . (v) Proposed parameter satisfying $\chi \equiv 11 \pmod{12}$ enables more efficient implementation pairing. Moreover, the authors implemented several candidate curves and compared performances for the lower Hamming weight.

Previous Works: BN curve is one of the most widely studied pairing-friendly curves. The most relevant work similar to this is Costello et al.'s [8] proposal on restricting the parameter for BLS curve for embedding degree 24. They also mention the efficiency of the Miller's algorithm. This paper does not only describes more details applying pseudo 8-sparse multiplication but also focus on the small Hamming weight of the parameter.

Organization of this Paper: Section 2 overviews several necessary backgrounds. Sections 3 and 4 give the required details with theoretic proofs of the proposal. The implementation results are compared in Sect. 5 and Sect. 6 which draws the conclusion.

2 Fundamentals

This section shows that the details of the necessary fundamentals of pairing over BN curve to keep the reference and for easy explanation of rest of the paper.

BN Curves: Barreto-Naehrig curve [4] is a class of non super-singular (ordinary) pairing-friendly elliptic curves of embedding degree $k = 12$ defined as $E/\mathbb{F}_p : y^2 = x^3 + b$. Its characteristic p , order r and Frobenius trace t are given as follows:

$$\begin{cases} p = p(\chi) = 36\chi^4 + 36\chi^3 + 24\chi^2 + 6\chi + 1, \\ r = r(\chi) = 36\chi^4 + 36\chi^3 + 18\chi^2 + 6\chi + 1, \\ t = t(\chi) = 6\chi^2 + 1. \end{cases} \quad (1)$$

where χ is an integer. In what follows, the parameter χ is called *BN parameter* and the prime p is called *BN prime*. If $\#E(\mathbb{F}_p) = r$, E becomes a BN curve.

Tower of the Extension Field: Pairing requires arithmetic operations in embedded extension fields. It is important to consider the way to construct the extension field since it affects to the efficiency of the pairing. Therefore, this paper especially focuses on the construction of efficient tower of the extension field. Bailey et al. [2] proposed the optimal extension field by the towering irreducible binomials. In the context of the pairing over BN curve, where $k = 12$, one of the way to construct the efficient extension field proposed by Aranha et al. [1] as follows:

$$\begin{cases} \mathbb{F}_{p^2} = \mathbb{F}_p[\alpha]/(\alpha^2 - (-1)), \\ \mathbb{F}_{p^6} = \mathbb{F}_{p^2}[\beta]/(\beta^3 - (\alpha + 1)), \\ \mathbb{F}_{p^{12}} = \mathbb{F}_{p^6}[\gamma]/(\gamma^2 - \beta), \end{cases} \quad (2)$$

where p is a BN prime and α, β, γ are one of the roots of the modular polynomials of $\mathbb{F}_{p^2}, \mathbb{F}_{p^6}$ and $\mathbb{F}_{p^{12}}$. The set of the basis elements constructing $\mathbb{F}_{p^{12}}$ vector is denoted as $\{1, \alpha, \beta, \alpha\beta, \beta^2, \alpha\beta^2, \gamma, \alpha\gamma, \beta\gamma, \alpha\beta\gamma, \beta^2\gamma, \alpha\beta^2\gamma\}$.

Ate-Based Pairing: While BN curve is applied in different variants of pairings, e.g. ate [7], optimal-ate [17] and χ -ate [15] pairing; the groups $\mathbb{G}_1, \mathbb{G}_2$ and \mathbb{G}_3 for such ate-based pairings are defined as $\mathbb{G}_1 = E(\mathbb{F}_{p^{12}})[r] \cap \text{Ker}(\phi - [1])$, $\mathbb{G}_2 = E(\mathbb{F}_{p^{12}})[r] \cap \text{Ker}(\phi - [p])$, $\mathbb{G}_3 = \mathbb{F}_{p^{12}}^*/(\mathbb{F}_{p^{12}}^*)^r$. $E(\mathbb{F}_{p^{12}})[r]$ denotes rational points of order r and $[s]$ denotes s times scalar multiplication for a rational point. ϕ denotes the Frobenius mapping given as $\phi : (x, y) \mapsto (x^p, y^p)$. $\text{Ker}(\cdot)$ is the kernel of \cdot , which means that $\text{Ker}(\cdot)$ is a set whose elements are mapped to an initial point by \cdot . In what follows, we consider $P \in \mathbb{G}_1 \subseteq E(\mathbb{F}_p)$ and $Q \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{12}})$. Then, optimal-ate $e_\alpha(Q, P)$ and χ -ate $e_\zeta(Q, P)$ pairing are given as follows:

$$\begin{aligned} e_\alpha(Q, P) &= \left\{ f_{6\chi+2, Q}(P) \cdot l_{[6\chi+2]Q, [p]Q}(P) \cdot l_{[6\chi+2+p]Q, [-p^2]Q}(P) \right\}^{\frac{p^{12}-1}{r}}, \\ e_\zeta(Q, P) &= \left\{ f_{\chi, Q}(P)^{(1+p^3)(1+p^{10})} \cdot l_{[\chi]Q, \phi^3([\chi]Q)}(P) \right. \\ &\quad \left. \cdot l_{[\chi]Q + \phi^3([\chi]Q), \phi^{10}([\chi]Q + \phi^3([\chi]Q))}(P) \right\}^{\frac{p^{12}-1}{r}}. \end{aligned}$$

where the first term of e_α and e_ζ denotes the output of Miller’s loop and the second and third terms are the line evaluations. An efficient way to calculate these line evaluation steps, called 7-sparse and pseudo 8-sparse multiplication are proposed in [12, 14]. The details of the line evaluation are discussed in Sect. 4.

