International Journal of Networking and Computing – www.ijnc.org, ISSN 2185-2847
Volume 11, Number 2, pages 383–411, July 2021

Restrictions of Integer Parameters for Generating Attractive BLS Subfamilies of Pairing-Friendly Elliptic Curves with Specific Embedding Degrees

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

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

Received: February 12, 2021
Revised: April 28, 2021
Accepted: June 2, 2021
Communicated by Toru Nakanishi

Abstract

Pairings are widely used for innovative protocols such as ID-based encryption and group signature authentication. According to the recent works, the Barreto-Lynn-Scott (BLS) family of pairing-friendly elliptic curves is suggested for the pairings at the various security levels. One of the important facts is that the BLS family has fixed polynomial parameters of a field characteristic and group order in terms of an integer x_0. For practical pairing-based protocols, we have to carefully find x_0 which leads to efficient pairings, however, this search of x_0 is typically complicated. Thus, it is desired some convenient ways of finding x_0 which have advantageous for the pairings. For this reason, Costello et al. proposed simple restrictions for finding x_0 that generates the specific BLS subfamilies of curves with embedding degree $k = 24$ having one of the best field and curve constructions for the pairings. Since there are demands of such restrictions for the other cases of the embedding degrees, the authors extend their work and provide these for the cases of $k = 2^m \cdot 3$ and 3^n with arbitrary integers $m, n > 0$ in this paper. The results will help to find new parameters which lead to one of the best performing pairings with the BLS family of curves with various k. The results also allow us to respond to change in the security levels of the pairings flexibly according to the progress in the security analyses in the future.

Keywords: Pairing-based cryptography, BLS curves, tower of extension fields.

1 Introduction

Background and motivation. Pairings on elliptic curves enable innovative protocols, e.g., ID-based encryption [9], group signature authentication [7], searchable encryption [8], attribute-based encryption [15], and homomorphic encryption [32]. Since these pairing-based protocols can be indirectly improved through the improvement of the pairings, researchers have been working on methods to construct several families of pairing-friendly elliptic curves [3, 4, 13, 22], optimizations of the pairing algorithm [10, 14, 20, 21, 28, 34, 38], security analyses [1, 2, 12, 17, 18], and so on. As one of recent works of the pairings, in [1], Barbulescu and Duquesne analyzed the key size of the pairings that have resistance against an attack for a discrete logarithm problem given by Kim et al. in [24]. Starting with this, researchers have been worked on the security analyses and gave recommendations of the elliptic curves in [2, 12, 17, 18]. According to these results, one of the parametric families of pairing-friendly elliptic curves given by Barreto, Lynn, and Scott in [3], which is so-called the *BLS family*, is often used for the pairings at the various security levels. The BLS family has high flexibility of the

choices of embedding degrees. Moreover, that can strongly supports optimizing the pairings, e.g., one can immediately find the shortest Miller loop [20, 38] and efficient algorithm for computing the final exponentiation without effort [19, 35]. Therefore, the BLS family will be regularly adopted for the pairings even if there is progress in the security analyses in the future.

In the context, the BLS family has specific rational polynomial parameters $p(x)$, $r(x)$, and $t(x)$ with some indeterminate x for generating pairing-friendly elliptic curves with embedding degree k of multiple of 3 except for $k = 18$. For an integer x_0 making $p(x_0)$ and $r(x_0)$ being primes and $t(x_0)$ being an integer, one can find an elliptic curve E defined over a prime field of order $p(x_0)$ with embedding degree k of which the group order $n(x_0)$ is given as $n(x_0) = p(x_0) + 1 - t(x_0)$ including a prime divisor $r(x_0)$. Such curve E is called the BLS curve. One can also find a twist E' of degree d of E defined over a field of order $p(x_0)^{k/d}$ of which the group order $n'(x_0)$ is divisible by $r(x_0)$. These two curves E and E' are often used for the pairings. As seen above, since x_0 strongly specifies the field and curve constructions of the BLS family, we have to carefully choose x_0 for realizing efficient pairings. However, since it is typically complicated for finding x_0 which has advantageous for the pairings, it is desired to establish some convenient ways of finding such x_0.

For the above reasons, in [11], Costello et al. proposed simple restrictions for finding x_0 given by the congruence classes $x_0 \equiv 7, 16, 31, 64 \pmod{72}$ which specifies the BLS family of pairing-friendly elliptic curves with $k = 24$. Once finding x_0 under their restrictions, there appear the specific subfamilies of the BLS family having the following nice options.

(i) A fixed tower of extension fields with fast arithmetics is available.
(ii) The BLS curve E is determined.
(iii) The twist E' is determined.

With the field option (i), it is found that the BLS subfamilies can result in fast pairings in terms of the efficiency of field arithmetics. Besides, with the field and curve options (i), (ii), and (iii), the BLS subfamilies contribute to reducing the pre-computation of the initial setting of the pairings and can also provide reusability of implementations. Thus, it is worth using these BLS subfamilies by restricting x_0 even though that narrows down the choices of the curves.

In fact, in [11], Costello et al. derived the restrictions for generating the BLS subfamilies having the field option (i) and added the curve options (ii) and (iii) to these subfamilies. In more detail, they derived the necessary and sufficient conditions for constructing their favorite tower of extension fields. Then, under the restrictions, they determined the curve equations of E and E' by checking the small cofactors of the group orders $n(x_0)$ and $n'(x_0)$, respectively. Although they only focused on the case of $k = 24$, there are demands of similar results for the other cases of embedding degrees. Fortunately, since there is a possibility that their techniques can be straightforwardly extended for different embedding degrees, the authors try to clarify these in this paper.

Our results and contribution. The authors extend [11] and provide restrictions for finding x_0 that can generate the specific BLS subfamilies of pairing-friendly elliptic curves with more generalized embedding degrees $k = 2^m \cdot 3$ and 3^n for any integer $m, n > 0$ as shown in the below.

- For $k = 2^m \cdot 3$, the authors propose to restrict x_0 by the congruence classes $x_0 \equiv 7, 10, 16, 28, 31, 34 \pmod{36}$ for $m = 1$; $x_0 \equiv 7, 16, 31, 64 \pmod{72}$ for $m > 1$. Once finding x_0 under the restrictions, the BLS subfamilies of curves with $k = 2^m \cdot 3$ having the options (i), (ii), and (iii) are generated (see Theorems 6, 7 and 8).
- For $k = 3^n$, the authors propose to restrict x_0 by $x_0 \equiv 4 \pmod 6$. Once finding x_0 under the restriction, the BLS subfamily of curves with $k = 3^n$ having the options (i) and (ii) is generated (see Theorems 9 and 10). Although the authors can not give the twist option (iii) to the subfamily just by extending [11], the authors give a conjecture (see Conjecture 1).

In the process of obtaining the results, the authors present the group order $n'(x_0)$ of the twist E' for the cases of $k = 2^m \cdot 3$ and 3^n (see Theorems 4 and 5).

The results can contribute to an easy search of the parameters x_0 which lead to one of the efficient pairings with the BLS family of curves with $k = 2^m \cdot 3$ and 3^n in terms of the field arithmetics. Indeed, the authors find several sample parameters x_0 for the pairings with the BLS family of curves

with $k = 9, 12, 24$, and 27 at the 128 and 192-bit security levels (see Tables 3 and 4). The pairings on the curves with sample parameters are enough efficient as shown in evaluation by an implementation using C language (see Tables 5 and 6). Although [11] also provided many parameters for $k = 24$, the authors confirm that the parameters found by this work result in more efficient pairings at the current 192-bit security level than that of the previous ones. In addition to this, since all x_0 in the certain restriction have the common field and curve constructions, the results can also support to change of x_0 smoothly. For example, if there exists an implementation of the pairing with a certain x_0 satisfying the restriction, we can update x_0 without changing the implementation of the field and curve arithmetics as long as x_0 is chosen from the same restriction. Thus, if there is progress in the security analyses, the results also allow us to flexibly respond to the update of x_0 without changing implementations as far as possible. Moreover, since the results are available for the curves with generalized embedding degrees k, these will be useful for the researcher and implementer of the pairings for a long time.

The Differences from the previous version. Note that this paper is an extended version of the authors' previous work [30] submitted in CANDAR'20 workshop. The previous version proposed the same restrictions for the BLS family of curves with $k = 2^m \cdot 3$ and 3^n and also described that the generated BLS subfamilies have the options (i) and (ii). However, the previous version could not give the twist option (iii) at all. This is because that there was a lack of knowledge of the group order $n'(x_0)$ of the twist E' for the generalized embedding degrees, and thus the curve determination techniques given by [11] could not be applied. Contrary, this paper drive $n'(x_0)$ for both the cases of $k = 2^m \cdot 3$ and 3^n and determine the curve equation of E' for the case of $k = 2^m \cdot 3$. As the other differences, this paper provides the sample parameters x_0 with the implementation results.

Organization. The rest of this paper is organized below. Sect. 2 provides a brief background on pairings. In Sect. 3, the authors describe the review of the BLS family and the previous work [11]. Sect. 4 gives the mathematical preliminaries for driving the restrictions for constructing the tower of extension fields and determining the curve equations. Before describing the proposal, the authors derive the group order of the twist E' in Sect. 5. Then, in Sect. 6, the authors describe the proposed restrictions for generating BLS subfamilies with mathematical grounds. Applying the proposal, Sect. 7 provides the sample parameters. Sect. 8 evaluates the pairings on the curves with the parameters given in Sect. 7 by the implementation. Finally, Sect. 9 draws the conclusion.

2 Background on Pairings

In the following subsections, the authors present brief explanations of the elliptic curves and pairings.

2.1 Elliptic Curves

Let p be a prime and q be p or power of p. Let $\mathbb{F}_q$ be a finite field of order q. Let $\mathbb{F}_q^*$ be a multiplicative group of $\mathbb{F}_q$ and let $\overline{\mathbb{F}}_q$ be an algebraic closure of $\mathbb{F}_q$. For a prime $p > 3$ and non-negative integer i, consider the cases where $q = p^i$, an elliptic curve E of Weierstrass form defined over $\mathbb{F}_q$ is given as follows:

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

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

Let $n = \#E(\mathbb{F}_q)$ which is the number of rational points. Let t be an integer defined as $t = q+1-n$ which is called the *Frobenius trace of* E. If E is ordinary, there is a square-free integer D such that

$DV^2 = 4q - t^2$ with an integer V. If $q = p$, D is known as the CM discriminant. The value of D is related to $j(E)$, e.g., if $D = 3$, then $j(E) = 0$. Let r be a prime factor of n. Then, there exists an entire group of order r defined as $E(\overline{\mathbb{F}}_q)[r] = \{P \mid P \in E(\overline{\mathbb{F}}_q), [r]P = \mathcal{O}\}$ which is called a *r-torsion subgroup*. The smallest integer $k \geq 1$ satisfying $r \mid (q^k - 1)$ is called an embedding degree with respect to r. The r-torsion subgroup defined over $\mathbb{F}_{q^k}$ has a structure such that $E(\mathbb{F}_{q^k})[r] \cong \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$, i.e., $\#E(\mathbb{F}_{q^k})[r] = r^2$. This implies that $E(\mathbb{F}_{q^k})[r]$ has $(r + 1)$ different subgroups of order r since the identity $\mathcal{O}$ overlaps into all subgroups of order r.

There exists an elliptic curve $E'/\mathbb{F}_{q^{k/d}}$ with an isomorphism $\phi_d : E'(\mathbb{F}_{q^k}) \to E(\mathbb{F}_{q^k})$ where d is the smallest integer such that $d \mid k$ in which ϕ_d can be defined. Then, E' is called a twist of degree d of E. Although that is not immediate derivation from the definition, there are only possible degrees $d \in \{1, 2, 3, 4, 6\}$[1] corresponding to $j(E)$, e.g., if $j(E) = 0$, then $d \in \{1, 2, 3, 6\}$. The important fact is that there is a unique twist $E'/\mathbb{F}_{q^{k/d}}$ such that r divides $n' = \#E'(\mathbb{F}_{q^{k/d}})$. The authors call such a twist E' as a *correct twist*. With the correct twist, ϕ_d involves a group isomorphism $G' \to G$ where $G' = E'(\mathbb{F}_{q^k})[r]$ and $G \subset E(\mathbb{F}_{q^k})[r]$, which can be written as $G = E(\mathbb{F}_{q^k})[r] \cap \ker(\pi_q - [q]) \subset E(\mathbb{F}_{q^k})$ with the q-th power Frobenius endomorphism π_q and is often exploited for pairings.

As seen above, the properties of the elliptic curves are typically specified by the integers (k, D, q, r, t), which is often discussed as the set (q, r, t). Rather than that, q is typically fixed as $q = p$ for the pairings. According to [13], the elliptic curves having small k, large r, and appropriate ρ-value $\rho = \log_2 p / \log_2 r$ such that $1 \leq \rho \leq 2$ are called *pairing-friendly*. Although it is typically not easy to constructing pairing-friendly elliptic curves, there are several construction methods that are based on an idea of the parameterization of (p, r, t) by the polynomials $(p(x), r(x), t(x))$ in $\mathbb{Q}[x]$ making the curves with the favorite properties [3,4,13,22]. In this paper, the set of pairing-friendly elliptic curves specified by $(p(x), r(x), t(x))$ are called as a *parametric family of pairing-friendly elliptic curves*.

2.2 Pairings

Let $E/\mathbb{F}_p$ be a pairing-friendly elliptic curve with a prime divisor r of $\#E(\mathbb{F}_p)$ and embedding degree k with respect to r, i.e., $r \mid (p^k - 1)$. Let G_1 and G_2 be subgroups of $E(\mathbb{F}_{p^k})[r]$ of order r. For points $P \in G_1$ and $Q \in G_2$, a Tate pairing τ_r, which is non-degenerate and bilinear, is defined as follows:

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

where $f_{r,P}$ is a rational function with a divisor $\mathrm{div}(f_{r,P}) = r(P) - r(\mathcal{O})$. The value of the rational function can be computed by Miller's algorithm [28] which can reach $f_{r,P}(Q)$ with $\log_2 r$ iterations. Miller's algorithm is often extended for a double-and-add/sub algorithm as described in [6,37]. The standard Tate pairing has an undesirable property that the output lies in an equivalence class, rather than being a unique element. To be suitable in practice, $(p^k - 1)/r$ is raised to the output of the Tate pairing as follows:

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

where μ_r is a group of r-th roots of the identity of $\mathbb{F}_{p^k}^*$. The above pairing is called a *reduced Tate pairing* and the additional exponentiation is called the *final exponentiation*. Especially for the parametric families of pairing-friendly elliptic curves, the final exponentiation can be efficiently computed by using p-th power of Frobenius endomorphisms since the exponent can be represented as a polynomial in base p [14, 34].

Let G_1 and G_2 be the subgroups defined as $G_1 = E(\mathbb{F}_{p^k})[r] \cap \ker(\pi_p - [1]) = E(\mathbb{F}_p)[r]$ and $G_2 = E(\mathbb{F}_{p^k})[r] \cap \ker(\pi_p - [p]) \subset E(\mathbb{F}_{p^k})$, respectively. The groups are the eigenspaces of π_p on $E(\mathbb{F}_{p^k})[r]$, i.e., $G_1 \oplus G_2 = E(\mathbb{F}_{p^k})[r]$. Restricting the reduced Tate pairing to swap the arguments as $G_2 \times G_1$ with the above subgroups leads to an *ate pairing* α_T defined as follows [21]:

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

where $T = t - 1$ and $f_{T,Q}$ is a rational function with a divisor $\mathrm{div}(f_{T,Q}) = T(Q) - ([T]Q) - (T - 1)(\mathcal{O})$. Since the iterative parameter T is much smaller than r, ate pairings are more practical than the

[1] If $d = 1$, E' is typically not called the twist of E. However, in this paper, E' with $d = 1$ is also called the twist.

reduced Tate pairings. According to [20, 38], ate-like pairings which require at least $\log_2 r/\phi(k)$ iterations can be constructed corresponding to the curves where ϕ is Euler's totient function. Such pairings are known as *optimal ate pairings*.

