Efficient Pairings Final Exponentiation Using Cyclotomic Cubing for Odd Embedding Degrees Curves

Walid Haddaji[1,3*], Loubna Ghammam[2], Nadia El Mrabet[3], Leila Ben Abdelghani[4]

[1,3*]Science and technology for defense lab LR19DN01, Center for military research, military academy, Tunis, Tunisia.

[2]ITK Engineering GmbH, Im Speyerer Tal 6 Rülzheim76761, Germany.

[3]Laboratory of Secure System and Architecture (SSA), Ecole des Mines de Saint Etienne, 880 Rte de Mimet, Campus Georges Charpak Provence, 13120, Gardanne, France.

[4]Laboratory of Analysis, Probability and Fractals, Faculty of Sciences, Environment Avenue, Omrane, 5000, Monastir, Tunisia.

*Corresponding author(s). E-mail(s): haddajiwalid95@gmail.com;
Contributing authors: loubna.ghammam@itk-engineering.de; nadia.elmrabet@emse.fr; leila.benabdelghani@fsm.rnu.tn;

Abstract

In pairings-based cryptographic applications, final exponentiation with a large fixed exponent ensures distinct outputs for the Tate pairing and its derivatives. Despite notable advancements in optimizing elliptic curves with even embedding degrees, improvements for those with odd embedding degrees, particularly those divisible by **3**, remain underexplored. This paper introduces three methods for applying cyclotomic cubing in final exponentiation and enhancing computational efficiency. The first allows for the execution of one cyclotomic cubing based on the final exponentiation structure. The second leverages some existing seeds structure to enable the use of cyclotomic cubing and extends this strategy to generate new seeds. The third allows generating sparse ternary representation seeds to apply cyclotomic cubing as an alternative to squaring. These optimizations improve performance by up to **19.3%** when computing the final exponentiation for the optimal Ate pairing on $\boldsymbol{BLS}\mathbf{15}$ and $\boldsymbol{BLS}\mathbf{27}$, the target elliptic curves of this study.

Keywords: Elliptic curves, pairings, final exponentiation, cyclotomic cubing, arithmetic.

1 Introduction

Pairings over elliptic curves are crucial for various cryptographic applications, e.g., identity-based encryption [7], short signatures [8], and tri-partite Diffie-Hellman [19]. Significant efforts [5, 6, 20] have been dedicated to developing various families of elliptic curves tailored for pairing applications. Additionally, Additionally, researchers have focused on optimizing the Miller loop [18, 28] and the final exponentiation [16, 21, 26, 27], as these steps account for the majority of the computational complexity in pairings. In [2–4], Barbulescu et al. introduced new parameters that resist an attack on the discrete logarithm problem (DLP) , which was proposed by Kim et al. in [23]. They also demonstrated that, at the 128-security level, the Barreto-Lynn-Scott family of elliptic curves with an embedding degree $k = 12$ ($BLS12$) and the Kachisa-Schaefer-Scott family of elliptic curves with $k = 16$ ($KSS16$) can offer a more efficient pairing than the Barreto-Naehrig family (BN). Barbulescu et al. revealed that elliptic curve families with $k = 9, 15, 27$ might rival $BLS12$, $KSS16$, and (BN).

The final exponentiation consists of computing

$$\frac{p^k-1}{r} = \frac{p^k-1}{\Phi_k(p)} \times \frac{\Phi_k(p)}{r}, \text{ where}$$

ϕ_k is the k-th cyclotomic polynomial, the easy part consists of $\frac{p^k-1}{r}$, which is simple to compute, and the hard part is $\frac{\Phi_k(p)}{r}$, which demands effort. The hard part is carried out within a cyclotomic subgroup. The central operation here is an exponentiation by a fixed integer known as the seed. This uses the square-and-multiply (**SM**) method: it squares for each bit of the seed and multiplies when the bit is 1. If possible, cyclotomic squaring should replace regular squaring to improve efficiency. It plays a crucial role in speeding up the hard part of pairings over curves with even embedding degrees, such as *BLS12*, *KSS16*, and *BLS24*. However, this operation is not available for curves with odd embedding degrees, such as $BLS27$. For these curves, **SM** uses standard squaring and multiplication. Granger and Scott [16] found that techniques for cyclotomic squaring could be adapted for curves with odd embedding degrees divisible by 3, leading to *cyclotomic cubing*.Nanjo et al. [25] showed that cyclotomic cubing is 30% faster than regular cubing in $\mathbb{F}_{p^{15}}$ and more efficient than squaring plus multiplication in $\mathbb{F}_{p^{15}}$ and $\mathbb{F}_{p^{27}}$. The structure of the hard part in *BLS* curves, along with certain seed forms, enables partial cyclotomic cubing. This enhances optimization while maintaining the efficiency of binary representation. In [25], the authors found that cyclotomic cubing over $\mathbb{F}_{p^{15}}$ is not fast enough to replace **SM** with **CM**. Instead, it may be beneficial for seeds with sparse ternary representations. This led us to explore it as an alternative to **SM**, aiming to leverage cyclotomic cubing's efficiency in pairings over $BLS15$ and $BLS15$.