3 Attractive Classes of BN Curves

This section shows that the proposed classes of BN curves can result in efficient pairing implementations. Table 1 shows two classes of the BN curve parameter, categorized as *Class 1* and *Class 2*. The conditions $\chi \equiv 7 \pmod{12}$ and $\chi \equiv 11 \pmod{12}$ are satisfied by *Class 1* and *Class 2*, respectively. The advantages of choosing such parameters are following.

- The efficient tower of $\mathbb{F}_{p^{12}}$ given in Eq. (2) can be constructed (See Lemma 1 below).
- The coefficients of the curve E/\mathbb{F}_p to be a BN curve can be determined uniquely. Once a BN parameter satisfying $\chi \equiv 7, 11 \pmod{12}$ is found, the BN curves are immediately given as $y^2 = x^3 + 2^{6l-1}$, $y^2 = x^3 + 2^{6l+1}$, where l is an integer (See Lemma 2 below). The curve $y^2 = x^3 + 2^{6l+1}$ can have an obvious generator point $(-2^{2l}, \pm 2^{3l})$. And also $y^2 = x^3 + 2^{6l-1}$ has $(-2^{2l}, \pm(-2)^{-1/2} \cdot 2^{3l})$, where -2 is a quadratic residue in \mathbb{F}_p since -1 and 2 are quadratic non-residues in \mathbb{F}_p (See Theorem 1).
- The correct twisted curves can also be determined uniquely. The parameter $\chi \equiv 7, 11 \pmod{12}$ results in twisted curve as $y^2 = x^3 + 2^{6l-1}(\alpha + 1)$, $y^2 = x^3 + 2^{6l+1}(\alpha + 1)^{-1}$ (See Lemma 3 below).

Table 1. Two attractive classes of the BN curve

Type	Condition of χ	Efficient tower of	BN curve E/\mathbb{F}_p	Twisted curve E'/\mathbb{F}_{p^2}
<i>Class 1</i>	$\chi \equiv 7 \pmod{12}$	✓	$y^2 = x^3 + 2^{6l-1}$	$y^2 = x^3 + 2^{6l-1}(\alpha + 1)$
<i>Class 2</i>	$\chi \equiv 11 \pmod{12}$	✓	$y^2 = x^3 + 2^{6l+1}$	$y^2 = x^3 + 2^{6l+1}(\alpha + 1)^{-1}$

3.1 Using Parameters Satisfying $\chi \equiv 7, 11 \pmod{12}$

This subsection shows how the proposed condition of χ can result in efficient tower of $\mathbb{F}_{p^{12}}$ by using the theorem of quadratic and cubic residue in \mathbb{F}_p .

Theorem 1. *Let $(-)$ be the Legendre symbol and $(-)_3$ be a multiplicative function defined as follows:*

$$\left(\frac{\mu}{p}\right)_3 \begin{cases} = 1 & \text{if } \mu \text{ is a cubic residue in } \mathbb{F}_p, \\ \neq 1 & \text{if } \mu \text{ is a cubic non-residue in } \mathbb{F}_p. \end{cases}$$

If the characteristic p is a BN prime; quadratic and cubic residue properties for certain elements in \mathbb{F}_p are given by the condition of BN parameter χ as follows:

$$(a) \left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } \chi \equiv 0 \pmod{2}, \\ -1 & \text{if } \chi \equiv 1 \pmod{2}. \end{cases} \quad (3a)$$

$$(b) \left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } \chi \equiv 0, 1 \pmod{4}, \\ -1 & \text{if } \chi \equiv 2, 3 \pmod{4}. \end{cases} \quad (3b)$$

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

Proof. For the details of the proof, please refer to [16, §5.1]. \square

Lemma 1. *If the characteristic p is a BN prime and χ satisfies $\chi \equiv 7, 11 \pmod{12}$, the efficient tower of the extension field given in Eq. (2) can be constructed.*

Proof. To construct $\mathbb{F}_p \xrightarrow{\alpha^2 - (-1)} \mathbb{F}_{p^2}$, $\alpha^2 - (-1)$ should be an irreducible polynomial over \mathbb{F}_p . Therefore, -1 has to be a quadratic non-residue in \mathbb{F}_p . Then, χ should be satisfying $\chi \equiv 1 \pmod{2}$ from Eq. (3a). In the similar way, when constructing $\mathbb{F}_{p^2} \xrightarrow{\beta^3 - (\alpha+1)} \mathbb{F}_{p^6} \xrightarrow{\gamma^2 - \beta} \mathbb{F}_{p^{12}}$, $(\alpha + 1)$ should be a quadratic and cubic non-residue in \mathbb{F}_{p^2} . This condition means that $2 \in \mathbb{F}_p$ has to be a quadratic and cubic non-residue as shown in the following equations.

$$\begin{aligned} (\alpha + 1)^{\frac{p^2-1}{2}} &= ((\alpha + 1)^p(\alpha + 1))^{\frac{p-1}{2}} = 2^{\frac{p-1}{2}} = -1, \\ (\alpha + 1)^{\frac{p^2-1}{3}} &= ((\alpha + 1)^p(\alpha + 1))^{\frac{p-1}{3}} = 2^{\frac{p-1}{3}} \neq 1. \end{aligned}$$

According to Eqs. (3b) and (3c), if 2 is a quadratic and cubic non-residue in \mathbb{F}_p , χ should satisfy $\chi \equiv 1, 2 \pmod{3}$, $\chi \equiv 2, 3 \pmod{4}$. Therefore, the condition to construct efficient extension field is given by $\chi \equiv 1, 2 \pmod{3}$, $\chi \equiv 3 \pmod{4}$ which means $\chi \equiv 7, 11 \pmod{12}$. \square

From the proposed conditions, it is clear that it shrinks the probability of getting smaller Hamming weight (HW) of χ . Smaller Hamming weight (less than 6) is a catalyst for efficient Miller's algorithm and final exponentiation. Since, according to [3], for 128-bit security, the $\lceil \log_2 \chi \rceil = 114$ is expected. Therefore, an exhaustive search can result in smaller Hamming weight along with the proposed conditions.