Let $E'/\mathbb{F}_{p^{k/d}}$ be the correct twist of degree d of E. With a twist isomorphism ϕ_d, let $G_1' = \phi_d^{-1}(G_1) \subset E'(\mathbb{F}_{p^k})[r]$ and $G_2' = \phi_d^{-1}(G_2) = E'(\mathbb{F}_{p^{k/d}})[r]$ be preimages of G_1 and G_2 under ϕ_d, respectively. Note that G_2 is a special subgroup of which the preimage is defined over $\mathbb{F}_{p^{k/d}}$. Then, the ate pairing can also be moved entirely on E' as follows:

$$\alpha_T' : G_2' \times G_1' \to \mu_r, (Q', P') \mapsto f_{T,Q'}'(P')^{(p^k-1)/r}, \tag{5}$$

where $f_{T,Q'}'$ is a rational function with a divisor $\mathrm{div}(f_{T,Q'}') = T(Q') - ([T]Q') - (T-1)(\mathcal{O}')$ with the point at infinity $\mathcal{O}'$ on E'. Although the ate pairings α_T and α_T' are typically not distinguished, the outputs of α_T and α_T' does not necessarily take the same value even though the inputs satisfy $P' = \phi_d^{-1}(P)$ and $Q' = \phi_d^{-1}(Q)$, rather than, there is a relation $\alpha_T(Q,P)^{\gcd(d,6)} = \alpha_T'(Q',P')^{\gcd(d,6)}$ (see Theorem 1 in [10]). Since the fields in which the groups G_1 and G_2' are smaller than these of G_1' and G_2', respectively, the ate pairings are often regarded as $G_2' \times G_1$. To make the movement of the curves easily and enable an efficient arithmetics, a tower of extension fields constructed by quotient rings by binomial ideals are often adopted for the pairings [5].

3 Review of the BLS family and Previous Work

In this section, the authors introduce the BLS family of pairing-friendly elliptic curves which are often used for the pairings.

3.1 Construction of the BLS family

The BLS family [3] has the polynomial parameters for constructing pairing-friendly elliptic curves with the CM discriminant $D = 3$, i.e., zero j-invariant, and the embedding degree k of multiple of 3 except for $k = 18$. For the cases of $k = 2^m \cdot 3$ and 3^n with arbitrary positive integers m and n, there are the following polynomial parameters $(p(x), r(x), t(x))$ with $V(x)$ such that $3V(x)^2 = 4p(x) - t(x)^2$.

- $k = 2^m \cdot 3$

$$\begin{cases} r(x) &= \Phi_k(x) = x^{2^m} - x^{2^{m-1}} + 1, \\ p(x) &= (x-1)^2/3 \cdot r(x) + x, \\ t(x) &= x + 1, \\ V(x) &= (x-1)/3 \cdot (2x^{2^{m-1}} - 1), \end{cases} \tag{6}$$

- $k = 3^n$

$$\begin{cases} r(x) &= \Phi_k(x)/3 = (x^{2\cdot 3^{n-1}} + x^{3^{n-1}} + 1)/3, \\ p(x) &= (x-1)^2 \cdot r(x) + x, \\ t(x) &= x + 1, \\ V(x) &= (x-1)/3 \cdot (2x^{3^{n-1}} + 1), \end{cases} \tag{7}$$

where $\Phi_k(x)$ is the k-th cyclotomic polynomial.

Let x_0 be an integer making $p(x_0)$ and $r(x_0)$ being primes and $t(x_0)$ and $V(x_0)$ being integers. Note that the condition $x_0 \equiv 1 \pmod 3$ leads to all involved parameters being integers. Then, there is an elliptic curve $E/\mathbb{F}_{p(x_0)} : y^2 = x^3 + b$ such that the group order is given by $n(x_0) = \#E(\mathbb{F}_{p(x_0)}) = p(x_0) + 1 - t(x_0)$ with the prime divisor $r(x_0)$. The curve also has the embedding degree k with respect to $r(x_0)$, i.e., k is the minimal integer satisfying $r(x_0) \mid (p(x_0)^k - 1)$. Such curve is called a *BLS curve*. Let $d = 6$ and 3 for $k = 2^m \cdot 3$ and 3^n, respectively. Then, there exist a correct twist $E'/\mathbb{F}_{p(x_0)^{k/d}} : y^2 = x^3 + b'$ of degree d of E such that $r(x_0) \mid n'(x_0) = \#E'(\mathbb{F}_{p(x_0)^{k/d}})$, however, $n'(x_0)$ have not been explicitly provided except for the cases with some concrete embedding degrees.

Let $G_1 = E(\mathbb{F}_{p(x_0)})[r(x_0)]$ and $G_2' = E'(\mathbb{F}_{p(x_0)^{k/d}})[r(x_0)]$ be subgroups of order $r(x_0)$ on E and E', respectively. Then, the ate pairing $G_2' \times G_1$ can be computed by Miller's algorithm with one of the shortest iterations $T = t(x_0) + 1 = x_0$ since $\log_2 r(x_0)/\phi(k) \approx \log_2 x_0$. This means that the ate pairing is exactly one of the optimal ate pairings. Moreover, according to [19,35], the exponent $(p(x_0)^k - 1)/r(x_0)$ of the final exponentiation automatically decomposed into the polynomials in base $p(x_0)$ by using a property that $p(x_0)$ is represented as $p(x_0) = h(x_0) \cdot r(x_0) + x_0$ where $h(x_0)$ is a certain polynomial. This immediately provides one of the efficient algorithms for computing the final exponentiation.

3.2 Previous work by Costello et al.

From the constructions of the BLS family, it is found that the integer parameter x_0 strongly characterizes the BLS family. Thus, the choice of x_0 is one of the important factors to realize the efficient pairings with the BLS family. In [11], Costello et al. observed that and proposed the restrictions of x_0 for generating specific subfamilies of the BLS family of curves with $k = 24$ which facilitate efficient instantiations of the pairings as follows:

$$x_0 \equiv 7, 16, 31, 64 \pmod{72}. \tag{8}$$

Once finding x_0 under the above restriction, we have the specific subfamilies of the BLS family with the options (i) the fixed tower of extension fields with one of the best performing arithmetics is always available, (ii) the BLS curve $E/\mathbb{F}_{p(x_0)}$ is immediately determined, and (iii) the correct twist $E'/\mathbb{F}_{p(x_0)^4}$ of degree 6 of E is also immediately determined. In fact, Costello et al. described the following theorems.

Theorem 1 *If x_0 satisfies Eq. (8), the following tower of extension fields is always available.*

$$\begin{cases} \mathbb{F}_{p(x_0)^2} &= \mathbb{F}_{p(x_0)}[u]/(u^2+1), & \text{where } u^2 = -1, u \in \mathbb{F}_{p(x_0)^2}, \\ \mathbb{F}_{p(x_0)^4} &= \mathbb{F}_{p(x_0)^2}[v]/(v^2+u+1), & \text{where } v^2 = -(u+1), v \in \mathbb{F}_{p(x_0)^4}, \\ \mathbb{F}_{p(x_0)^{24}} &= \mathbb{F}_{p(x_0)^4}[w]/(w^6+v), & \text{where } w^6 = -v, w \in \mathbb{F}_{p(x_0)^{24}}, \end{cases}$$

Theorem 2 *If x_0 satisfies Eq. (8), the BLS curve $E/\mathbb{F}_{p(x_0)}$ is immediately determined as follows:*

$$E/\mathbb{F}_{p(x_0)} : \begin{cases} y^2 = x^3 + 1, & \text{if } x_0 \equiv 7, 31 \pmod{72}, \\ y^2 = x^3 + 4, & \text{if } x_0 \equiv 16 \pmod{72}, \\ y^2 = x^3 - 2, & \text{if } x_0 \equiv 64 \pmod{72}. \end{cases}$$

Theorem 3 *Suppose that the tower of extension fields of degree $k = 24$ and BLS curve $E/\mathbb{F}_{p(x_0)}$ are constructed as in Theorems 1 and 2 with x_0 satisfying Eq. (8). Then, the correct twist $E'/\mathbb{F}_{p(x_0)^4}$ of degree 6 of E is immediately determined as follows:*

$$E'/\mathbb{F}_{p(x_0)^4} : \begin{cases} y^2 = x^3 \pm 1/v, & \text{if } x_0 \equiv 7 \pmod{72}, \\ y^2 = x^3 \pm 4v, & \text{if } x_0 \equiv 16 \pmod{72}, \\ y^2 = x^3 \pm v, & \text{if } x_0 \equiv 31 \pmod{72}, \\ y^2 = x^3 \pm 2/v, & \text{if } x_0 \equiv 64 \pmod{72}. \end{cases}$$

Proof of Theorems 1, 2, and 3. Please refer to Sect. 3 in [11]. □

The field and curve options can reduce the time-consuming pre-computation of the curve constructions. Moreover, these fixed constructions give rise to the flexibility of scaling the size of the parameters without changing any of the implementations for the field and curve arithmetics. Thus, it is important to clarify the restrictions of x_0 which result in such BLS subfamilies, however, there exists only the work for the case of $k = 24$.

4 Mathematical Fundamentals

The authors describe the mathematical preliminaries to derive the restrictions of the integer parameter for the BLS family of pairing-friendly elliptic curves which are referred to in the previous work [11]. In the following, Sect. 4.1 and 4.2 provide the power residue properties and construction method of extension fields, respectively. Besides, Sect. 4.3 describes the possible group orders of the ordinary curves with $D = 3$ including the BLS family.

4.1 Power residue properties

Let p be a prime and d be a cofactor of $\#\mathbb{F}_p^* = p-1$. If there exists $g \in \mathbb{F}_p^*$ such that $a = g^d$, we say that *a is d-th residue in $\mathbb{F}_p^*$*, otherwise, we say that *a is d-th non-residue in $\mathbb{F}_p^*$*. The d-th residue properties can be determined by the value of $a^{(p-1)/d} \in \{1, \zeta, \zeta^2, \ldots \zeta^{d-1}\}$ where ζ is a primitive d-th root of the identity in $\mathbb{F}_p^*$. In the following, the authors discuss the cases of $d = 2$ and 3.

Let $(\frac{a}{p})$ be a symbol defined as $(\frac{a}{p}) = a^{(p-1)/2} \in \{1, -1\}$, which is known as the Legendre symbol. If $(\frac{a}{p}) = 1$, a is quadratic residue in $\mathbb{F}_p^*$, otherwise, a is quadratic non-residue in $\mathbb{F}_p^*$. Similarly, let $(\frac{a}{p})_3$ be a symbol defined as $(\frac{a}{p})_3 = a^{(p-1)/3} \in \{1, \epsilon, \epsilon^2\}$ where ϵ is a primitive cube root of the identity in $\mathbb{F}_p^*$. If $(\frac{a}{p})_3 = 1$, a is cubic residue in $\mathbb{F}_p^*$, otherwise, a is cubic non-residue in $\mathbb{F}_p^*$. Then, there are the following lemmas.

Lemma 1 *For an odd prime p, the following is true.*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4, \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$
$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8, \\ -1 & \text{if } p \equiv \pm 3 \pmod 8, \end{cases}$$
$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 3, \\ -1 & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

Proof of Lemma 1. Please refer to [25]. □

Lemma 2 *(Euler's conjecture.)*[2] *Let p be a prime $p \equiv 1 \pmod 3$ written as $p = a^2 + 3b^2$ with integers a and b. Then, the following is true.*

$$\left(\frac{2}{p}\right)_3 \begin{cases} = 1 & \text{if } 3 \mid b, \\ \neq 1 & \text{if } 3 \nmid b. \end{cases}$$

Proof of Lemma 2. Please refer to [26]. □

The power residue properties can also be extended for an extension field $\mathbb{F}_q$ of $\mathbb{F}_p$, where $q = p^n$ with an integer $n > 1$. For $\alpha \in \mathbb{F}_q^*$, let $N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha)$ be the norm of α defined over $\mathbb{F}_p^*$ which is a multiplicative function defined by the product of all the conjugates of α, i.e.,

$$N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) = \prod_{i=0}^{n-1} (\alpha)^{p^i} \in \mathbb{F}_p^*. \tag{9}$$

If $p \mid (d-1)$, the d-th power residue properties of α in $\mathbb{F}_q^*$ can be regarded as d-th residue properties of $N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha)$ in $\mathbb{F}_p^*$ since $\alpha^{(q-1)/d} = N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha)^{(p-1)/d}$.

4.2 Constructing the extension fields

Let p be a prime and $q = p^n$ with an integer $n > 0$. To admit an extension field $\mathbb{F}_{q^m}$ of degree m of $\mathbb{F}_q$ defined as $\mathbb{F}_{q^m} = \mathbb{F}_q(x) = \mathbb{F}_q[x]/(x^m - \zeta)$ with $\zeta \in \mathbb{F}_q$, it is known that the binomial $x^m - \zeta$ must be irreducible in $\mathbb{F}_q[x]$. Note that the details are shown in [27]. According to [5], the irreducibility of the binomial can be verified as follows:

[2] Although Euler's conjecture is traditionally called "conjecture", it has already been proven.

Lemma 3 *The binomial $x^m - \zeta$ is irreducible in $\mathbb{F}_q[x]$ if the following two conditions are satisfied.*

(a) Each prime factor d of m divides $(p-1)$ and $N_{\mathbb{F}_q/\mathbb{F}_p}(\zeta)$ is d-th non-residue in $\mathbb{F}_p^*$.
(b) If $m \equiv 0 \pmod 4$, then $q \equiv 1 \pmod 4$.

Proof of Lemma 3. Please refer to [5]. □

In [5], Benger and Scott described that a condition of p for constructing a fixed extension field of degree $k = 2^m \cdot 3^n$ for $n, m > 0$ can be easily obtained by applying Lemma 3 since the quadratic and cubic residue properties of the specific element in $\mathbb{F}_p^*$ can be obtained by Lemmas 1 and 2. As examples, they provided conditions for constructing some implementation-friendly towers of extension fields for the BN and KSS families of curves with $k = 12$ and 18, respectively. With the same strategy, Costello et al. reached the condition of the integer parameter x_0 for constructing the tower of extension fields as shown in Theorem 1.

4.3 Determining the curve equations

Let p be a prime such that $p \equiv 1 \pmod 6$ and let $q = p^n$ with an integer $n > 0$. Let $E/\mathbb{F}_q$ be an ordinary elliptic curve defined over $\mathbb{F}_q$ with $D = 3$, i.e., $j(E) = 0$, which has the curve equation $y^2 = x^3 + b$. Then, all the possible group orders $\#E(\mathbb{F}_q)$ can be obtained by taking $b \in \{1, g, g^2, g^3, g^4, g^5\}$ where g is quadratic and cubic non-residue in $\mathbb{F}_q^*$. Indeed, the possible orders are given as follows:

$$\begin{cases} n_0 &= q + 1 - t, \\ n_1 &= q + 1 - (t - 3V)/2, \\ n_2 &= q + 1 - (-t - 3V)/2, \\ n_3 &= q + 1 + t, \\ n_4 &= q + 1 - (-t + 3V)/2, \\ n_5 &= q + 1 - (t + 3V)/2, \end{cases} \tag{10}$$

where t and V are integers satisfying $3V^2 = 4q - t^2$. Therefore, the curve E with the specific order can be obtained by a randomly chosen b with a probability of 1/6.

Let $E'/\mathbb{F}_q$ be a twist of degree d of E. Since $j(E) = 0$, there are only the possibilities $d \in \{1, 2, 3, 6\}$. The curve equation of $E'/\mathbb{F}_q$ is given as $y^2 = x^3 + b/\delta$ where

$$\delta \text{ is } \begin{cases} \text{quadratic and cubic residue in } \mathbb{F}_q^* & \text{if } d = 1, \\ \text{quadratic non-residue and cubic residue in } \mathbb{F}_q^* & \text{if } d = 2, \\ \text{quadratic residue and cubic non-residue in } \mathbb{F}_q^* & \text{if } d = 3, \\ \text{quadratic and cubic non-residue in } \mathbb{F}_q^* & \text{if } d = 6. \end{cases} \tag{11}$$

Thus, once E is determined, the possibilities of finding the twist E' of degree $d = \{1, 2\}$ and $\{3, 6\}$ of E are 1 and 1/2, respectively. According to [21], if $\#E(\mathbb{F}_q) = n_0$, the possible group orders $\#E'(\mathbb{F}_q)$ are also determined as follows:

$$\#E'(\mathbb{F}_q) = \begin{cases} n_0 & \text{if } d = 1, \\ n_3 & \text{if } d = 2, \\ n_2, n_4 & \text{if } d = 3, \\ n_1, n_5 & \text{if } d = 6. \end{cases} \tag{12}$$

The curve equations can be determined or narrowed down by checking the small cofactors of $\#E(\mathbb{F}_q)$ by using the following Lemma 4. Note that (a) and (b) in Lemma 4 are found by [11] (similar lemmas can also be found in [29,33]), and (c) is found by this work. The authors also show the complete proof of Lemma 4.

Lemma 4 *Let E be an ordinary elliptic curve with $D = 3$ defined over $\mathbb{F}_q$, where $q = p^n$ with an integer $n > 0$ and p is an odd prime such that $p \equiv 1 \pmod 6$. Then, the following is true.*

(a) If and only if $2 \mid \#E(\mathbb{F}_q)$, b is cubic residue in $\mathbb{F}_q^*$.

(b) *If and only if* $3 \mid \#E(\mathbb{F}_q)$ *and* $9 \nmid \#E(\mathbb{F}_q)$, b *is quadratic residue in* $\mathbb{F}_q^*$ *and* $4b$ *is cubic non-residue in* $\mathbb{F}_q^*$.
(c) *If and only if* $9 \mid \#E(\mathbb{F}_q)$, b *is quadratic residue in* $\mathbb{F}_q^*$ *and* $4b$ *is cubic residue in* $\mathbb{F}_q^*$.

Proof of Lemma 4. (a): If $2 \mid \#E(\mathbb{F}_q)$, $E(\mathbb{F}_q)$ involves points of order 2 given as $P_2 = (-\sqrt[3]{b}, 0)$, which is not equal to $\mathcal{O}$. Thus, b is cubic residue in $\mathbb{F}_q^*$.

(b): If $3 \mid \#E(\mathbb{F}_q)$, $E(\mathbb{F}_q)$ involves a subgroup or subgroups of $E(\mathbb{F}_q)$ of order 3, i.e., there exists a group structure given as $E(\mathbb{F}_q)[3] \cong \mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, which consists points of order 3 given as $P_3 = (0, \sqrt{b})$ or both P_3 and $P_3' = (-\sqrt[3]{4b}, \sqrt{-3} \cdot \sqrt{b})$. Note that $\sqrt{-3} \in \mathbb{F}_q$ from (c) in Lemma 1. If $3 \mid \#E(\mathbb{F}_q)$ and $9 \nmid \#E(\mathbb{F}_q)$, then $E(\mathbb{F}_q)$ has a group structure of $E(\mathbb{F}_q)[3] \cong \mathbb{Z}/3\mathbb{Z}$ but does not have $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. This means P_3 is in $E(\mathbb{F}_q)$ but P_3' is not in $E(\mathbb{F}_q)$. Therefore, it is found that b is quadratic residue in $\mathbb{F}_q^*$ and $4b$ is cubic non-residue in $\mathbb{F}_q^*$.

(c): If $9 \mid \#E(\mathbb{F}_q)$, $E(\mathbb{F}_q)$ involves either $E(\mathbb{F}_q)[9] \cong \mathbb{Z}/9\mathbb{Z}$ or $E(\mathbb{F}_q)[3] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Indeed, $E(\mathbb{F}_q)$ does not have $E(\mathbb{F}_q)[9] \cong \mathbb{Z}/9\mathbb{Z}$ but has $E(\mathbb{F}_q)[3] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ by the following reasons.

(i) In this case of q, 9 does not divide the possible group orders expect for $\#E(\mathbb{F}_q)$. This can be easily found by checking the values of the possible group orders modulo 9 with the possible q, t, and V satisfying $3V^2 = 4q - t^2$.
(ii) There exists an ordinary elliptic curve given as $\tilde{E}/\mathbb{F}_q : y^2 = x^3 + \tilde{b}$ defined over $\mathbb{F}_q$ having a group order of multiple of 9 with the group structure $\tilde{E}(\mathbb{F}_q)[3] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ since there exactly exists $\tilde{b}$ in $\mathbb{F}_q^*$ which gives rise to points of order 3 denoted as $\tilde{P}_3 = (0, \sqrt{\tilde{b}})$ and $\tilde{P}_3' = (-\sqrt[3]{4\tilde{b}}, \sqrt{-3} \cdot \sqrt{\tilde{b}})$ in $\tilde{E}(\mathbb{F}_q)$.

The above means that E is isomorphic to $\tilde{E}$ over $\mathbb{F}_q$. Thus, there exist points P_3 and P_3' in $E(\mathbb{F}_q)$ and b is quadratic residue in $\mathbb{F}_q^*$ and $4b$ is cubic residue in $\mathbb{F}_q^*$. □

In [11], Costello et al. applied (a) and (b) of Lemma 4 for the BLS family of pairing-friendly elliptic curves with $k = 24$ and completely determined the curve equations as found in Theorems 2 and 3. Thus, there is a possibility that this strategy is also available for the BLS family of curves with the other embedding degrees.

5 Group Order of Correct Twists

To determine the twist equation by using Lemma 4, the knowledge of the group order of the correct twist is required. In the following Sect. 5.1 and 5.2, the authors give the knowledge for the BLS family of curves for $k = 2^m \cdot 3$ and 3^n with any $m, n > 0$, respectively.

5.1 The case of $k = 2^m \cdot 3$ for any $m > 0$

Let $p(x)$, $r(x)$, $t(x)$, and $V(x)$ be the polynomials fixed as Eq. (6) for the BLS family of pairing-friendly elliptic curves with $k = 2^m \cdot 3$ for any $m > 0$. For an integer x_0 making $p(x_0)$ and $r(x_0)$ being primes and $t(x_0)$ and $V(x_0)$ being integers, let $E/\mathbb{F}_{p(x_0)}$ and $E'/\mathbb{F}_{p(x_0)^{2^{m-1}}}$ be the BLS curve and correct twist of degree 6 of E. For any integer $s > 0$, let $t_s(x_0) = p(x_0)^s + 1 - \#E(\mathbb{F}_{p(x_0)^s})$ be a trace of E defined over $\mathbb{F}_{p(x_0)^s}$ and $V_s(x_0)$ be a parameter such that $3V_s(x_0)^2 = 4p(x_0)^s - t_s(x_0)^2$. Then, the group order of the correct twist is specifically represented in the following.

Theorem 4 *For* $k = 2^m \cdot 3$ *with any* $m > 0$, *the group order of the correct twist* $E'/\mathbb{F}_{p(x_0)^{2^{m-1}}}$ *of degree* 6 *of* E *is uniquely given as*

$$\#E'(\mathbb{F}_{p(x_0)^{2^{m-1}}}) = p(x_0)^{2^{m-1}} + 1 - \frac{t_{2^{m-1}}(x_0) - 3V_{2^{m-1}}(x_0)}{2}.$$

To prove Theorem 4, the authors provide the following Lemmas 5, 6, and 7.

Lemma 5 *For any integer $l \geq 0$, $t_{2^{l+1}}(x_0)$ and $V_{2^{l+1}}(x_0)$ can be built from the knowledge of $t_{2^l}(x_0)$ and $V_{2^l}(x_0)$ as follows:*

$$t_{2^{l+1}}(x_0) = t_{2^l}(x_0)^2 - 2p(x_0)^{2^l},$$
$$V_{2^{l+1}}(x_0) = t_{2^l}(x_0) \cdot V_{2^l}(x_0).$$

Proof of Lemma 5. According to Theorem 2.3.1 in [36], for any $l > 0$, the trace $t_{2^l}(x_0) = p^{2^l} + 1 - \#E(\mathbb{F}_{p(x_0)^{2^l}})$ can be written as $t_{2^l}(x_0) = \alpha^{2^l} + \beta^{2^l}$ where α and β are roots of the polynomial $X^2 - t(x_0) \cdot X + p(x_0)$, i.e., $\alpha \cdot \beta = p(x_0)$ and $\alpha + \beta = t(x_0)$. Thus, $t_{2^{l+1}}(x_0)$ can be represented as

$$t_{2^{l+1}}(x_0) = \alpha^{2^{l+1}} + \beta^{2^{l+1}} = (\alpha^{2^l} + \beta^{2^l})^2 - 2(\alpha \cdot \beta)^{2^l} = t_{2^l}(x_0)^2 - 2p(x_0)^{2^l}.$$

Moreover, with the above, the following is also obtained.

$$\begin{aligned} 3V_{2^{l+1}}(x_0)^2 &= 4p(x_0)^{2^{l+1}} - t_{2^{l+1}}(x_0)^2 \\ &= 4p(x_0)^{2^{l+1}} - (t_{2^l}(x_0)^2 - 2p(x_0)^{2^l})^2 \\ &= 4p(x_0)^{2^{l+1}} - t_{2^l}(x_0)^4 + 4t_{2^l}(x_0)^2 \cdot p(x_0)^{2^l} - 4p(x_0)^{2^{l+1}} \\ &= t_{2^l}(x_0)^2 \cdot (4 \cdot p(x_0)^{2^l} - t_{2^l}(x_0)^2) \\ &= t_{2^l}(x_0)^2 \cdot 3V_{2^l}(x_0)^2, \end{aligned}$$

which leads to $V_{2^{l+1}}(x_0) = t_{2^l}(x_0) \cdot V_{2^l}(x_0)$. □

Lemma 6 *For any integer $l \geq 0$, the following holds.*

$$t_{2^l}(x_0) \equiv x_0^{2^l} + 1 \pmod{r(x_0)}.$$

Proof of Lemma 6. The authors give proof of the lemma by induction on l.

(i) For $l = 0$, it is obvious that $t_{2^0}(x_0) = t(x_0) \equiv x_0 + 1 \pmod{r(x_0)}$.

(ii) For $l = s$ with an integer $s > 0$, suppose that $t_{2^s}(x_0) \equiv x_0^{2^s} + 1 \pmod{r(x_0)}$. According to Lemma 5 and $p(x_0) = (x_0 - 1)/3 \cdot r(x_0) + x_0 \equiv x_0 \pmod{r(x_0)}$, we have the following.

$$\begin{aligned} t_{2^{s+1}}(x_0) &= t_{2^s}(x_0)^2 - 2p(x_0)^{2^s} \\ &\equiv t_{2^s}(x_0)^2 - 2x_0^{2^s} && \pmod{r(x_0)} \\ &\equiv (x_0^{2^s} + 1)^2 - 2x_0^{2^s} && \pmod{r(x_0)} \\ &\equiv x_0^{2^{s+1}} + 1 && \pmod{r(x_0)}. \end{aligned}$$

Thus, $t_{2^{s+1}}(x_0) \equiv x_0^{2^{s+1}} + 1 \pmod{r(x_0)}$ is also true for $l = s + 1$.

Since both the base case (i) and the inductive step (ii) have been proven, $t_{2^l}(x_0) \equiv x_0^{2^l} + 1 \pmod{r(x_0)}$ holds for any $l \geq 0$. □

Lemma 7 *For any integer $l > 0$, the following holds.*

$$\frac{t_{2^l}(x_0) \pm 3V_{2^l}(x_0)}{2} \equiv \sum_{i=0}^{2^l-1} x_0^i \cdot \frac{t(x_0) \pm 3V(x_0)}{2} - \sum_{i=1}^{2^l-1} x_0^i \pmod{r(x_0)}.$$

Proof of Lemma 7. The authors give proof of the lemma by induction on l.

(i) For $l = 1$, from Lemmas 5, 6, and $p(x_0) \equiv x_0 \pmod{r(x_0)}$, the following can be obtained.

$$\begin{aligned} \frac{t_2(x_0) \pm 3V_2(x_0)}{2} &= \frac{(t(x_0)^2 - 2p(x_0)) \pm (t(x_0) \cdot 3V(x_0))}{2} \\ &= t(x_0) \cdot \frac{t(x_0) \pm 3V(x_0)}{2} - p(x_0) \\ &\equiv (x_0 + 1) \cdot \frac{t(x_0) \pm 3V(x_0)}{2} - x_0 \pmod{r(x_0)}. \end{aligned}$$

Thus, the lemma is true for $l = 1$.

(ii) For $l = s$ with an integer $s > 1$, suppose that the lemma is true. Then, we have the following.

$$\begin{aligned}
\frac{t_{2^{s+1}}(x_0) \pm 3V_{2^{s+1}}(x_0)}{2} &= \frac{(t_{2^s}(x_0)^2 - 2p(x_0)^{2^s}) \pm (t_{2^s}(x_0) \cdot 3V_{2^s}(x_0))}{2} \\
&= t_{2^s}(x_0) \cdot \frac{t_{2^s}(x_0) \pm 3V_{2^s}(x_0)}{2} - p(x_0)^{2^s} \\
&\equiv (x_0^{2^s} + 1) \cdot \left(\sum_{i=0}^{2^s-1} x_0^i \cdot \frac{t(x_0) \pm 3V(x_0)}{2} - \sum_{i=1}^{2^s-1} x_0^i \right) - x_0^{2^s} \pmod{r(x_0)} \\
&\equiv \left(\sum_{i=2^s}^{2^{s+1}-1} x_0^i + \sum_{i=0}^{2^s-1} x_0^i \right) \cdot \frac{t(x_0) \pm 3V(x_0)}{2} \\
&\qquad - \sum_{i=2^s+1}^{2^{s+1}-1} x_0^i - \sum_{i=1}^{2^s-1} x_0^i - x_0^{2^s} \pmod{r(x_0)} \\
&\equiv \sum_{i=0}^{2^{s+1}-1} x_0^i \cdot \frac{t(x_0) \pm 3V(x_0)}{2} - \sum_{i=1}^{2^{s+1}-1} x_0^i \pmod{r(x_0)}.
\end{aligned}$$

Thus, the lemma is also true for $l = s + 1$.

Since both the base case (i) and the inductive step (ii) have been proven, it is clear that the lemma is true for any $l > 0$. □

Then, the authors provide the proof of Theorem 4 by using the above lemmas.