3.2 Determining BN Curves and Twisted Curves

In this part, we show how uniquely the BN curves' and its twisted curves' coefficients can be determined in E/\mathbb{F}_p and E'/\mathbb{F}_{p^2} , respectively. For the reference in our proof, we recall the theorem given by Shirase as follows:

Theorem 2. Let p be a BN prime, and let $n_0 = n_0(\chi)$, $n_1 = n_1(\chi)$, $n_2 = n_2(\chi)$, $n_3 = n_3(\chi)$, $n_4 = n_4(\chi)$ and $n_5 = n_5(\chi)$ be polynomials defined as

$$\begin{aligned} n_0(\chi) &= 12\chi^2(3\chi^2 + 3\chi + 1), & n_1(\chi) &= 36\chi^4 + 36\chi^3 + 18\chi^2 + 1, \\ n_2(\chi) &= 3(12\chi^4 + 12\chi^3 + 10\chi^2 + 2\chi + 1), & n_3(\chi) &= 4(9\chi^4 + 9\chi^3 + 9\chi^2 + 3\chi + 1), \\ n_4(\chi) &= 3(12\chi^4 + 12\chi^3 + 10\chi^2 + 4\chi + 1), & n_5(\chi) &= 36\chi^4 + 36\chi^3 + 18\chi^2 + 6\chi + 1. \end{aligned}$$

Then, the group orders of $E_2 : y^2 = x^3 + 2$ are determined as follows:

$$\#E_2(\mathbb{F}_p) = \begin{cases} n_0 & \text{if } \chi \equiv 0, 9 \pmod{12}, \\ n_1 & \text{if } \chi \equiv 7, 10 \pmod{12}, \\ n_2 & \text{if } \chi \equiv 5, 8 \pmod{12}, \\ n_3 & \text{if } \chi \equiv 3, 6 \pmod{12}, \\ n_4 & \text{if } \chi \equiv 1, 4 \pmod{12}, \\ n_5 & \text{if } \chi \equiv 2, 11 \pmod{12}. \end{cases} \quad (4)$$

Proof. Please refer to [16, § 5.2]. □

Remark 1. The group orders n_0, n_1, n_2, n_3, n_4 and n_5 can be denoted as

$$\begin{aligned} n_0 &= p + 1 - (3f + t)/2, & n_1 &= p + 1 - (3f - t)/2, & n_2 &= p + 1 - (-t), \\ n_3 &= p + 1 - (-3f - t)/2, & n_4 &= p + 1 - (-3f + t)/2, & n_5 &= p + 1 - t, \end{aligned}$$

where p is a BN prime, t is a Frobenius trace and $f = f(\chi) = 6\chi^2 + 4\chi + 1$ is an integer. From the definition [4], an elliptic curve which has the order $n_5 = r$ becomes BN curve.

Remark 2. The divisibility of the group order by 2 or 3 of the curve $E_b(\mathbb{F}_{p^k}) : y^2 = x^3 + b$ depends on its coefficient. If the coefficient b is a cubic residue in \mathbb{F}_{p^k} , $\#E_b(\mathbb{F}_{p^k})$ is divisible by 2, since there exists an obvious rational point $(-b^{1/3}, 0)$ of order 2. Therefore, if p is a BN prime and b has a cubic residue property, $\#E_b(\mathbb{F}_p)$ can be determined as n_0 or n_3 . Similarly, if the coefficient b is quadratic residue in \mathbb{F}_p , $\#E_b(\mathbb{F}_p)$ is divisible by 3 and determined as n_0, n_2 or n_4 .

Lemma 2. (i) The BN parameter χ satisfying $\chi \equiv 11 \pmod{12}$ results in the BN curve as $E_{2^{6l+1}}/\mathbb{F}_p : y^2 = x^3 + 2^{6l+1}$, where $l \in \mathbb{Z}$. (ii) If the parameter satisfies $\chi \equiv 7 \pmod{12}$, the curve $E_{2^{6l-1}}/\mathbb{F}_p : y^2 = x^3 + 2^{6l-1}$ always becomes BN curve.

Proof. (i) If the BN parameter satisfies $\chi \equiv 11 \pmod{12}$, we first note that the group order $\#E_2(\mathbb{F}_p)$ is n_5 from Eq. (4) in Theorem 2. Then, let us consider a map from $E_{2^{6l+1}}$ to E_2 given as follows:

$$E_{2^{6l+1}} : y^2 = x^3 + 2^{6l+1} \rightarrow E_2 : y^2 = x^3 + 2, \quad (x, y) \mapsto (2^{-2l}x, 2^{-3l}y).$$

It is easily found that the map is isomorphic in \mathbb{F}_p since 2^{-2l} and 2^{-3l} are elements in \mathbb{F}_p . Therefore, we got the equation $\#E_{2^{6l+1}}(\mathbb{F}_p) = \#E_2(\mathbb{F}_p) = n_5$.