Proof of Theorem 4. According to Eq. (12), the group order of the twist of $E/\mathbb{F}_{p(x_0)}$ can be determined corresponding the twist degree d. In this case, since $d = 6$, it is found that $\#E'(\mathbb{F}_{p(x_0)^{2^{m-1}}})$ is given by one of the following.

$$\begin{aligned}
n'_0(x_0) &= p(x_0)^{2^{m-1}} + 1 - \frac{t_{2^{m-1}}(x_0) + 3V_{2^{m-1}}(x_0)}{2}, \\
n'_1(x_0) &= p(x_0)^{2^{m-1}} + 1 - \frac{t_{2^{m-1}}(x_0) - 3V_{2^{m-1}}(x_0)}{2},
\end{aligned}$$

Besides, from the definition, the group order of the correct twist is divisible by $r(x_0)$. Thus, to prove the theorem, it is enough to show that $r(x_0)$ divides $n'_1(x_0)$ but does not divide $n'_0(x_0)$, i.e., $n'_0(x_0) \not\equiv 0 \pmod{r(x_0)}$ and $n'_1(x_0) \equiv 0 \pmod{r(x_0)}$. Note that $r(x_0) = x_0^{2^m} - x_0^{2^{m-1}} + 1 \equiv 0 \pmod{r(x_0)}$ in this case.

Applying Lemma 7, the possible group orders $n'_0(x_0)$ modulo $r(x_0)$ can be denoted as follows:

$$\begin{aligned}
n'_0(x_0) &\equiv x_0^{2^{m-1}} + 1 - \left(\sum_{i=0}^{2^{m-1}-1} x_0^i \cdot \frac{t(x_0) + 3V(x_0)}{2} - \sum_{i=1}^{2^{m-1}-1} x_0^i \right) && \pmod{r(x_0)} \\
&\equiv x_0^{2^{m-1}} + 1 - \sum_{i=0}^{2^{m-1}-1} x_0^i \cdot ((x_0 - 1) \cdot x^{2^{m-1}} + 1) + \sum_{i=1}^{2^{m-1}-1} x_0^i && \pmod{r(x_0)} \\
&\equiv x_0^{2^{m-1}} + 1 - (x_0^{2^{m-1}} - 1) \cdot x_0^{2^{m-1}} - \sum_{i=0}^{2^{m-1}-1} x_0^i + \sum_{i=1}^{2^{m-1}-1} x_0^i && \pmod{r(x_0)} \\
&\equiv x_0^{2^{m-1}} + 1 - x_0^{2^m} + x_0^{2^{m-1}} - 1 && \pmod{r(x_0)} \\
&\equiv -x_0^{2^m} + 2x_0^{2^{m-1}} && \pmod{r(x_0)}.
\end{aligned}$$

On the other hand, for $n_1'(x_0)$ modulo $r(x_0)$, we have the following.

$$\begin{aligned}
n_1'(x_0) &\equiv x_0^{2^{m-1}} + 1 - \left(\sum_{i=0}^{2^{m-1}-1} x_0^i \cdot \frac{t(x_0) - 3V(x_0)}{2} - \sum_{i=1}^{2^{m-1}-1} x_0^i \right) && \pmod{r(x_0)} \\
&\equiv x_0^{2^{m-1}} + 1 - \sum_{i=0}^{2^{m-1}-1} x_0^i \cdot (-(x_0-1) \cdot x^{2^{m-1}} + x_0) + \sum_{i=1}^{2^{m-1}-1} x_0^i && \pmod{r(x_0)} \\
&\equiv x_0^{2^{m-1}} + 1 + (x_0^{2^{m-1}} - 1) \cdot x_0^{2^{m-1}} - \sum_{i=1}^{2^{m-1}} x_0^i + \sum_{i=1}^{2^{m-1}-1} x_0^i && \pmod{r(x_0)} \\
&\equiv x_0^{2^{m-1}} + 1 + x_0^{2^m} - x_0^{2^{m-1}} - x_0^{2^{m-1}} && \pmod{r(x_0)} \\
&\equiv x_0^{2^m} - x_0^{2^{m-1}} + 1 && \pmod{r(x_0)} \\
&\equiv 0 && \pmod{r(x_0)},
\end{aligned}$$

Thus, Theorem 4 is true. □

5.2 The case of $k = 3^n$ for any $n > 0$

Let $p(x)$, $r(x)$, $t(x)$, and $V(x)$ be the polynomials fixed as Eq. (7) for the BLS family of pairing-friendly elliptic curves with $k = 3^n$ for any $n > 0$. For an integer x_0 making $p(x_0)$ and $r(x_0)$ being primes and $t(x_0)$ and $V(x_0)$ being integers, let $E/\mathbb{F}_{p(x_0)}$ and $E'/\mathbb{F}_{p(x_0)^{3^{n-1}}}$ be the BLS curve and correct twist of degree 3 of E. For any integer $s > 0$, let $t_s(x_0) = p(x_0)^s + 1 - \#E(\mathbb{F}_{p(x_0)^s})$ be a trace of E defined over $\mathbb{F}_{p(x_0)^s}$ and $V_s(x_0)$ be an integer such that $3V_s(x_0)^2 = 4p(x_0)^s - t_s(x_0)^2$. Then, the group order of the correct twist can be represented as shown in the below.

Theorem 5 *For $k = 3^n$ with any $n > 0$, the group order of the correct twist $E'/\mathbb{F}_{p(x_0)^{3^{n-1}}}$ of degree 3 of E is uniquely given as the following.*

$$\#E'(\mathbb{F}_{p(x_0)^{3^{n-1}}}) = p(x_0)^{3^{n-1}} + 1 - \frac{-t_{3^{n-1}}(x_0) - 3V_{3^{n-1}}(x_0)}{2}.$$

Theorem 5 can be proven with the following Lemmas 8, 9, and 10.

Lemma 8 *For any integer $l \geq 0$, $t_{3^{l+1}}(x_0)$ and $V_{3^{l+1}}(x_0)$ can be built from the knowledge of $t_{3^l}(x_0)$ and $V_{3^l}(x_0)$ as follows:*

$$\begin{aligned}
t_{3^{l+1}}(x_0) &= t_{3^l}(x_0)^3 - 3p(x_0)^{3^l} \cdot t_{3^l}(x_0), \\
V_{3^{l+1}}(x_0) &= V_{3^l}(x_0) \cdot (t_{3^l}(x_0)^2 - p(x_0)^{3^l}).
\end{aligned}$$

Proof of Lemma 8. Similar to proof of Lemma 5, for any $l > 0$, the trace $t_{3^l}(x_0) = p^{3^l} + 1 - \#E(\mathbb{F}_{p(x_0)^{3^l}})$ can be written as $t_{3^l}(x_0) = \alpha^{3^l} + \beta^{3^l}$ where α and β are roots of the polynomial $X^2 - t(x_0) \cdot X + p(x_0)$, i.e., $\alpha \cdot \beta = p(x_0)$ and $\alpha + \beta = t(x_0)$ (see [36]). Thus, $t_{3^{l+1}}(x_0)$ can be denoted as follows:

$$t_{3^{l+1}}(x_0) = \alpha^{3^{l+1}} + \beta^{3^{l+1}} = (\alpha^{3^l} + \beta^{3^l})^3 - 3(\alpha \cdot \beta)^{3^l} \cdot (\alpha^{3^l} + \beta^{3^l}) = t_{3^l}(x_0)^3 - 3p(x_0)^{3^l} \cdot t_{3^l}(x_0).$$

Besides, we also have the following.

$$\begin{aligned}
3V_{3^{l+1}}(x_0)^2 &= 4p(x_0)^{3^{l+1}} - t_{3^{l+1}}(x_0)^2 \\
&= 4p(x_0)^{3^{l+1}} - (t_{3^l}(x_0)^3 - 3p(x_0)^{3^l} \cdot t_{3^l}(x_0))^2 \\
&= 4p(x_0)^{3^{l+1}} - t_{3^l}(x_0)^6 + 6p(x_0)^{3^l} \cdot t_{3^l}(x_0)^4 - 9p(x_0)^{2 \cdot 3^l} \cdot t_{3^l}(x_0)^2 \\
&= (4p(x_0)^{3^l} - t_{3^l}(x_0)^2) \cdot (t_{3^l}(x_0)^2 - p(x_0)^{3^l})^2 \\
&= 3V_{3^l}(x_0)^2 \cdot (t_{3^l}(x_0)^2 - p(x_0)^{3^l})^2,
\end{aligned}$$

which leads to $V_{3^{l+1}}(x_0) = V_{3^l}(x_0) \cdot (t_{3^l}(x_0)^2 - p(x_0)^{3^l})$. □

Lemma 9 *For any integer $l \geq 0$, the following holds.*

$$t_{3^l}(x_0) \equiv x_0^{3^l} + 1 \pmod{r(x_0)}.$$

Proof of Lemma 9. The authors give proof of the lemma by induction on l.

(i) For $l = 0$, it is clear that $t_{3^0}(x_0) = t(x_0) \equiv x_0 + 1 \pmod{r(x_0)}$.

(ii) For $l = s$ with an integer $s > 0$, let $t_{3^s}(x_0) \equiv x_0^{3^s} + 1 \pmod{r(x_0)}$ be ture. Then, according to Lemma 5 and $p(x_0) \equiv x_0 \pmod{r(x_0)}$, the case of $l = s + 1$ can be obtained as follows:

$$\begin{aligned} t_{3^{s+1}}(x_0) &= t_{3^l}(x_0)^3 - 3p(x_0)^{3^s} \cdot t_{3^s}(x_0) \\ &\equiv (x_0^{3^s} + 1)^3 - 3x_0^{3^s} \cdot (x_0^{3^s} + 1) && \pmod{r(x_0)} \\ &\equiv x_0^{3^{s+1}} + 3x_0^{2\cdot 3^s} + 3x_0^{3^s} + 1 - 3x_0^{2\cdot 3^s} - 3x_0^{3^s} && \pmod{r(x_0)} \\ &\equiv x_0^{3^{s+1}} + 1 && \pmod{r(x_0)}. \end{aligned}$$

Thus, $t_{3^{s+1}}(x_0) \equiv x_0^{3^{s+1}} + 1 \pmod{r(x_0)}$ is also held for $l = s + 1$.

Since both the base case (i) and inductive step (ii) have been proven, $t_{3^l}(x_0) \equiv x_0^{3^l} + 1 \pmod{r(x_0)}$ is true for any $l > 0$. □

Lemma 10 *For any integer $l > 0$, the following holds.*

$$\frac{-t_{3^l}(x_0) \pm 3V_{3^l}(x_0)}{2} \equiv \sum_{i=0}^{3^l-1} x_0^i \cdot \frac{-t(x_0) \pm 3V(x_0)}{2} + \sum_{i=1}^{3^l-1} x_0^i \pmod{r(x_0)}.$$

Proof of Lemma 10. The authors give proof of the lemma by induction on l.

(i) For $l = 1$, from Lemmas 8, 9, and $p(x_0) \equiv x_0 \pmod{r(x_0)}$, we can find the following.

$$\begin{aligned} \frac{-t_3(x_0) \pm 3V_3(x_0)}{2} &= \frac{-(t(x_0)^3 - 3p(x_0) \cdot t(x_0)) \pm 3V(x_0) \cdot (t(x_0)^2 - p(x_0))}{2} \\ &= \frac{-t(x_0) \cdot (t(x_0)^2 - p(x_0)) + 2p(x_0) \cdot t(x_0) \pm 3V(x_0) \cdot (t(x_0)^2 - p(x_0))}{2} \\ &= (t(x_0)^2 - p(x_0)) \cdot \frac{-t(x_0) \pm 3V(x_0)}{2} + p(x_0) \cdot t(x_0). \end{aligned}$$

Then, taking modulo $r(x_0)$,

$$\frac{-t_3(x_0) \pm 3V_3(x_0)}{2} \equiv (x_0^2 + x_0 + 1) \cdot \frac{-t(x_0) \pm 3V(x_0)}{2} + (x_0^2 + x_0) \pmod{r(x_0)}.$$

The above shows that the lemma is true for $l = 1$.

(ii) For $l = s$ with an integer $s > 1$, suppose that the lemma is true. With the assumption, for $l = s + 1$, the following can be obtained.

$$\begin{aligned} \frac{-t_{3^{s+1}}(x_0) \pm 3V_{3^{s+1}}(x_0)}{2} &= \frac{-(t_{3^s}(x_0)^3 - 3p(x_0)^{3^s} \cdot t_{3^s}(x_0)) \pm 3V_{3^s}(x_0) \cdot (t_{3^s}(x_0)^2 - p(x_0)^{3^s})}{2} \\ &= \frac{-t_{3^s}(x_0) \cdot (t_{3^s}(x_0)^2 - p(x_0)^{3^s}) + 2p(x_0)^{3^s} \cdot t_{3^s}(x_0) \pm 3V_{3^s}(x_0) \cdot (t_{3^s}(x_0)^2 - p(x_0)^{3^s})}{2} \\ &= (t_{3^s}(x_0)^2 - p(x_0)^{3^s}) \cdot \frac{-t_{3^s}(x_0) \pm 3V_{3^s}(x_0)}{2} + p(x_0)^{3^s} \cdot t_{3^s}(x_0). \end{aligned}$$

Similarly, taking modulo $r(x_0)$, we have the following.

$$\begin{aligned}
\frac{-t_{3^{s+1}}(x_0) \pm 3V_{3^{s+1}}(x_0)}{2} &\equiv (x_0^{2\cdot 3^s} + x_0^{3^s} + 1) \cdot \left(\sum_{i=0}^{3^s-1} x_0^i \cdot \frac{-t(x_0) \pm 3V(x_0)}{2} + \sum_{i=1}^{3^s-1} x_0^i \right) \\
&\quad + (x_0^{2\cdot 3^s} + x_0^{3^s}) \pmod{r(x_0)} \\
&\equiv \left(\sum_{i=2\cdot 3^s}^{3^{s+1}-1} x_0^i + \sum_{i=3^s}^{2\cdot 3^s-1} x_0^i + \sum_{i=0}^{3^s-1} x_0^i \right) \cdot \frac{-t(x_0) \pm 3V(x_0)}{2} \\
&\quad + \sum_{i=2\cdot 3^s+1}^{3^{s+1}-1} x_0^i + \sum_{i=3^s+1}^{2\cdot 3^s-1} x_0^i + \sum_{i=1}^{3^s-1} x_0^i + (x_0^{2\cdot 3^s} + x_0^{3^s}) \pmod{r(x_0)} \\
&\equiv \sum_{i=0}^{3^{s+1}-1} x_0^i \cdot \frac{-t(x_0) \pm 3V(x_0)}{2} + \sum_{i=1}^{3^{s+1}-1} x_0^i \pmod{r(x_0)}.
\end{aligned}$$

Thus, the lemma is also true for $l = s + 1$.

Since both the base case (i) and the inductive step (ii) have been proven, the lemma is true for any $l > 0$. □

In the following, the authors provide the proof of Theorem 5 by using the above lemmas.

Proof of Theorem 5. According to Eq. (12), the group order $\#E(\mathbb{F}_{p(x_0)^{3^{n-1}}})$ of twist of degree 3 of $E/\mathbb{F}_{p(x_0)}$ is given by one of the following.

$$\begin{aligned}
n'_0(x_0) &= p(x_0)^{3^{n-1}} + 1 - \frac{-t_{3^{n-1}}(x_0) + 3V_{3^{n-1}}(x_0)}{2}, \\
n'_1(x_0) &= p(x_0)^{3^{n-1}} + 1 - \frac{-t_{3^{n-1}}(x_0) - 3V_{3^{n-1}}(x_0)}{2}.
\end{aligned}$$

Since the group order is divisible by $r(x_0)$, it is enough to show that $r(x_0)$ divides $n'_1(x_0)$ but does not divide $n'_0(x_0)$, i.e., $n'_0(x_0) \not\equiv 0 \pmod{r(x_0)}$ and $n'_1(x_0) \equiv 0 \pmod{r(x_0)}$. Applying Lemma 10, the possible group order $n'_0(x_0)$ modulo $r(x_0) = x_0^{2\cdot 3^{n-1}} + x_0^{3^{n-1}} + 1$ can be written as follows:

$$\begin{aligned}
n'_0(x_0) &\equiv x_0^{3^{n-1}} + 1 - \left(\sum_{i=0}^{3^{n-1}-1} x_0^i \cdot \frac{-t(x_0) + 3V(x_0)}{2} + \sum_{i=1}^{3^{n-1}-1} x_0^i \right) \pmod{r(x_0)} \\
&\equiv x_0^{3^{n-1}} + 1 - \sum_{i=0}^{3^{n-1}-1} x_0^i \cdot ((x_0 - 1) \cdot x_0^{3^{n-1}} - 1) - \sum_{i=1}^{3^{n-1}-1} x_0^i \pmod{r(x_0)} \\
&\equiv x_0^{3^{n-1}} + 1 - (x_0^{3^{n-1}} - 1) \cdot x_0^{3^{n-1}} + \sum_{i=0}^{3^{n-1}-1} x_0^i - \sum_{i=1}^{3^{n-1}-1} x_0^i \pmod{r(x_0)} \\
&\equiv x_0^{3^{n-1}} + 1 - x_0^{2\cdot 3^{n-1}} + x_0^{3^{n-1}} + 1 \pmod{r(x_0)} \\
&\equiv -x_0^{2\cdot 3^{n-1}} + 2x_0^{3^{n-1}} + 2 \pmod{r(x_0)}
\end{aligned}$$

For the case of $n_1'(x_0)$ modulo $r(x_0)$,

$$\begin{aligned}
n_0'(x_0) &\equiv x_0^{3^{n-1}} + 1 - \left(\sum_{i=0}^{3^{n-1}-1} x_0^i \cdot \frac{-t(x_0) - 3V(x_0)}{2} + \sum_{i=1}^{3^{n-1}-1} x_0^i \right) && (\mathrm{mod}\ r(x_0)) \\
&\equiv x_0^{3^{n-1}} + 1 - \sum_{i=0}^{3^{n-1}-1} x_0^i \cdot (-(x_0-1) \cdot x_0^{3^{n-1}} - x_0) - \sum_{i=1}^{3^{n-1}-1} x_0^i && (\mathrm{mod}\ r(x_0)) \\
&\equiv x_0^{3^{n-1}} + 1 + (x_0^{3^{n-1}} - 1) \cdot x_0^{3^{n-1}} + \sum_{i=1}^{3^{n-1}} x_0^i - \sum_{i=1}^{3^{n-1}-1} x_0^i && (\mathrm{mod}\ r(x_0)) \\
&\equiv x_0^{3^{n-1}} + 1 + x_0^{2\cdot 3^{n-1}} - x_0^{3^{n-1}} + x_0^{3^{n-1}} && (\mathrm{mod}\ r(x_0)) \\
&\equiv x_0^{2\cdot 3^{n-1}} + x_0^{3^{n-1}} + 1 && (\mathrm{mod}\ r(x_0)) \\
&\equiv 0 && (\mathrm{mod}\ r(x_0)).
\end{aligned}$$

From the above, Theorem 5 is true. □

6 Proposed Restriction of Integer Parameter for Generating Attractive BLS subfamilies

The authors extend Costello et al.'s work [11] and provide the restrictions of integer parameter for the BLS subfamilies of pairing-friendly elliptic curves with $k = 2^m \cdot 3$ and 3^n with any $m, n > 0$. The details of the proposals for the cases of $k = 2^m \cdot 3$ and 3^n are described in the following Sect. 6.1 and 6.2, respectively.

6.1 The case of $k = 2^m \cdot 3$ for any $m > 0$

Let x_0 be an integer parameter for the BLS family of pairing-friendly elliptic curves with $k = 2^m \cdot 3$ where $m > 0$ is an arbitrary integer. The authors propose to restrict x_0 as follows:

$$x_0 \equiv \begin{cases} 7, 10, 16, 28, 31, 34\ (\mathrm{mod}\ 36) & \textit{if } m = 1, \\ 7, 16, 31, 64\ (\mathrm{mod}\ 72) & \textit{if } m > 1. \end{cases} \tag{13}$$

Once finding x_0 under the above restrictions, we have the specific BLS subfamilies with the options (i) a fixed tower of extension fields with one of the best performing arithmetics is always available, (ii) the BLS curve $E/\mathbb{F}_{p(x_0)}$ is immediately determined, and (iii) the correct twist $E'/\mathbb{F}_{p(x_0)^{2^{m-1}}}$ is also immediately determined. These constructions also enable one of the simplest twist isomorphisms. The details of the field and curve options (i), (ii), and (iii) are summarized in Table 1. Note that the case of $m = 2$ can provide almost the same results of [11] described in Sect. 3.2. The authors also provide Theorems 6, 7, and 8 which show the correctness that the proposed BLS subfamilies have the options. Before the theorems, the authors present the knowledge of the quadratic and cubic residue properties in $\mathbb{F}_{p(x_0)}^*$ in the following Lemma 11.

Lemma 11 *For the symbols* $(\frac{\cdot}{p(x_0)})$ *and* $(\frac{\cdot}{p(x_0)})_3$*, the following is true.*

(a) For $m = 1$*,*

$$\left(\frac{-1}{p(x_0)}\right) = \begin{cases} 1 & \textit{if } x_0 \equiv 1\ (\mathrm{mod}\ 12), \\ -1 & \textit{if } x_0 \equiv 4, 7, 10\ (\mathrm{mod}\ 12). \end{cases}$$

For $m > 1$*,*

$$\left(\frac{-1}{p(x_0)}\right) = \begin{cases} 1 & \textit{if } x_0 \equiv 1, 10\ (\mathrm{mod}\ 12), \\ -1 & \textit{if } x_0 \equiv 4, 7\ (\mathrm{mod}\ 12). \end{cases}$$

Table 1: Field and curve options for the proposed BLS subfamilies of curves with $k = 2^m \cdot 3$ for any $m > 0$, where $z = v^6 \in \mathbb{F}_{p(x_0)^{2^{m-1}}}$ with $v \in \mathbb{F}_{p(x_0)^{2^m \cdot 3}}$ defined in Eq. (15).

(a) $m = 1$

x_0 (mod 36)	Tower *(see Theorem 6)*	BLS curve $E/\mathbb{F}_{p(x_0)}$ *(see Theorem 7)*	Twist $E'/\mathbb{F}_{p(x_0)^{2^{m-1}}}$ *(see Theorem 8)*
7	Eq. (14)	$y^2 = x^3 + 1$	$y^2 = x^3 - 4$
31	Eq. (14)	$y^2 = x^3 + 1$	$y^2 = x^3 - 1/4$
10, 28	Eq. (14)	$y^2 = x^3 - 2$	$y^2 = x^3 - 1$
16, 34	Eq. (14)	$y^2 = x^3 + 4$	$y^2 = x^3 - 1$

(b) $m > 1$

x_0 (mod 72)	Tower *(see Theorem 6)*	BLS curve $E/\mathbb{F}_{p(x_0)}$ *(see Theorem 7)*	Twist $E'/\mathbb{F}_{p(x_0)^{2^{m-1}}}$ *(see Theorem 8)*
7	Eq. (15)	$y^2 = x^3 + 1$	$y^2 = x^3 + 1/z$
16	Eq. (15)	$y^2 = x^3 + 4$	$y^2 = x^3 + 4z$
31	Eq. (15)	$y^2 = x^3 + 1$	$y^2 = x^3 + z$
64	Eq. (15)	$y^2 = x^3 - 2$	$y^2 = x^3 - 2/z$

(b) For $m = 1$,

$$\left(\frac{2}{p(x_0)}\right) = \begin{cases} 1 & \text{if } x_0 \equiv 1, 19 \pmod{24}, \\ -1 & \text{if } x_0 \equiv 4, 7, 10, 13, 16, 22 \pmod{24}. \end{cases}$$

For $m = 2$,

$$\left(\frac{2}{p(x_0)}\right) = \begin{cases} 1 & \text{if } x_0 \equiv 1, 4, 10, 19 \pmod{24}, \\ -1 & \text{if } x_0 \equiv 7, 13, 16, 22 \pmod{24}. \end{cases}$$

For $m > 2$,

$$\left(\frac{2}{p(x_0)}\right) = \begin{cases} 1 & \text{if } x_0 \equiv 1, 4, 19, 22 \pmod{24}, \\ -1 & \text{if } x_0 \equiv 7, 10, 13, 16 \pmod{24}. \end{cases}$$

(c) For $m > 0$,

$$\left(\frac{2}{p(x_0)}\right)_3 \begin{cases} = 1 & \text{if } x_0 \equiv 1, 4 \pmod{18}, \\ \neq 1 & \text{if } x_0 \equiv 7, 10, 13, 16 \pmod{18}. \end{cases}$$

Proof of Lemma 11. (a) and (b): The authors refer to Lemma 1 and verify the value of $p(x_0)$ modulo 4 and 8. As a result, (a) and (b) are obtained.

(c): The authors refer to Euler's conjecture given in Lemma 2. In the following, the authors classify x_0 satisfying $x_0 \equiv 1 \pmod 3$ into two cases, i.e., $x_0 \equiv 1 \pmod 6$ and $x_0 \equiv 4 \pmod 6$.

If $x_0 \equiv 1 \pmod 6$, $p(x_0)$ can be modified as follows:

$$\begin{aligned} p(x_0) &= \left(\frac{t(x_0)}{2}\right)^2 + 3\left(\frac{V(x_0)}{2}\right)^2 \\ &= \left(\frac{x_0 + 1}{2}\right)^2 + 3\left(\frac{x_0 - 1}{6} \cdot (2x_0^{2^{m-1}} - 1)\right)^2. \end{aligned}$$

For $b(x_0) = (x_0 - 1)/6 \cdot (2x_0^{2^{m-1}} - 1)$, if $x_0 \equiv 1 \pmod{18}$ then 3 divides $b(x_0)$; if $x_0 \equiv 7, 13 \pmod{18}$ then 3 does not divides $b(x_0)$. Thus, according to (b) in Lemma 2, if $x_0 \equiv 1 \pmod{18}$ then $(\frac{2}{p})_3 = 1$; if $x_0 \equiv 7, 13 \pmod{18}$ then $(\frac{2}{p})_3 \neq 1$.

If $x_0 \equiv 4 \pmod 6$, $p(x_0)$ can be represented as follows:

$$\begin{aligned} p(x_0) &= \left(\frac{t(x_0) - 3V(x_0)}{4}\right)^2 + 3\left(\frac{t(x_0) + V(x_0)}{4}\right)^2 \\ &= \left(\frac{-(x_0-1)\cdot x_0^{2^{m-1}} + x_0}{2}\right)^2 + 3\left(\frac{(x_0-1)\cdot x_0^{2^{m-1}} + x_0 + 2}{6}\right)^2. \end{aligned}$$

For $b(x_0) = ((x_0-1)\cdot x_0^{2^{m-1}} + x_0 + 2)/6$, if $x_0 \equiv 4 \pmod{18}$ then 3 divides $b(x_0)$; if $x_0 \equiv 10, 16 \pmod{18}$ then 3 does not divide $b(x_0)$. In the same manner, it is obtained that if $x_0 \equiv 4 \pmod{18}$ then $(\frac{2}{p(x_0)})_3 = 1$; if $x_0 \equiv 10, 16 \pmod{18}$ then $(\frac{2}{p(x_0)})_3 \neq 1$. □

Then, the authors provide Theorems 6, 7, and 8 associated with the construction of the tower of extension fields, BLS curve, and twist required for the pairing with the BLS family of curves with $k = 2^m \cdot 3$ with any $m > 0$.

Theorem 6 *If x_0 satisfy the condition Eq. (13), the following tower of extension fields is always available. For $m = 1$,*

$$\begin{cases} \mathbb{F}_{p(x_0)^2} &= \mathbb{F}_{p(x_0)}[u]/(u^2+1), & \text{where } u^2 = -1, u \in \mathbb{F}_{p(x_0)^2}, \\ \mathbb{F}_{p(x_0)^6} &= \mathbb{F}_{p(x_0)^2}[v]/(v^3-2), & \text{where } v^3 = 2, v \in \mathbb{F}_{p(x_0)^6}. \end{cases} \tag{14}$$

For $m > 1$,

$$\begin{cases} \mathbb{F}_{p(x_0)^2} &= \mathbb{F}_{p(x_0)}[u]/(u^2+1), & \text{where } u^2 = -1, u \in \mathbb{F}_{p(x_0)^2}, \\ \mathbb{F}_{p(x_0)^{2^m\cdot 3}} &= \mathbb{F}_{p(x_0)^2}[v]/(v^{2^{m-1}\cdot 3} - (u+1)), & \text{where } v^{2^{m-1}\cdot 3} = u+1, v \in \mathbb{F}_{p(x_0)^{2^m\cdot 3}}. \end{cases} \tag{15}$$

Proof of Theorem 6 For $m = 1$, to admit the tower of extension fields, the binomials u^2+1 and v^3-2 must be irreducible in $\mathbb{F}_{p(x_0)}[u]$ and $\mathbb{F}_{p^2(x_0)}[v]$, respectively. According to (a) in Lemma 3, the binomial u^2+1 is irreducible in $\mathbb{F}_{p(x_0)}[u]$ if -1 is quadratic non-residue in $\mathbb{F}_p^*$. The binomial v^3-2 is irreducible in $\mathbb{F}_{p(x_0)^2}[v]$ if the norm of 2, which is computed as $N_{\mathbb{F}_{p(x_0)^2}/\mathbb{F}_{p(x_0)}}(2) = 2\cdot 2^{p(x_0)} = 2^2 = 4 \in \mathbb{F}_{p(x_0)}$, is cubic non-residue in $\mathbb{F}_{p(x_0)}^*$. Note that (b) in Lemma 3 is satisfied for both cases. Since it is found that if x_0 satisfies Eq. (13), $(\frac{-1}{p(x_0)}) = -1$ and $(\frac{2}{p(x_0)})_3 \neq 1$ which results in $(\frac{4}{p(x_0)})_3 \neq 1$ from Lemma 11, the tower is available.

Similarly, for $m > 1$, to admit the tower of extension fields, the binomials u^2+1 and $v^{2^{m-1}\cdot 3} - (u+1)$ must be irreducible in $\mathbb{F}_{p(x_0)}[u]$ and $\mathbb{F}_{p^2(x_0)}[v]$, respectively. According to (a) in Lemma 3, the binomial u^2+1 is irreducible in $\mathbb{F}_{p(x_0)}[u]$ if -1 is quadratic non-residue in $\mathbb{F}_p^*$. The binomial $v^{2^{m-1}\cdot 3} - (u+1)$ is irreducible in $\mathbb{F}_{p(x_0)^2}$ if the the norm of $(u+1)$, which is computed by $N_{\mathbb{F}_{p(x_0)^2}/\mathbb{F}_{p(x_0)}}(u+1) = (u+1)\cdot(u+1)^{p(x_0)} = (u+1)\cdot(-u+1) = -u^2+1 = 2 \in \mathbb{F}_{p(x_0)}$, is quadratic and cubic non-residue in $\mathbb{F}_{p(x_0)}^*$. Besides, (b) in Lemma 3 is satisfies for both cases. Since it is found that if x_0 satisfies Eq. (13), $(\frac{-1}{p(x_0)}) = -1$, $(\frac{2}{p(x_0)}) = -1$, and $(\frac{2}{p(x_0)})_3 \neq 1$ from Lemma 11, the tower is available. □

Theorem 7 *Under the same assumptions as in Theorem 6, the BLS curve $E/\mathbb{F}_{p(x_0)}$ can be determined as follows: For $m = 1$,*

$$E/\mathbb{F}_{p(x_0)} : \begin{cases} y^2 = x^3 + 1 & \text{if } x_0 \equiv 7, 31 \pmod{36} \\ y^2 = x^3 + 4 & \text{if } x_0 \equiv 16, 34 \pmod{36} \\ y^2 = x^3 - 2 & \text{if } x_0 \equiv 10, 28 \pmod{36} \end{cases}$$

For $m > 1$,

$$E/\mathbb{F}_{p(x_0)} : \begin{cases} y^2 = x^3 + 1 & \text{if } x_0 \equiv 7, 31 \pmod{72} \\ y^2 = x^3 + 4 & \text{if } x_0 \equiv 16 \pmod{72} \\ y^2 = x^3 - 2 & \text{if } x_0 \equiv 64 \pmod{72} \end{cases}$$

Proof of Theorem 7. The authors verify the cofactors of the possible group orders to determine the coefficient b of the BLS curve by using Lemma 4. From the definition, the curve with the group order $n(x_0) = p(x_0) + 1 - t(x_0)$ is the BLS curve.