(ii) If the BN parameter satisfies $\chi \equiv 7 \pmod{12}$, the group order $\#E_2(\mathbb{F}_p)$ is n_1 from Eq. (4). Then, let us consider following twist mapping.

$$E_{2^{6l-1}} : y^2 = x^3 + 2^{6l-1} \rightarrow E_{2^{6l+1}} : y^2 = x^3 + 2^{6l+1}, (x, y) \mapsto (2^{\frac{2}{3}}x, 2y).$$

Since 2 is a cubic non-residue element in \mathbb{F}_p , the isomorphic mapping exists in \mathbb{F}_{p^3} and we can say that $E_{2^{6l-1}}$ is a twisted curve of $E_{2^{6l+1}}$ with the twist degree 3. There exist two types of twist of degree 3. $E_{2^{6l-1}}$ has only two possible group orders given as $p + 1 - (3f_1 - t_1)/2$ or $p + 1 - (-3f_1 - t_1)/2$, where t_1 is the Frobenius trace of $E_{2^{6l+1}}(\mathbb{F}_p)$ and f_1 is computed by $4p = t_1^2 + 3f_1^2$ [13]. We can represent t_1, f_1 as $t_1 = t_1(\chi) = 6\chi^2 + 6\chi + 1, f_1 = f_1(\chi) = 6\chi^2 + 2\chi + 1$ since $\#E_{2^{6l+1}}(\mathbb{F}_p) = n_1$. Thus, the possible group order can be obtained as $n_5 = 36\chi^4 + 36\chi^3 + 18\chi^2 + 6\chi + 1$ and $n_3 = 4(9\chi^4 + 9\chi^3 + 9\chi^2 + 3\chi + 1)$. As discussed in Remark 2, when the group order of elliptic curves can be divisible by 2, coefficients of the curves should have cubic residue property. Here, $\#E_{2^{6l-1}}(\mathbb{F}_p)$ cannot have 2 as a factor since the curve coefficient 2^{6l-1} has cubic non-residue property. Finally we can find $\#E_{2^{6l-1}}(\mathbb{F}_p) = n_5$. According to Remark 1, the curves having the order n_5 become BN curve, $E_{2^{6l-1}}$ and $E_{2^{6l+1}}$ end up as BN curve for the respective conditions of χ . \square

Next, we show the proof of the twisted curve E'/\mathbb{F}_{p^2} can be determined as $y^2 = x^3 + 2^{6l-1}(\alpha + 1), y^2 = x^3 + 2^{6l+1}(\alpha + 1)^{-1}$ for each parameters.

Lemma 3. *When $\mathbb{F}_{p^{12}}$ is constructed by Eq. (2), the correct sextic twist with E' can be obtained uniquely. If the parameter satisfies $\chi \equiv 7 \pmod{12}$, $E'_{2^{6l-1}}/\mathbb{F}_{p^2} : y^2 = x^3 + 2^{6l-1}(\alpha + 1)$ becomes twisted curve. When $\chi \equiv 11 \pmod{12}$, $E'_{2^{6l+1}}/\mathbb{F}_{p^2} : y^2 = x^3 + 2^{6l+1}(\alpha + 1)^{-1}$ becomes twisted curve.*

Proof. There exist two twists of E with the degree 6, E' has only two possible group orders given as $p^2 + 1 - (-3f_2 + t_2)/2$ or $p^2 + 1 - (3f_2 + t_2)/2$ [13], where t_2 is a Frobenius trace of E over \mathbb{F}_{p^2} computed as $t_2 = t^2 - 2p$. f_2 is an integer calculated by $4p^2 = t_2^2 + 3f_2^2$. In the context of BN curve, t_2 and f_2 are given by $t_2 = t_2(\chi) = -36\chi^4 - 72\chi^3 - 36\chi^2 - 12\chi - 1$ and $f_2 = f_2(\chi) = (6\chi^2 + 1)(6\chi^2 + 4\chi + 1)$, respectively. Then, the possible group orders can be denoted as $4(324\chi^8 + 648\chi^7 + 756\chi^6 + 540\chi^5 + 288\chi^4 + 108\chi^3 + 30\chi^2 + 6\chi + 1)$ or $(36\chi^4 + 36\chi^3 + 18\chi^2 + 6\chi + 1)(36\chi^4 + 36\chi^3 + 30\chi^2 + 6\chi + 1)$. Thus, it is found that the twisted curve order becomes $\#E'(\mathbb{F}_{p^2}) = (36\chi^4 + 36\chi^3 + 18\chi^2 + 6\chi + 1)(36\chi^4 + 36\chi^3 + 30\chi^2 + 6\chi + 1)$ since E' has a unique order such that $r = r(\chi) \mid \#E'(\mathbb{F}_{p^2})$. It means that $E'(\mathbb{F}_{p^2})$ cannot be divisible by 2. Therefore, the twisted curve E' coefficients should be a cubic non-residue in \mathbb{F}_{p^2} . Now in the case of the BN curve denoted as $y^2 = x^3 + 2^{6l+1}$, twisted curves can be denoted as $y^2 = x^3 + 2^{6l+1}(\alpha + 1)$ or $y^2 = x^3 + 2^{6l+1}(\alpha + 1)^{-1}$ since $(\alpha + 1)$ and $(\alpha + 1)^{-1}$ are quadratic and cubic non-residue in \mathbb{F}_{p^2} . Then, the cubic residue properties of each curve coefficients can be denoted as follows:

$$\begin{aligned} (2^{6l+1}(\alpha + 1))^{\frac{p^2-1}{3}} &= \left((2^{6l+1}(\alpha + 1))^{p+1} \right)^{\frac{p-1}{3}} = \left((2^{6l+1})^2 \cdot 2 \right)^{\frac{p-1}{3}} = 1, \\ (2^{6l+1}(\alpha + 1)^{-1})^{\frac{p^2-1}{3}} &= \left((2^{6l+1}(\alpha + 1)^{-1})^{p+1} \right)^{\frac{p-1}{3}} = \left((2^{6l+1})^2 \cdot 2^{-1} \right)^{\frac{p-1}{3}} \neq 1. \end{aligned}$$

Since the coefficient of E' needs to be a cubic non-residue in \mathbb{F}_{p^2} , the twisted curve is determined as $y^2 = x^3 + 2^{6l+1}(\alpha + 1)^{-1}$. In the case of $y^2 = x^3 + 2^{6l-1}$, its twisted curves are also derived in the same way. \square

4 Implementation Pairing Using Attractive Classes

This section shows the overview of sparse multiplication techniques and describes the implementation difference between two classes.

4.1 Overview: Sparse Multiplication for Miller's Algorithm

It is well known that the line evaluation can be optimized by applying the 7-sparse multiplication [12]. Mori et al. [14] have shown a more efficient technique called the pseudo 8-sparse multiplication for BN curve in the affine coordinate.

Let $P(x_P, y_P)$ be a rational point in \mathbb{G}_1 and $Q(x_Q, y_Q)$ and $T(x_T, y_T)$ be rational points in \mathbb{G}_2 . Let us consider the sextic twist given as

$$\psi_6 : E'(\mathbb{F}_{p^2}) \rightarrow E(\mathbb{F}_{p^{12}}), (x_{Q'}, y_{Q'}) \mapsto (x_Q z^{-1/3}, y_Q z^{-1/2}),$$

where z is a quadratic and cubic non-residue in \mathbb{F}_{p^2} . Applying this mapping, Q and T can be considered as points $Q'(x_{Q'}, y_{Q'}) = (z^{1/3}x_Q, z^{1/2}y_Q)$ and $T'(x_{T'}, y_{T'}) = (z^{1/3}x_Q, z^{1/2}y_Q)$ on E' . Let the elliptic curve addition be $T' + Q' = R'(x_{R'}, y_{R'})$. Then, the line evaluation and elliptic curve addition (ECA) can be calculated as

$$\begin{aligned} A &= \frac{1}{x_{Q'} - x_{T'}}, B = y_{Q'} - y_{T'}, C = AB, D = x_{T'} + x_{Q'}, x_{R'} = C^2 - D \\ E &= Cx_{T'} - y_{T'}, y_{R'} = E - Cx_{R'}, \\ l_{T', Q'}(P) &= y_P - z^{-1/6}Cx_P + z^{-1/2}E. \end{aligned} \quad (5)$$

Here, all the variables (A, B, C, D, E) are calculated as \mathbb{F}_{p^2} elements. There exist 7 zero coefficients in Eq. (5) which lead to *7-sparse multiplication*.

The line evaluation can be more optimized by multiplying y_P^{-1} in both side of Eq. (5) as $y_P^{-1}l_{T', Q'}(P) = 1 - z^{-1/6}C(x_P y_P^{-1}) + z^{-1/2}E y_P^{-1}$. One of the non-zero coefficient becomes 1 and it realizes more efficient multiplications. However, comparing with Eq. (5), it is found that they need a little more calculation for $x_P y_P^{-1}$ and y_P^{-1} . To minimize the computation overhead of $x_P y_P^{-1}$, let us consider the following isomorphic mapping.

$$\hat{E}(\mathbb{F}_p) : y^2 = x^3 + b\hat{z} \rightarrow E(\mathbb{F}_p) : y^2 = x^3 + b, (x, y) \mapsto (\hat{z}^{-1/3}x, \hat{z}^{-1/2}y),$$

$$\hat{E}'(\mathbb{F}_{p^2}) : y^2 = x^3 + bz\hat{z} \rightarrow E'(\mathbb{F}_{p^2}) : y^2 = x^3 + bz, (x, y) \mapsto (\hat{z}^{-1/3}x, \hat{z}^{-1/2}y),$$

where \hat{z} is a quadratic and cubic residue in \mathbb{F}_p defined as $\hat{z} = (x_P y_P^{-1})^6$. Then, a rational point $\hat{P} \in \hat{E}$ can be represented as $\hat{P}(x_{\hat{P}}, y_{\hat{P}}) = (x_P^3 y_P^{-2}, x_P^3 y_P^{-2})$. In the same way, $\hat{Q}', \hat{T}' \in \hat{E}'$ can be denoted as $\hat{Q}'(x_{\hat{Q}'}, y_{\hat{Q}'}) = (x_P^2 y_P^{-2} x_{Q'}, x_P^3 y_P^{-3} y_{Q'})$,

Algorithm 1. Pseudo 8-Sparse Multiplication for *Class 1*

Input: $a = (a_0 + a_1\beta + a_2\beta^2) + (a_3 + a_4\beta + a_5\beta^2)\gamma$, $b = 1 + b_4\beta\gamma + b_5\beta^2\gamma$
Output: $c = (c_0 + c_1\beta + c_2\beta^2) + (c_3 + c_4\beta + c_5\beta^2)\gamma$
where $a_i, b_j, c_i \in \mathbb{F}_{p^2}$ ($i = 0, \dots, 5, j = 4, 5$)