If $x_0 \equiv 7, 31 \pmod{36}$ for $m = 1$; $x_0 \equiv 7, 31 \pmod{72}$ for $m > 1$, then $n(x_0)$ is divisible by 6 but the other group orders are not divisible by 6. According to (a) and (b) in Lemma 4, the coefficient b of the BLS curve is quadratic and cubic residue element b in $\mathbb{F}^*_{p(x_0)}$. Such the coefficient can be chosen as $b = 1$ since it is obvious that $(\frac{1}{p(x_0)}) = 1$ and $(\frac{1}{p(x_0)})_3 = 1$.

Similarly, if $x_0 \equiv 16, 34 \pmod{36}$ for $m = 1$; $x_0 \equiv 16 \pmod{72}$ for $m > 1$, $n(x_0)$ is always divisible by 3 but is not divisible by 2 and 9, however, the other group orders do not have such the properties of cofactors. Thus, according to (a) and (b) in Lemma 4, b is quadratic residue and cubic non-residue in $\mathbb{F}^*_{p(x_0)}$ and $4b$ is cubic non-residue in $\mathbb{F}^*_{p(x_0)}$. Then, the coefficient b of the BLS curve can be explicitly chosen as $b = 4$ since $(\frac{2}{p(x_0)})_3 \neq 1$ from Lemma 11.

Finally, if $x_0 \equiv 10, 28 \pmod{36}$ for $m = 1$; $x_0 \equiv 64 \pmod{72}$ for $m > 1$, 9 always divides $n(x_0)$ but 2 does not divide $n(x_0)$ and the other group orders are not divisible by 9. According to (a) and (c) in Lemma 4, it is found that b is quadratic residue and cubic non-residue in $\mathbb{F}^*_{p(x_0)}$, and $4b$ is cubic residue in $\mathbb{F}^*_{p(x_0)}$. Such the coefficient b of the BLS curve can be chosen as $b = 16$ since $(\frac{2}{p(x_0)})_3 \neq 1$ from Lemma 11. Since the quadratic and cubic residue properties of -2 and 16 are exactly the same, $b = -2$ can also be chosen for the BLS curve. □

Theorem 8 *Suppose that the tower of extension fields is constructed as in Theorem 6 and $E/\mathbb{F}_{p(x_0)}$ be the BLS curve determined as in Theorem 7. Then, the correct twist $E'/\mathbb{F}_{p(x_0)^{2^{m-1}}}$ of degree 6 of E can be determined as follows: For $m = 1$,*

$$E'/\mathbb{F}_{p(x_0)^{2^{m-1}}} : \begin{cases} y^2 = x^3 - 4 & \text{if } x_0 \equiv 7 \pmod{36}, \\ y^2 = x^3 - 1/4 & \text{if } x_0 \equiv 31 \pmod{36}, \\ y^2 = x^3 - 1 & \text{if } x_0 \equiv 10, 16, 28, 34 \pmod{36}. \end{cases}$$

For $m > 1$, letting $z = v^6 \in \mathbb{F}_{p(x_0)^{2^{m-1}}}$ with $v \in \mathbb{F}_{p(x_0)^{2^m \cdot 3}}$ such that $v^{2^{m-1} \cdot 3} = u + 1$,

$$E'/\mathbb{F}_{p(x_0)^{2^{m-1}}} : \begin{cases} y^2 = x^3 + 1/z & \text{if } x_0 \equiv 7 \pmod{72}, \\ y^2 = x^3 + 4z & \text{if } x_0 \equiv 16 \pmod{72}, \\ y^2 = x^3 + z & \text{if } x_0 \equiv 31 \pmod{72}, \\ y^2 = x^3 - 2/z & \text{if } x_0 \equiv 64 \pmod{72}. \end{cases}$$

Proof of Theorem 8. The authors verify the cofactors of the group order $n'(x_0)$ of the correct twist $E'/\mathbb{F}_{p(x_0)^{2^{m-1}}} : y^2 = x^3 + b'$ to determine b' by using Lemma 4. As described in Sect. 4.3, b' can be represented as $b' = b/\delta$ where b is the coefficient of the BLS curve and δ is quadratic and cubic non-residue in $\mathbb{F}^*_{p(x_0)^{2^{m-1}}}$. The authors also verify the cofactors of the group order $n''(x_0)$ of the twist $E''/\mathbb{F}_{p(x_0)^{2^{m-1}}} : y^2 = x^3 + b''$ of degree 2 of E', where $b'' = b'/\delta^3 = b \cdot \delta^4$. Note that $n'(x_0)$ is derived as in Theorem 4 and $n''(x_0) = 2p(x_0)^{2^{m-1}} + 2 - n'(x_0)$ from Eq. (12).

For $m = 1$, if $x_0 \equiv 7 \pmod{36}$, it is found that $n'(x_0)$ is not divisible by 2, 3, and 9. It is also found that $n''(x_0)$ is divisible by 3, but is not divisible by 2 and 9. Thus, according to Lemma 4, we obtain the following informations.

(a) b' is quadratic and cubic non-residue in $\mathbb{F}^*_{p(x_0)}$.
(b) b'' is quadratic residue and cubic non-residue in $\mathbb{F}^*_{p(x_0)}$.
(c) $4b''$ is cubic non-residue in $\mathbb{F}^*_{p(x_0)}$.

In this condition, the coefficient b of the BLS curve is determined as $b = 1$ and -4 is quadratic and cubic non-residue in $\mathbb{F}^*_{p(x_0)}$. Thus, the coefficient b' of the correct twist $E'/\mathbb{F}^*_{p(x_0)}$ can be denoted as either $b' = -1/4$ or -4. In addition, the coefficient b'' of the twist $E''/\mathbb{F}^*_{p(x_0)}$ of degree 2 of E' can also be denoted as either $b'' = 1/4^4$ or 4^4. From the above, it is found that the both candidates of b' and b'' satisfy (a) and (b), however, (c) is satisfied if $b'' = (-4)^4$, which leads to $b' = -4$. Thus,

the authors obtain $b' = -4$. In the same manner, the other cases of $x_0 \equiv 10, 16, 28, 31, 34 \pmod{36}$ can also be obtained.

For $m > 1$, if $x_0 \equiv 7 \pmod{72}$, $n'(x_0)$ is not divisible by 2, 3, and 9. Besides, if m is even, $n''(x_0)$ is divisible by 9, but is not divisible by 2, otherwise, $n''(x_0)$ is divisible by 3, but is not divisible by 2 and 9. Thus, the following informations are obtained from Lemma 4.

(a) b' is quadratic and cubic non-residue in $\mathbb{F}^*_{p(x_0)^{2^{m-1}}}$.
(b) b'' is quadratic residue and cubic non-residue in $\mathbb{F}^*_{p(x_0)^{2^{m-1}}}$.
(c) If m is even, $4b''$ is cubic residue in $\mathbb{F}^*_{p(x_0)^{2^{m-1}}}$, otherwise, $4b''$ is cubic non-residue in $\mathbb{F}^*_{p(x_0)^{2^{m-1}}}$.

Under this condition, the coefficient b of the BLS curve is determined as $b = 1$. Besides, $z = v^6$ is quadratic and cubic non-residue in $\mathbb{F}^*_{p(x_0)^{2^{m-1}}}$ since the norm of z, which is computed as follows, is quadratic and cubic non-residue in $\mathbb{F}^*_{p(x_0)}$.

$$\begin{aligned} N_{\mathbb{F}_{p(x_0)^{2^{m-1}}}/\mathbb{F}_{p(x_0)}}(z) &= z^{\sum_{i=0}^{2^{m-1}-1} p(x_0)^i} = z^{(p^{2^{m-2}}+1)\cdot\sum_{i=0}^{2^{m-2}-1} p(x_0)^i} \\ &= (-z^2)^{\sum_{i=0}^{2^{m-2}-1} p(x_0)^i} = (-z^{2^2})^{\sum_{i=0}^{2^{m-3}-1} p(x_0)^i} = \cdots \\ &= (-z^{2^{m-2}})^{p(x_0)+1} = (-v^{2^{m-1}\cdot 3})^{p(x_0)+1} = (-(u+1))^{p(x_0)+1} \\ &= -(u+1)\cdot(u-1) = 2. \end{aligned}$$

Thus, the coefficient b' of the correct twist $E'/\mathbb{F}^*_{p(x_0)^{2^{m-1}}}$ can be denoted as either $b' = 1/z$ or z. Besides, the coefficient b'' of the twist $E''/\mathbb{F}^*_{p(x_0)^{2^{m-1}}}$ of degree 2 of E' can also be denoted as either $b'' = 1/z^4$ or z^4. From the above, it is found that the both candidates of b' and b'' satisfy (a) and (b). As for (c), since the norm of $4/z^4$ and $4z^4$ are computed as $N_{\mathbb{F}_{p(x_0)^{2^{m-1}}}/\mathbb{F}_{p(x_0)}}(4/z^4) = 2^{2\cdot 2^{m-1}-4}$ and $N_{\mathbb{F}_{p(x_0)^{2^{m-1}}}/\mathbb{F}_{p(x_0)}}(4z^4) = 2^{2\cdot 2^{m-1}+4}$ in the same manner as the computation of the norm of z, respectively, it is found that (c) is satisfied if $b'' = 1/z^4$, which leads to $b' = 1/z$. Thus, the authors obtain $b' = 1/z$. The other cases of $x_0 \equiv 16, 31, 64 \pmod{72}$ can also be determined. □

6.2 The case of $k = 3^n$ for any $n > 0$

Let x_0 be an integer parameter for the BLS family of pairing-friendly elliptic curves with $k = 3^n$ where $n > 0$ is an arbitrary integer. The authors propose to restrict x_0 as follows:

$$x_0 \equiv 4 \pmod{6}. \tag{16}$$

Once finding x_0 under the above restriction, we have the specific BLS subfamily with the options (i) a fixed tower of extension fields with one of the best performing arithmetics is always available, and (ii) the BLS curve $E/\mathbb{F}_{p(x_0)}$ is immediately determined. In addition to this, the BLS subfamily might have the option (iii) the correct twist $E'/\mathbb{F}_{p(x_0)^{3^{n-1}}}$ is also immediately determined. If that is true, these constructions also enable one of the simplest twist isomorphisms. Table 2 shows the details of the field and curve options. The authors also provide Theorems 9 and 10 which shows the correctness that the proposed BLS subfamily has the options (i) and (ii), respectively. Though we need another theorem for the discussion, unfortunately, the authors do not complete proof, yet. Therefore, the authors show Conjecture 1 about the options (iii). Before theorems and conjecture, the authors present the knowledge of the quadratic and cubic residue properties in $\mathbb{F}^*_{p(x_0)}$ in the following Lemma 12.

Lemma 12 *For any $n > 0$, the following is true.*

$$\left(\frac{2}{p(x_0)}\right)_3 \begin{cases} = 1 & \text{if } x_0 \equiv 1, 4 \pmod{18}, \\ \neq 1 & \text{if } x_0 \equiv 7, 10, 13, 16 \pmod{18}. \end{cases}$$

Table 2: Field and curve options for the proposed BLS subfamily of curves with $k = 3^n$ for any $n > 0$, where $z = u^3 \in \mathbb{F}_{p(x_0)^{3^{n-1}}}$ with $u \in \mathbb{F}_{p(x_0)^{3^n}}$ defined in Eq. (17).

x_0 (mod 6)	Tower *(see Theorem 9)*	BLS curve $E/\mathbb{F}_{p(x_0)}$ *(see Theorem 10)*	Twist $E'/\mathbb{F}_{p(x_0)^{3^{n-1}}}$ *(see Conjecture 1)*
4	Eq. (17)	$y^2 = x^3 + 16$	$y^2 = x^3 + 16z^2$

Proof of Lemma 12. The authors classify x_0 into $x_0 \equiv 1 \pmod 6$ and $x_0 \equiv 4 \pmod 6$.

If $x_0 \equiv 1 \pmod 6$, $p(x_0)$ can be modified as follows:

$$\begin{aligned} p(x_0) &= \left(\frac{t(x_0)}{2}\right)^2 + 3\left(\frac{V(x_0)}{2}\right)^2 \\ &= \left(\frac{x_0+1}{2}\right)^2 + 3\left(\frac{x_0-1}{6}\cdot(2x_0^{3^{n-1}}+1)\right)^2. \end{aligned}$$

For $b(x_0) = (x_0-1)/6 \cdot (2x_0^{3^{n-1}}+1)$, 3 divides $b(x_0)$. According to Lemma 2, 2 is cubic residue in $\mathbb{F}^*_{p(x_0)}$ under this condition.

Similarly, if $x_0 \equiv 4 \pmod 6$, $p(x_0)$ can be modified as follows:

$$\begin{aligned} p(x_0) &= \left(\frac{t(x_0)+3V(x_0)}{4}\right)^2 + 3\left(\frac{t(x_0)-V(x_0)}{4}\right)^2 \\ &= \left(\frac{(x_0-1)\cdot x_0^{3^{n-1}}+x_0}{2}\right)^2 + 3\left(\frac{-(x_0-1)\cdot x_0^{3^{n-1}}+x_0+2}{6}\right)^2. \end{aligned}$$

For $b(x_0) = (-(x_0-1)\cdot x_0^{3^{n-1}}+x_0+2)/6$, 3 does not divide b_0. Thus, it is obtained that 2 is cubic non-residue in $\mathbb{F}^*_{p(x_0)}$ from Lemma 2. □

Then, the authors provide Theorems 9 and 10 associated with the construction of the tower of extension fields and BLS curve.