1	$t_0 \leftarrow a_0b_4, t_1 \leftarrow a_1b_5, t_2 \leftarrow a_0 + a_1, t_3 \leftarrow b_4 + b_5;$	$(2\tilde{m}_2 + 2\tilde{a}_2)$
2	$t_2 \leftarrow t_2t_3 - t_0 - t_1;$	$(\tilde{m}_2 + 2\tilde{a}_2)$
3	$c_5 \leftarrow a_5 + t_2, c_4 \leftarrow a_4 + t_0 + a_2b_5(\alpha + 1);$	$(\tilde{m}_2 + 3\tilde{a}_2 + \tilde{B}_2)$
4	$c_3 \leftarrow a_3 + (a_2b_4 + t_1)(\alpha + 1);$	$(\tilde{m}_2 + 2\tilde{a}_2 + \tilde{B}_2)$
5	$t_0 \leftarrow a_3b_4, t_1 \leftarrow a_4b_5, t_2 \leftarrow a_3 + a_4, t_2 \leftarrow t_2t_3 - t_0 - t_1;$	$(3\tilde{m}_2 + 3\tilde{a}_2)$
6	$c_0 \leftarrow a_0 + t_2(\alpha + 1), c_1 \leftarrow a_1 + (t_1 + a_5b_4)(\alpha + 1);$	$(\tilde{m}_2 + 3\tilde{a}_2 + 2\tilde{B}_2)$
7	$c_2 \leftarrow a_2 + t_0 + a_5b_5(\alpha + 1);$	$(\tilde{m}_2 + 2\tilde{a}_2 + \tilde{B}_2)$

return $c;$

$\hat{T}'(x_{\hat{T}'}, y_{\hat{T}'}) = (x_{\hat{P}}^2 y_{\hat{P}}^{-2} x_{T'}, x_{\hat{P}}^3 y_{\hat{P}}^{-3} y_{T'})$. Applying these rational points for line evaluation, $x_{\hat{P}} y_{\hat{P}}^{-1}$ becomes 1. Therefore, line evaluation can be optimized as

$$\hat{l}_{\hat{T}', \hat{Q}'}(\hat{P}) = y_{\hat{P}}^{-1} l_{\hat{T}', \hat{Q}'}(\hat{P}) = 1 - z^{-1/6} C + z^{-1/2} E y_{\hat{P}}^{-1}. \quad (6)$$

The remaining 7 zero and 1 one coefficients in Eq. (6) lead to an efficient multiplication called *pseudo 8-sparse multiplication*.

4.2 Line Evaluation for the Proposed Attractive Classes

Here, this paper describes the line evaluation for two classes of BN curves. In what follows, the cost of the multiplication, constant multiplication, squaring, addition/subtraction and inversion over \mathbb{F}_{p^k} are represented as $\tilde{m}_k, \tilde{n}_{u_k}, \tilde{s}_k, \tilde{a}_k$ and \tilde{i}_k , respectively. The costs of multiplication by $(\alpha + 1)$ and $(\alpha + 1)^{-1}$ are especially denoted as \tilde{B}_2 and \tilde{B}_2^{-1} .

Using Class 1: It is found that the sextic twist parameter z is $(\alpha + 1)$ since the twisted curve of *Class 1* is $E' : y^2 = x^3 + 2^{6l-1}(\alpha + 1)$ from Table 1. Therefore, the sextic twist mapping for *Class 1* is given as follows:

$$\begin{aligned} E'(\mathbb{F}_{p^2}) : y^2 = x^3 + 2^{6l-1}(\alpha + 1) &\rightarrow E(\mathbb{F}_{p^{12}}) : y^2 = x^3 + 2^{6l-1}, \\ (x, y) &\mapsto ((\alpha + 1)^{-1/3}x, (\alpha + 1)^{-1/2}y) = ((\alpha + 1)^{-1}x\beta^2, (\alpha + 1)^{-1}y\beta\gamma). \end{aligned}$$

Then, the line evaluation of the pseudo 8-sparse form can be obtained for the rational point $\hat{P} \in \hat{E}'(\mathbb{F}_p)$ and $\hat{Q}', \hat{T}' \in \hat{E}'(\mathbb{F}_{p^2})$ as follows:

$$\hat{l}_{\hat{T}', \hat{Q}'}(P) = 1 - (\alpha + 1)^{-1} C \beta^2 \gamma + (\alpha + 1)^{-1} E y_{\hat{P}}^{-1} \beta \gamma. \quad (7)$$

Finally, the pseudo 8-sparse multiplication is calculated by Algorithm 1.

Using *Class 2*: The twist parameter z for E' from Table 1 is $(\alpha+1)^{-1}$. Therefore, the sextic twist mapping for *Class 2* is given as follows:

$$\begin{aligned} E'(\mathbb{F}_{p^2}) : y^2 = x^3 + 2^{6l+1}(\alpha+1)^{-1} &\rightarrow E(\mathbb{F}_{p^{12}}) : y^2 = x^3 + 2^{6l+1}, \\ (x, y) &\mapsto ((\alpha+1)^{1/3}x, (\alpha+1)^{1/2}y) = (x\beta, y\beta\gamma). \end{aligned}$$

Then, the line evaluation of the pseudo 8-sparse form can be obtained in affine coordinate for the rational point $\hat{P} \in \hat{E}'(\mathbb{F}_p)$ and $\hat{Q}', \hat{T}' \in \hat{E}'(\mathbb{F}_{p^2})$ as follows:

$$\hat{l}_{\hat{T}', \hat{Q}'}(\hat{P}) = 1 - C\gamma + Ey_{\hat{P}}^{-1}\beta\gamma. \quad (8)$$

Therefore, Algorithm 2 shows the derived pseudo 8-sparse multiplication.