Theorem 9 *If x_0 satisfies Eq. (16), the following tower of extension fields is always available.*

$$\mathbb{F}_{p^{3^n}(x_0)} = \mathbb{F}_{p(x_0)}[u]/(u^{3^n}-2), \text{where } u^{3^n} = 2, u \in \mathbb{F}_{p(x_0)^{3^n}}. \tag{17}$$

Proof of Theorem 9. To adopt the tower of extension fields given in Eq. (17), the binomial $u^{3^n}-2$ has to be irreducible in $\mathbb{F}_{p(x_0)}[u]$, i.e., $3 \mid (p(x_0)-1)$ and 2 is cubic non-residue in $\mathbb{F}^*_{p(x_0)}$ from Lemma 3. The former requirement is satisfied for any x_0. If $x_0 \equiv 4 \pmod 6$, the latter requirement is also satisfied since $(\frac{2}{p(x_0)})_3 \neq 1$ under this condition as found in Lemma 12. □

Theorem 10 *Under the same assumptions as Theorem 9, the BLS curve with $k = 3^n$ is immediately determined as $E/\mathbb{F}_{p(x_0)} : y^2 = x^3 + 16$ for any $n > 0$.*

Proof of Theorem 10. The authors verify the cofactors of the possible group orders, which $n(x_0) = p(x_0) + 1 - t(x_0)$ is the group order of the BLS curve. If $x_0 \equiv 4 \pmod 6$, 9 always divides $n(x_0)$, however, 2 does not divide that. Note that the other group orders cannot be divisible by 9. According to (a) and (c) in Lemma 4, the coefficient b of the BLS curve is quadratic residue and cubic non-residue in $\mathbb{F}^*_{p(x_0)}$ and $4b$ is cubic residue in $\mathbb{F}^*_{p(x_0)}$. From Lemma 12, such the coefficient can be chosen as $b = 16$. □

Unfortunately, the authors can not determine the correct twist $E'/\mathbb{F}_{p(x_0)^{3^{n-1}}}$ by using Lemma 4 since the field $\mathbb{F}_{p^{3^{n-1}}}$ in which twist is defined always makes the coefficient b of the BLS curves $E/\mathbb{F}_{p(x_0)}$ being cubic residue in $\mathbb{F}^*_{p(x_0)^{3^{n-1}}}$. However, the authors make the following prediction from the experimental results of the determination of the twist equation with some small n.

Conjecture 1 *With x_0 satisfying Eq. (16), suppose that the tower of extension fields is constructed as in Theorem 9 and $E/\mathbb{F}_{p(x_0)}$ be the BLS curve determined as in Theorem 10. The correct twist of degree 3 of E can be determined as $E'/\mathbb{F}_{p(x_0)^{3^{n-1}}} : y^2 = x^3 + 16z^2$ where $z = u^3 \in \mathbb{F}_{p(x_0)^{3^{n-1}}}$ with $u \in \mathbb{F}_{p(x_0)^{3^n}}$ such that $u^{3^n} = 2$.*

Moreover, there is a possibility that Conjecture 1 can be proven by using another twist determination technique given by Yasuda et al. in [39], however, their technique is not so simpler than Costello et al.'s one [11] and require the knowledge of number theory. According to [39], the authors just find that if the following Conjecture 2 is true, Conjecture 1 is true.

Conjecture 2 *Let ϵ be a primitive cube root of the identity in $\mathbb{F}^*_{p(x_0)}$ which is represented as $\epsilon \equiv -(1 + t(x_0) \cdot V(x_0)^{-1})/2 \pmod{p(x_0)}$. If $x_0 \equiv 4 \pmod 6$, the following is always true.*

$$\epsilon \cdot 2^{\frac{p(x_0)-1}{3}} \equiv 1 \pmod{p(x_0)}.$$

The authors leave proof of the above conjectures as the future works.

7 Application

In this section, the authors apply our proposal and provide sample parameters x_0 for generating the proposed BLS subfamilies of curves with $k = 2^m \cdot 3$ and 3^n for $m, n \in \{2, 3\}$, i.e., $k = 9$, 12, 24, and 27. For $k = 24$, although Costello et al. provided many candidates of x_0 in [11], the authors reproduce the parameters based on the current security analysis [17]. According to the suggestions of [17], the authors adopt the curves with $k \in \{9, 12\}$ and $\{24, 27\}$ for the pairings at the 128 and 192-bit security levels, respectively. For the 128-bit security, the authors search x_0 which gives rise to $r(x_0)$ with $\log_2 r(x_0) \geq 256$ and $p(x_0)$ with $\log_2 p(x_0)^k \geq 5,472$ for $k = 9$ and $\log_2 p(x_0)^k \geq 5,376$ for $k = 12$. For the 192-bit security, the authors also search x_0 which gives rise to $r(x_0)$ with $\log_2 r(x_0) \geq 384$ and $p(x_0)$ with $\log_2 p(x_0)^k \geq 12,202$ for $k = 24$ and $\log_2 p(x_0)^k \geq 11,496$ for $k = 27$. The parameters x_0 having the low-Hamming weight are found for efficiency reasons of the pairings. According to [31], for $k = 3^n$ such that $2 \nmid k$, since it is also effective for fast Miller's algorithm to choose x_0 with the specific binary representations such that $x_0 = \sum_{i=0}^{\log_2 x_0 - 1} 2^i t_i$ where $t_i \in \{0, 1\}$ or $\{-1, 0\}$, the authors adopt that for searching x_0.

Tables 3 and 4 show the sample parameters x_0 for the pairings with the BLS family of curves with $k = 12, 9, 24$ and 27. The important fact is that all parameters result in the fixed field and curve constructions as in Tables 1 and 2 depending on the congruence classes of x_0. Although the twist equations for the case of $k = 3^n$ are just conjecture, the authors verify that all the parameters for the cases $k = 9$ and 27 can provide the correct twist in Table 2. This fixed field and curve constructions allow us to reduce the initial settings of the pairings. Moreover, if there are existing implementations of the pairings with some x_0 in a certain congruence class, we can reuse the implementation codes of the field and curve arithmetics for these of the pairings with new x_0 as long as x_0 is chosen from the same congruence class. Thus, the proposal contributes to not only finding new parameters but also smooth updating of x_0 corresponding to the progress of the security analyses. Note that the recent work [1] also carefully found x_0 even though they might not have the knowledge for finding nice x_0 except for $k = 24$.

8 Evaluation

The authors evaluate the parameters for the pairings on BLS curves with $k = \{9, 12, 24, 27\}$ given in Sect. 7 by an implementation. For efficient implementation, the authors adopt the state-of-the-art optimizations described below. For Miller's algorithm, the authors adopt efficient formulas for computing Miller's algorithm given by Costello et al. in [10]. The projective and affine formulas are adopted for the pairings at the 128 and 192-bit security level, respectively. For the case of the curves with $k = 9$ and 27, the revised version of Miller's algorithm by Nanjo et al. in [31] is adopted

Table 3: Sample parameters x_0 for the attractive BLS subfamilies of pairing-friendly elliptic curves with $k = 12$ and 24 for the pairings at the 128 and 192-bit security levels, respectively.

(a) $k = 12$, 128-bit security level.

No.	x_0 (mod 72)	x_0	HW(x_0)	$\log_2 p(x_0)$	$\log_2 p(x_0)^k$	$\log_2 r(x_0)$
1	7	$-2^{76} - 2^{28} - 2^{23} - 2^0$	4	455	5453	305
2	7	$+2^{75} - 2^{61} + 2^{31} - 2^0$	4	449	5381	300
3	7	$-2^{75} + 2^{52} + 2^{40} + 2^7 - 2^0$	5	449	5381	300
4	7	$-2^{75} + 2^{54} - 2^{36} + 2^4 - 2^0$	5	449	5381	300
5	7	$-2^{75} + 2^{70} + 2^{50} - 2^{44} - 2^0$	5	449	5378	300
6	16	$-2^{77} - 2^{59} + 2^9$ [1]	3	461	5525	309
7	16	$-2^{77} + 2^{50} + 2^{33}$ [1]	3	461	5525	308
8	16	$+2^{75} + 2^{65} - 2^{45} - 2^{10}$	4	449	5382	301
9	16	$-2^{75} - 2^{26} + 2^{21} - 2^{10}$	4	449	5381	301
10	16	$+2^{75} - 2^{60} + 2^{45} + 2^{24}$	4	449	5381	300
11	31	$+2^{76} - 2^{72} - 2^{12} - 2^0$	4	454	5447	304
12	31	$+2^{75} + 2^{40} - 2^{36} - 2^0$	4	449	5381	301
13	31	$+2^{75} - 2^{70} - 2^5 - 2^0$	4	449	5378	300
14	31	$-2^{75} - 2^{55} - 2^{42} + 2^{40} - 2^0$	5	449	5381	301
15	31	$-2^{75} - 2^{51} + 2^{40} - 2^{14} - 2^0$	5	449	5381	301
16	64	$+2^{75} + 2^{54} - 2^{27}$	3	449	5381	301
17	64	$+2^{76} - 2^{70} + 2^{66}$	3	455	5452	304
18	64	$+2^{75} + 2^{69} + 2^{64} + 2^{35}$	4	449	5383	301
19	64	$+2^{75} + 2^{55} - 2^{54} - 2^{27}$	4	449	5381	301
20	64	$-2^{75} + 2^{45} + 2^{43} - 2^6$	4	449	5381	300

(b) $k = 24$, 192-bit security level.

No.	x_0 (mod 72)	x_0	HW(x_0)	$\log_2 p(x_0)$	$\log_2 p(x_0)^k$	$\log_2 r(x_0)$
1	7	$-2^{51} - 2^{28} + 2^{11} - 2^0$ [11]	4	509	12202	409
2	7	$+2^{51} - 2^{32} - 2^{20} + 2^3 - 2^0$	5	509	12202	408
3	7	$-2^{51} - 2^{34} + 2^{24} + 2^{14} - 2^0$	5	509	12202	409
4	7	$-2^{51} + 2^{30} - 2^{24} - 2^{13} - 2^0$	5	509	12202	408
5	7	$-2^{51} - 2^{48} - 2^{21} - 2^{13} - 2^0$	5	511	12243	410
6	16	$+2^{51} + 2^{41} + 2^{34} + 2^{11}$	4	509	12203	409
7	16	$-2^{51} - 2^{48} + 2^{45} + 2^{39}$ [11]	4	510	12238	410
8	16	$+2^{51} + 2^{41} - 2^{36} - 2^5$	4	509	12203	409
9	16	$+2^{52} - 2^{49} + 2^{20} + 2^{10}$	4	517	12396	415
10	16	$+2^{52} - 2^{48} - 2^{46} + 2^{15}$	4	518	12414	416
11	31	$+2^{51} - 2^{15} - 2^8 - 2^0$ [11]	4	509	12202	408
12	31	$-2^{52} - 2^{28} + 2^{18} - 2^0$ [11]	4	519	12442	417
13	31	$-2^{51} + 2^{30} - 2^{19} + 2^{11} - 2^0$	5	509	12202	408
14	31	$+2^{51} + 2^{27} - 2^{12} + 2^3 - 2^0$	5	509	12202	409
15	31	$-2^{51} + 2^{38} - 2^{10} + 2^4 - 2^0$	5	509	12202	408
16	64	$-2^{51} + 2^{34} - 2^4$	3	509	12202	408
17	64	$-2^{52} - 2^{39} + 2^{16}$ [1]	3	519	12443	417
18	64	$-2^{51} + 2^{35} - 2^{34} - 2^4$	4	509	12202	408
19	64	$+2^{51} + 2^{27} + 2^{17} + 2^4$	4	509	12202	409
20	64	$+2^{51} - 2^{39} + 2^{33} - 2^{10}$	4	509	12202	408

Table 4: Sample parameters x_0 for the attractive BLS subfamily of pairing-friendly elliptic curves with $k = 9$ and 27 for the pairings at the 128 and 192-bit security levels, respectively.

(a) $k = 9$, 128-bit security level.

No.	x_0 (mod 6)	x_0	HW(x_0)	$\log_2 p(x_0)$	$\log_2 p(x_0)^k$	$\log_2 r(x_0)$
1	4	$-2^{77} - 2^{62} + 2^{20}$	3	615	5530	461
2	4	$-2^{77} - 2^{19} + 2^{9}$	3	615	5530	461
3	4	$-2^{77} - 2^{75} - 2^{32}$	3	617	5553	463
4	4	$+2^{77} + 2^{62} + 2^{35} + 2^{25}$	4	615	5530	461
5	4	$+2^{76} + 2^{74} + 2^{46} + 2^{22}$	4	609	5481	457
6	4	$-2^{76} - 2^{75} - 2^{70} - 2^{25} - 2^{1}$	5	612	5501	459
7	4	$-2^{76} - 2^{74} - 2^{65} - 2^{63} - 2^{19}$	5	609	5481	457
8	4	$-2^{76} - 2^{75} - 2^{57} - 2^{51} - 2^{18}$	5	612	5500	458
9	4	$-2^{76} - 2^{74} - 2^{54} - 2^{34} - 2^{28}$	5	609	5481	457
10	4	$+2^{76} + 2^{74} + 2^{42} + 2^{31} + 2^{27}$	5	609	5481	457
11	4	$+2^{76} + 2^{75} + 2^{74} + 2^{60} + 2^{19}$	5	613	5516	460
12	4	$+2^{76} + 2^{74} + 2^{65} + 2^{54} + 2^{11}$	5	609	5481	457

(b) $k = 27$, 192-bit security level.

No.	x_0 (mod 6)	x_0	HW(x_0)	$\log_2 p(x_0)$	$\log_2 p(x_0)^k$	$\log_2 r(x_0)$
1	4	$-2^{22} - 2^{12} + 2^{8} - 2^{6}$	4	439	11838	395
2	4	$+2^{23} - 2^{18} + 2^{14} - 2^{10}$	4	458	12354	412
3	4	$-2^{23} - 2^{17} + 2^{8} - 2^{1}$	4	459	12390	413
4	4	$+2^{22} + 2^{18} + 2^{13} + 2^{4} + 2^{1}$	5	441	11886	397
5	4	$-2^{22} - 2^{21} - 2^{19} - 2^{6} - 2^{1}$	5	453	12216	408
6	4	$-2^{23} - 2^{17} - 2^{11} - 2^{10} - 2^{8}$	5	459	12390	413
7	4	$-2^{23} - 2^{18} - 2^{8} - 2^{7} - 2^{3}$	5	460	12402	414
8	4	$+2^{22} + 2^{21} + 2^{19} + 2^{14} + 2^{9} + 2^{7}$	6	453	12218	408
9	4	$+2^{22} + 2^{20} + 2^{14} + 2^{9} + 2^{4} + 2^{2}$	6	445	12014	401
10	4	$+2^{22} + 2^{14} + 2^{11} + 2^{8} + 2^{4} + 2^{2}$	6	439	11841	395
11	4	$+2^{22} + 2^{17} + 2^{9} + 2^{7} + 2^{5} + 2^{4}$	6	440	11862	396
12	4	$-2^{22} - 2^{21} - 2^{15} - 2^{13} - 2^{11} - 2^{9}$	6	451	12159	406
13	4	$-2^{22} - 2^{11} - 2^{10} - 2^{9} - 2^{8} - 2^{6}$	6	439	11838	395
14	4	$-2^{22} - 2^{11} - 2^{10} - 2^{9} - 2^{6} - 2^{4}$	6	439	11838	395
15	4	$-2^{22} - 2^{21} - 2^{17} - 2^{12} - 2^{10} - 2^{8}$	6	451	12170	406

as appropriate according to x_0 of the loop parameter. For the final exponentiation algorithm, we adopt the state-of-the-art algorithm given by Hayashida et al. in [19]. For the curves with $k = 12$ and 24, we also use the compressed squaring in the cyclotomic subgroup in the full extension field given by Karabina in [23], which is available during computation of the hard part of the final exponentiation. Unfortunately, the curves with $k = 9$ and 27 cannot have such efficient squaring in the final exponentiation.

With the above optimizations, the authors implement the software for executing the pairings by C language. The authors use the big integer arithmetics are implemented by using `mp_limb_t` data type of the GMP library [16]. The software is compiled with GCC 8.3.0 with the option `-O2 -march=native` and is executed by 3.50GHz Intel(R) Core(TM) i7-7567U CPU running macOS Big Sur version 11.2.3. To evaluate the parameters, the average execution times of 100,000 trials of Miller's algorithm and final exponentiation are measured. Note that the measurement is performed by repeating the functions for 1,000 random inputs 100 times.