Algorithm 2. Pseudo 8-Sparse Multiplication for *Class 2*

Input: $a = (a_0 + a_1\beta + a_2\beta^2) + (a_3 + a_4\beta + a_5\beta^2)\gamma$, $b = 1 + b_3\gamma + b_4\beta\gamma$

Output: $c = (c_0 + c_1\beta + c_2\beta^2) + (c_3 + c_4\beta + c_5\beta^2)\gamma$

where $a_i, b_j, c_i \in \mathbb{F}_{p^2}$ ($i = 0, \dots, 5, j = 4, 5$)

- 1 $t_0 \leftarrow a_0b_3, t_1 \leftarrow a_1b_4, t_2 \leftarrow a_0 + a_1, t_3 \leftarrow b_3 + b_4;$ $(2\tilde{m}_2 + 2\tilde{a}_2)$
- 2 $t_2 \leftarrow t_2t_3 - t_0 - t_1;$ $(\tilde{m}_2 + 2\tilde{a}_2)$
- 3 $c_4 \leftarrow a_4 + t_2, c_3 \leftarrow a_3 + t_0 + a_2b_4(\alpha + 1);$ $(\tilde{m}_2 + 3\tilde{a}_2 + \tilde{B}_2)$
- 4 $c_5 \leftarrow a_5 + t_1 + a_2b_3;$ $(\tilde{m}_2 + 2\tilde{a}_2)$
- 5 $t_0 \leftarrow a_3b_3, t_1 \leftarrow a_4b_4, t_2 \leftarrow a_3 + a_4, t_2 \leftarrow t_2t_3 - t_0 - t_1;$ $(3\tilde{m}_2 + 3\tilde{a}_2)$
- 6 $c_2 \leftarrow a_2 + t_2, c_1 \leftarrow a_1 + t_0 + a_5b_4(\alpha + 1);$ $(\tilde{m}_2 + 3\tilde{a}_2 + \tilde{B}_2)$
- 7 $c_0 \leftarrow a_0 + (t_1 + a_5b_3)(\alpha + 1);$ $(\tilde{m}_2 + 2\tilde{a}_2 + \tilde{B}_2)$

return c ;

Comparing Class 1 and Class 2: Table 2 shows the calculation costs of the sextic twist, computation of line evaluation/ECA, and pseudo 8-sparse multiplication for *Class 1* and *Class 2*. It is easily found that *Class 1* requires more \tilde{B}_2 and \tilde{B}_2^{-1} computation, making it costlier than *Class 2*. This cost incurs due to the twist coefficient z . The details of the costs are given by $\tilde{B}_2 = 2\tilde{a}_1$ and $\tilde{B}_2^{-1} = 2\tilde{m}_{u_1} +$

Table 2. Calculation cost of the sextic twist, line evaluation and ECA and pseudo 8-sparse multiplication for proposed classes

Type	Sextic twist	Line evaluation and ECA		Pseudo 8-sparse multiplication
		$\hat{T} \neq \hat{Q}$	$\hat{T} = \hat{Q}$	
<i>Class 1</i>	$2\tilde{B}_2^{-1}$	$3\tilde{m}_2 + \tilde{m}_{u_2} + \tilde{s}_2 + 6\tilde{a}_2 + \tilde{i}_2 + 2\tilde{B}_2^{-1}$	$3\tilde{m}_2 + \tilde{m}_{u_2} + 2\tilde{s}_2 + 7\tilde{a}_2 + \tilde{i}_2 + 2\tilde{B}_2^{-1}$	$10\tilde{m}_2 + 17\tilde{a}_2 + 5\tilde{B}_2$
<i>Class 2</i>	0	$3\tilde{m}_2 + \tilde{m}_{u_2} + \tilde{s}_2 + 6\tilde{a}_2 + \tilde{i}_2$	$3\tilde{m}_2 + \tilde{m}_{u_2} + 2\tilde{s}_2 + 7\tilde{a}_2 + \tilde{i}_2$	$10\tilde{m}_2 + 17\tilde{a}_2 + 3\tilde{B}_2$

$2\tilde{a}_1$. Although the costs are seemingly insignificant than other \mathbb{F}_p operations, however, they appear repeatedly in line evaluation, ECA calculation and sparse multiplication in the Miller’s algorithm for more than 114 times. Therefore, the authors suggest that using *Class 2* is a better choice for efficient pairing implementation.

5 Experimental Result

This section gives details of the experimental implementation. The source code can be found in Github¹. The big integer arithmetic is implemented using the `mpz_t` data type of GMP [11] library. In what follows, multiplication, squaring, addition/subtraction/negation and inversion in \mathbb{F}_p are denoted as M , S , A and I , respectively. This paper assumes that $M = 5A$, $S = 4.5A$ and $I = 30A$ for performance comparison (based on the average time of 1 million \mathbb{F}_p operations). The pairings are implemented by using pseudo 8-sparse multiplication for the Miller’s algorithm (see Sect. 4) and Fuentes-Castaneda et al.’s [10] final exponentiation algorithm. Table 3 shows the computational environment. The parameters of the proposed classes of the BN curve at the 128-bit security level are given in Table 4. Table 5 shows the operation count based on the counter in the implementation code. The result also shows the average execution time of 100 pairings.

Table 5 shows that Miller’s algorithm using *Class 2* is more than 3.9% efficient than *Class 1*. It is also found that the performance of *Class 2* for the parameter of the Hamming weight 6 is close to the *Class 1* with the Hamming weight 4. According to Table 5, the efficiency precedence can be expressed as $(ii) > (i) \approx (iv) > (iii)$. Therefore, the authors conclude that *Class 2* is a better choice for efficient pairing implementation. The total cost in execution time is subject to the environment. However, the time cost is coherent with the operation count.