Tables 5 and 6 show the results of the average execution time of Miller's algorithm and final exponentiation. The results are analyzed as follows:

- Comparing the results between the same curves, the execution times of the pairings on the curves with small $\mathrm{HW}(x_0)$ are typically faster than that of the curves with large $\mathrm{HW}(x_0)$ since the performance of the pairing depends on the signed binary representation of x_0. Although some results do not follow this trend, the authors consider that it might come from the effects of cache and parallel processing. Rather than that, the execution times more strongly depend on the word size of $p(x_0)$. For example, for the curves with $k = 24$, the parameters of No. 18 could not result in the best performing pairing due to the word size of $p(x_0)$ even though that has the smallest Hamming weight. Besides, the authors could not find the difference between the congruence classes for the curves with $k = 12$ and 24, however, Costello et al. described that the difference of the twist isomorphisms between the congruence classes can affect the performance of Miller's algorithm in [11]. The authors consider that this effect might be small enough to ignore in this environment.
- Comparing the results between the same security levels, it is clear that the curves with $k = 12$ and $k = 24$ result in higher performance of the pairings at the 128 and 192-bit security levels comparing with the curves with $k = 9$ and 27, respectively. This cause of that the curves with $k = 9$ and 27 have low degree twists which can have disadvantage for computing Miller's algorithm. Besides, these curves cannot result in an efficient squaring in the cyclotomic multiplicative subgroup of the full extension field for computing the final exponentiation.

As a result, among the candidates shown in this paper, the authors suggest the curves with $k = 12$ with the parameters of No. 1, 6, 7, 11, and 17 for the pairing at the 128-bit security level. The authors also suggest the curves with $k = 24$ with the parameters of No. 16 for the pairing at the 192-bit security level.

9 Conclusion

In this paper, the authors extend the previous work [11] and provide the restrictions of the integer x_0 for generating the specific subfamilies of the BLS family of pairing-friendly elliptic curves with embedding degree $k = 2^m \cdot 3$ and 3^n for any integer $m, n > 0$. The proposed BLS subfamilies of curves with $k = 2^m \cdot 3$ result in efficient field arithmetics and immediately determination of the BLS curves $E/\mathbb{F}_{p(x_0)}$ and correct twist $E'/\mathbb{F}_{p(x_0)^{2^{m-1}}}$ of degree 6 of E. Similarly, the proposed BLS subfamily of curves with $k = 3^n$ also results in efficient field arithmetics and immediately determination of the BLS curves $E/\mathbb{F}_{p(x_0)}$, however, the correct twist $E'/\mathbb{F}_{p(x_0)^{3^{n-1}}}$ of degree 3 of E are not mathematically determined at this time. As a future work, the authors would like to overcome this remaining issues by providing proof of Conjectures 1 and 2.

Table 5: Average execution times for computing Miller's algorithm and final exponentiation for the pairings on BLS curves with $k = 12$ and 24 at the 128 and 192-bit security levels, respectively.

(a) $k = 12$, 128-bit security level.

No.	x_0 (mod 72)	x_0	HW(x_0)	Word size	Miller's alg. [ms]	Final exp. [ms]	Total [ms]
1	7	$-2^{76} - 2^{28} - 2^{23} - 2^0$	4	8	1.54	1.54	3.08
2	7	$+2^{75} - 2^{61} + 2^{31} - 2^0$	4	8	1.59	1.60	3.20
3	7	$-2^{75} + 2^{52} + 2^{40} + 2^7 - 2^0$	5	8	1.62	1.69	3.31
4	7	$-2^{75} + 2^{54} - 2^{36} + 2^4 - 2^0$	5	8	1.62	1.69	3.30
5	7	$-2^{75} + 2^{70} + 2^{50} - 2^{44} - 2^0$	5	8	1.57	1.64	3.21
6	16	$-2^{77} - 2^{59} + 2^9$ [1]	3	8	1.53	1.52	3.05
7	16	$-2^{77} + 2^{50} + 2^{33}$ [1]	3	8	1.54	1.52	3.06
8	16	$+2^{75} + 2^{65} - 2^{45} - 2^{10}$	4	8	1.59	1.66	3.25
9	16	$-2^{75} - 2^{26} + 2^{21} - 2^{10}$	4	8	1.59	1.66	3.25
10	16	$+2^{75} - 2^{60} + 2^{45} + 2^{24}$	4	8	1.59	1.66	3.25
11	31	$+2^{76} - 2^{72} - 2^{12} - 2^0$	4	8	1.51	1.52	3.03
12	31	$+2^{75} + 2^{40} - 2^{36} - 2^0$	4	8	1.59	1.61	3.20
13	31	$+2^{75} - 2^{70} - 2^5 - 2^0$	4	8	1.54	1.57	3.11
14	31	$-2^{75} - 2^{55} - 2^{42} + 2^{40} - 2^0$	5	8	1.61	1.70	3.30
15	31	$-2^{75} - 2^{51} + 2^{40} - 2^{14} - 2^0$	5	8	1.61	1.70	3.30
16	64	$+2^{75} + 2^{54} - 2^{27}$	3	8	1.59	1.58	3.17
17	64	$+2^{76} - 2^{70} + 2^{66}$	3	8	1.52	1.51	3.03
18	64	$+2^{75} + 2^{69} + 2^{64} + 2^{35}$	4	8	1.62	1.67	3.28
19	64	$+2^{75} + 2^{55} - 2^{54} - 2^{27}$	4	8	1.60	1.66	3.27
20	64	$-2^{75} + 2^{45} + 2^{43} - 2^6$	4	8	1.60	1.65	3.25

(b) $k = 24$, 192-bit security level.

No.	x_0 (mod 72)	x_0	HW(x_0)	Word size	Miller's alg. [ms]	Final exp. [ms]	Total [ms]
1	7	$-2^{51} - 2^{28} + 2^{11} - 2^0$ [11]	4	8	2.82	5.38	8.20
2	7	$+2^{51} - 2^{32} - 2^{20} + 2^3 - 2^0$	5	8	2.84	5.77	8.62
3	7	$-2^{51} - 2^{34} + 2^{24} + 2^{14} - 2^0$	5	8	2.84	5.77	8.60
4	7	$-2^{51} + 2^{30} - 2^{24} - 2^{13} - 2^0$	5	8	2.85	5.81	8.66
5	7	$-2^{51} - 2^{48} - 2^{21} - 2^{13} - 2^0$	5	8	2.84	5.77	8.61
6	16	$+2^{51} + 2^{41} + 2^{34} + 2^{11}$	4	8	2.79	5.49	8.28
7	16	$-2^{51} - 2^{48} + 2^{45} + 2^{39}$ [11]	4	8	2.81	5.54	8.35
8	16	$+2^{51} + 2^{41} - 2^{36} - 2^5$	4	8	2.78	5.48	8.27
9	16	$+2^{52} - 2^{49} + 2^{20} + 2^{10}$	4	9	3.31	6.49	9.80
10	16	$+2^{52} - 2^{48} - 2^{46} + 2^{15}$	4	9	3.32	6.52	9.84
11	31	$+2^{51} - 2^{15} - 2^8 - 2^0$ [11]	4	8	2.81	5.36	8.17
12	31	$-2^{52} - 2^{28} + 2^{18} - 2^0$ [11]	4	9	3.36	6.37	9.73
13	31	$-2^{51} + 2^{30} - 2^{19} + 2^{11} - 2^0$	5	8	2.83	5.77	8.60
14	31	$+2^{51} + 2^{27} - 2^{12} + 2^3 - 2^0$	5	8	2.84	5.77	8.61
15	31	$-2^{51} + 2^{38} - 2^{10} + 2^4 - 2^0$	5	8	2.85	5.81	8.66
16	64	$-2^{51} + 2^{34} - 2^4$	3	8	2.79	5.12	7.91
17	64	$-2^{52} - 2^{39} + 2^{16}$ [1]	3	9	3.30	6.03	9.34
18	64	$-2^{51} + 2^{35} - 2^{34} - 2^4$	4	8	2.82	5.55	8.37
19	64	$+2^{51} + 2^{27} + 2^{17} + 2^4$	4	8	2.81	5.55	8.36
20	64	$+2^{51} - 2^{39} + 2^{33} - 2^{10}$	4	8	2.82	5.57	8.39

Table 6: Average execution times for computing Miller's algorithm and final exponentiation for the pairings on BLS curves with $k = 9$ and 27 at the 128 and 192-bit security levels, respectively.

(a) $k = 9$, 128-bit security level.

No.	x_0 (mod 6)	x_0	HW(x_0)	Word size	Miller's alg. [ms]	Final exp. [ms]	Total [ms]
1	4	$-2^{77} - 2^{62} + 2^{20}$	3	10	2.38	3.41	5.79
2	4	$-2^{77} - 2^{19} + 2^{9}$	3	10	2.37	3.39	5.76
3	4	$-2^{77} - 2^{75} - 2^{32}$	3	10	2.33	3.38	5.71
4	4	$+2^{77} + 2^{62} + 2^{35} + 2^{25}$	4	10	2.35	3.36	5.71
5	4	$+2^{76} + 2^{74} + 2^{46} + 2^{22}$	4	10	2.34	3.34	5.69
6	4	$-2^{76} - 2^{75} - 2^{70} - 2^{25} - 2^{1}$	5	10	2.38	3.46	5.84
7	4	$-2^{76} - 2^{74} - 2^{65} - 2^{63} - 2^{19}$	5	10	2.41	3.51	5.92
8	4	$-2^{76} - 2^{75} - 2^{57} - 2^{51} - 2^{18}$	5	10	2.38	3.48	5.86
9	4	$-2^{76} - 2^{74} - 2^{54} - 2^{34} - 2^{28}$	5	10	2.39	3.49	5.89
10	4	$+2^{76} + 2^{74} + 2^{42} + 2^{31} + 2^{27}$	5	10	2.37	3.40	5.77
11	4	$+2^{76} + 2^{75} + 2^{74} + 2^{60} + 2^{19}$	5	10	2.34	3.35	5.69
12	4	$+2^{76} + 2^{74} + 2^{65} + 2^{54} + 2^{11}$	5	10	2.37	3.41	5.77

(b) $k = 27$, 192-bit security level.

No.	x_0 (mod 6)	x_0	HW(x_0)	Word size	Miller's alg. [ms]	Final exp. [ms]	Total [ms]
1	4	$-2^{22} - 2^{12} + 2^{8} - 2^{6}$	4	7	2.41	13.1	15.5
2	4	$+2^{23} - 2^{18} + 2^{14} - 2^{10}$	4	8	2.80	15.3	18.1
3	4	$-2^{23} - 2^{17} + 2^{8} - 2^{1}$	4	8	2.84	15.3	18.2
4	4	$+2^{22} + 2^{18} + 2^{13} + 2^{4} + 2^{1}$	5	7	2.31	12.7	15.1
5	4	$-2^{22} - 2^{21} - 2^{19} - 2^{6} - 2^{1}$	5	8	2.70	15.6	18.3
6	4	$-2^{23} - 2^{17} - 2^{11} - 2^{10} - 2^{8}$	5	8	2.80	16.1	18.9
7	4	$-2^{23} - 2^{18} - 2^{8} - 2^{7} - 2^{3}$	5	8	2.78	16.0	18.8
8	4	$+2^{22} + 2^{21} + 2^{19} + 2^{14} + 2^{9} + 2^{7}$	6	8	2.72	15.3	18.0
9	4	$+2^{22} + 2^{20} + 2^{14} + 2^{9} + 2^{4} + 2^{2}$	6	7	2.36	13.3	15.7
10	4	$+2^{22} + 2^{14} + 2^{11} + 2^{8} + 2^{4} + 2^{2}$	6	7	2.35	13.2	15.6
11	4	$+2^{22} + 2^{17} + 2^{9} + 2^{7} + 2^{5} + 2^{4}$	6	7	2.35	13.3	15.6
12	4	$-2^{22} - 2^{21} - 2^{15} - 2^{13} - 2^{11} - 2^{9}$	6	8	2.82	16.6	19.4
13	4	$-2^{22} - 2^{11} - 2^{10} - 2^{9} - 2^{8} - 2^{6}$	6	7	2.44	14.3	16.7
14	4	$-2^{22} - 2^{11} - 2^{10} - 2^{9} - 2^{6} - 2^{4}$	6	7	2.43	14.2	16.6
15	4	$-2^{22} - 2^{21} - 2^{17} - 2^{12} - 2^{10} - 2^{8}$	6	8	2.81	16.6	19.4

Acknowledgment

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

References

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

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

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

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

[5] Naomi Benger and Michael Scott. Constructing tower extensions of finite fields for implementation of pairing-based cryptography. In *International workshop on the arithmetic of finite fields*, pages 180–195. Springer, 2010.

[6] Jean-Luc Beuchat, Jorge E González-Díaz, Shigeo Mitsunari, Eiji Okamoto, Francisco Rodríguez-Henríquez, and Tadanori Teruya. High-speed software implementation of the optimal ate pairing over barreto–naehrig curves. In *International conference on pairing-based cryptography*, pages 21–39. Springer, 2010.

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

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

[9] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the weil pairing. *Journal of cryptology*, 17(4):297–319, 2004.

[10] Craig Costello, Tanja Lange, and Michael Naehrig. Faster pairing computations on curves with high-degree twists. In *International workshop on public key cryptography*, pages 224–242. Springer, 2010.

[11] Craig Costello, Kristin Lauter, and Michael Naehrig. Attractive subfamilies of bls curves for implementing high-security pairings. In *International conference on cryptology in India*, pages 320–342. Springer, 2011.

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

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

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

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

[16] Torbjörn Granlund and the GMP development team. Gnu mp: the gnu multiple precision arithmetic library, 6.1.2, 2015. `https://gmplib.org`.

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

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

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

[20] Florian Hess. Pairing lattices. In *International conference on pairing-based cryptography*, pages 18–38. Springer, 2008.

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

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

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

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

[25] Neal Koblitz. *A course in number theory and cryptography*, volume 114. Springer Science & Business Media, 1994.

[26] Franz Lemmermeyer. *Reciprocity laws: from Euler to Eisenstein*. Springer Science & Business Media, 2013.

[27] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20. Cambridge university press, 1997.

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

[29] Michael Naehrig. Constructive and computational aspects of cryptographic pairings. 2009.

[30] Yuki Nanjo, Masaaki Shirase, Takuya Kusaka, and Yasuyuki Nogami. Specific congruence classes of integer parameters for generating bls curves for fast pairings. In *International symposium on computing and networking workshop*, pages 348–354, 2020.

[31] Yuki Nanjo, Masaaki Shirase, Takuya Kusaka, and Yasuyuki Nogami. A technique for fast miller's algorithm of ate pairings on elliptic curves with embedding degrees of multiple of three. In *International technical conference on circuits/systems, computers and communications*, pages 283–287. IEEE, 2020.

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

[33] Geovandro CCF Pereira, Marcos A Simplício Jr, Michael Naehrig, and Paulo SLM Barreto. A family of implementation-friendly bn elliptic curves. *Journal of systems and software*, 84(8):1319–1326, 2011.

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

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

[36] Joseph H Silverman. *The arithmetic of elliptic curves (2nd edition)*, volume 106. Springer Science & Business Media, 2009.

[37] Tadanori Teruya, Kazutaka Saito, Naoki Kanayama, Yuto Kawahara, Tetsutaro Kobayashi, and Eiji Okamoto. Constructing symmetric pairings over supersingular elliptic curves with embedding degree three. In *International conference on pairing-based cryptography*, pages 97–112. Springer, 2013.

[38] Frederik Vercauteren. Optimal pairings. *IEEE transactions on information theory*, 56(1):455–461, 2010.

[39] Takanori Yasuda, Tsuyoshi Takagi, and Kouichi Sakurai. Constructing pairing-friendly elliptic curves using global number fields. In *International symposium on computing and networking*, pages 477–483. IEEE, 2015.