Table 3. Computational Environment

CPU	Memory	Compiler	OS	Language	Library
Intel(R) Core(TM) i7-7567U CPU @ 3.50 GHz	8 GB	GCC 4.2.1	macOS High Sierra 10.13.6	C	GMP ver 6.1.2 [11]

Table 4. Proposed classes of the parameter at the 128-bit security level (four types)

Type	χ	HW	BN curve	Twisted curve
(i) <i>Class 1</i> ^a	$2^{114} + 2^{101} - 2^{14} - 1$	4	$y^2 = x^3 + 32$	$y^2 = x^3 + 32(\alpha + 1)$
(ii) <i>Class 2</i>	$2^{114} + 2^{84} - 2^{53} - 1$	4	$y^2 = x^3 + 2$	$y^2 = x^3 + 2(\alpha + 1)^{-1}$
(iii) <i>Class 1</i>	$2^{114} + 2^{78} + 2^{51} - 2^{38} - 2^{36} - 1$	6	$y^2 = x^3 + 32$	$y^2 = x^3 + 32(\alpha + 1)$
(iv) <i>Class 2</i>	$2^{114} + 2^{94} + 2^{55} - 2^{53} - 2^3 - 1$	6	$y^2 = x^3 + 2$	$y^2 = x^3 + 2(\alpha + 1)^{-1}$

^a Proposed by Barbulescu et al. [3].

¹ http://github.com/YukiNanjo/BN12_attractive.

Table 5. Operation count and execution time using proposed classes

Type	Pairing operations		Time [ms]	Operation count			
				M	S	A	I
<i>(i) Class 1</i>	Miller's	Opt-ate	5.17	1696	9062	35770	125
	Alg.	χ -ate	4.88	1658	8893	35241	120
	Final Exp.		4.79	1428	8131	43102	1
<i>(ii) Class 2</i>	Miller's	Opt-ate	4.88	1201	9061	34774	125
	Alg.	χ -ate	4.75	1183	8892	34285	120
	Final Exp.		4.71	1428	8131	43102	1
<i>(iii) Class 1</i>	Miller's	Opt-ate	5.24	1728	9234	36298	129
	Alg.	χ -ate	5.03	1674	8979	35505	122
	Final Exp.		4.94	1428	8455	44446	1
<i>(iv) Class 2</i>	Miller's	Opt-ate	5.04	1217	9233	35270	129
	Alg.	χ -ate	4.82	1191	8978	34533	122
	Final Exp.		4.86	1428	8455	44446	1

6 Conclusion

This paper has proposed two attractive classes of BN curves for the efficient pairing implementation which result in not only constructing an efficient tower of the extension field but also instantaneously determining BN curve, its twisted curves and obvious generator points. Moreover, this paper clearly describes that the implementation difference of the Miller's algorithm between two classes applying pseudo 8-sparse multiplication. The authors conclude that Class 2 curve ($\chi \equiv 11 \pmod{12}$) is a better choice for efficient pairing. As a future work, the authors would like to examine the similar technique for other pairing-friendly curves.

Acknowledgement. This work was supported by the Strategic Information and Communications R&D Promotion Programme (SCOPE) of Ministry of Internal Affairs and Communications, Japan.

References

1. Aranha, D.F., Karabina, K., Longa, P., Gebotys, C.H., López, J.: Faster explicit formulas for computing pairings over ordinary curves. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 48–68. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-20465-4_5
2. Bailey, D.V., Paar, C.: Efficient arithmetic in finite field extensions with application in elliptic curve cryptography. *J. Cryptol.* **14**(3), 153–176 (2001)
3. Barbulescu, R., Duquesne, S.: Updating key size estimations for pairings. *J. Cryptol.* **2018**, 1–39 (2018). <https://doi.org/10.1007/s00145-018-9280-5>

4. 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). https://doi.org/10.1007/11693383_22
5. Boneh, D., Boyen, X.: Short signatures without random oracles. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 56–73. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-24676-3_4
6. Boneh, D., Lynn, B., Shacham, H.: Short signatures from the Weil pairing. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 514–532. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-45682-1_30
7. Cohen, H., et al.: Handbook of Elliptic and Hyperelliptic Curve Cryptography. CRC Press, Boca Raton (2005)
8. Costello, C., Lauter, K., Naehrig, M.: Attractive subfamilies of BLS curves for implementing high-security pairings. In: Bernstein, D.J., Chatterjee, S. (eds.) INDOCRYPT 2011. LNCS, vol. 7107, pp. 320–342. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-25578-6_23
9. Freeman, D., Scott, M., Teske, E.: A taxonomy of pairing-friendly elliptic curves. *J. Cryptol.* **23**(2), 224–280 (2010)
10. Fuentes-Castañeda, L., Knapp, E., Rodríguez-Henríquez, F.: Faster hashing to \mathbb{G}_2 . In: Miri, A., Vaudenay, S. (eds.) SAC 2011. LNCS, vol. 7118, pp. 412–430. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-28496-0_25
11. Granlund, T.: The GMP development team: GNU MP: the GNU multiple precision arithmetic library, 6.1. 0 edn. (2015)
12. Grewal, G., Azarderakhsh, R., Longa, P., Hu, S., Jao, D.: Efficient implementation of bilinear pairings on ARM processors. In: Knudsen, L.R., Wu, H. (eds.) SAC 2012. LNCS, vol. 7707, pp. 149–165. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-35999-6_11
13. Hess, F., Smart, N.P., Vercauteren, F.: The Eta pairing revisited. *IEEE Trans. Inf. Theory* **52**(10), 4595–4602 (2006)
14. Mori, Y., Akagi, S., Nogami, Y., Shirase, M.: Pseudo 8-sparse multiplication for efficient ate-based pairing on Barreto-Naehrig curve. In: Cao, Z., Zhang, F. (eds.) Pairing 2013. LNCS, vol. 8365, pp. 186–198. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-04873-4_11
15. Nogami, Y., Akane, M., Sakemi, Y., Katou, H., Morikawa, Y.: Integer variable chi-based ate pairing. *Pairing* **5209**, 178–191 (2008)
16. Shirase, M.: Barreto-Naehrig curve with fixed coefficient - efficiently constructing pairing-friendly curves (2010)
17. Vercauteren, F.: Optimal pairings. *IEEE Trans. Inf. Theory* **56**(1), 455–461 (2010)