Our contributions

This paper explores the use of the cyclotomic cubing in computing the final exponentiation of the optimal Ate. We propose the following methods:

1. **Direct Application of Cyclotomic Cubing:** This method directly applies cyclotomic cubing by leveraging the hard part's structure in the final exponentiation over *BLS* curves.
2. **Two Consecutive Active Bits (TCAB):** An active bit refers to a **1** in the binary representation of the seed. This method involves searching for a specific pattern of two consecutive active bits in the seed in order to perform cyclotomic cubing.
3. **Exponentiation using Sparse Ternary Representation:** This method allows to generate new sparse ternary seeds to apply cyclotomic cubing via the **CM** (cubing-and-multiply) method.

Note that this proposal is applicable to any elliptic curve with an odd embedding degree divisible by 3. However, in this paper we focus on the $BLS15$ and $BLS27$ elliptic curves, inspired by improvements in [11]. We place particular emphasis on $BLS27$ due to its suitability for computing the Miller loop and pairing products.

Organization of the paper

This paper is organized as follows: Section 2 establishes the mathematical background, focusing on arithmetic operations in finite fields with extension degrees that are odd divisible by 3. We also recall pairings over $BLS15$ and $BLS27$ elliptic curves. In Section 3, we present our techniques for applying cyclotomic cubing to compute the final exponentiation of the optimal Ate pairing over $BLS15$ and $BLS27$. In Section 4, we evaluate the pairing costs using new seeds presented in ternary representation. Finally, we summarize our findings and suggest future research directions.

Notations

Let $i \in \mathbb{N}^*$. For the remainder of this paper, we adopt the following notations:

- p a big prime number,
- E represents an elliptic curve defined over $\mathbb{F}_p$,
- $\mathbf{M_i}$ indicates the cost of multiplication in $\mathbb{F}_{p^i}$,
- $\mathbf{S_i}$ represents the cost of squaring in $\mathbb{F}_{p^i}$,
- $\mathbf{F_i}$ stands for a Frobenius operation in $\mathbb{F}_{p^i}$,
- $\mathbf{I_i}$ signifies the cost of inversion in $\mathbb{F}_{p^i}$,
- $\mathbf{C_{c_i}}$ represents the cost of cyclotomic cubing in $\mathbb{F}_{p^i}$,
- $\mathbf{I_{c_k}}$ signifies the cost of cyclotomic inversion in $\mathbb{F}_{p^i}$,
- For $u \in \mathbb{Z}$, $\mathbf{E_u}$ denotes the cost of exponentiation by u,

- **Sec-level** stands for the security level.

In this paper, we assume that $\mathbf{M_1} \approx \mathbf{S_1}$.

2 Background

Let k be a positive integer such that $3 \mid k$. This section presents the fundamental aspects of arithmetic over $\mathbb{F}_{p^k}$, focusing on cases where k is odd and divisible by 3. Additionally, it recalls pairings over elliptic curves with an embedding degree k. For more detailed information, the reader is referred to [1, 4, 11, 22, 25].

2.1 Costs of arithmetic operations over $\mathbb{F}_{p^k}$

We assume that $3 \mid k$, therefore $\mathbb{F}_{p^k}$ is represented as follows:

$$\mathbb{F}_{p^k} = \mathbb{F}_{p^{\frac{k}{3}}}[x]/(x^3 - \xi),$$

where ξ is a cubic non-residue in $\mathbb{F}_{p^{\frac{k}{3}}}$.
The costs of $\mathbf{M_k}$, $\mathbf{S_k}$, $\mathbf{F_k}$, and $\mathbf{I_k}$ are well studied in the literature [1]. Therefore, we will only recall them in Table 1. However, we will detail in this section the costs of cyclotomic inversion and cyclotomic cubing. Let us just recall the cyclotomic subgroup.
Definition 1. *The cyclotomic subgroup of $\mathbb{F}_{p^k}$ is given in [13] by:*

$$G_{\Phi_k(p)} = \{\alpha \in \mathbb{F}^*_{p^k}; \alpha^{\Phi_k(p)} = 1\}, \tag{1}$$

where ϕ_k is the $k-th$ cyclotomic polynomial. The order of $G_{\Phi_k(p)}$ is $\Phi_k(p)$.

Since this paper focuses on the fields $\mathbb{F}_{p^{15}}$ and $\mathbb{F}_{p^{27}}$, we recall that Fouotsa et al. demonstrated in [11] that the costs of cyclotomic inversion over $\mathbb{F}_{p^{15}}$ and $\mathbb{F}_{p^{27}}$ are given as follows:

$$\mathbf{I_{c_{15}}} = \mathbf{3M_5} + \mathbf{3S_5} \text{ and } \mathbf{I_{c_{27}}} = \mathbf{3M_9} + \mathbf{3S_9}.$$

The detailed method for performing this operation is provided in [25]. According to Nanjo et al., the cost of **cyclotomic cubing** over $\mathbb{F}_{p^k}$ is given by:

$$\mathbf{C_{c_k}} = 5\mathbf{M_{\frac{k}{3}}} + 4\mathbf{S_{\frac{k}{3}}} + 3\mathbf{m_{\frac{k}{3},\xi}} + 9\mathbf{A_{\frac{k}{3}}} + \mathbf{a_{\frac{k}{3},1}} + 4\mathbf{h_{\frac{k}{3}}},$$

where $\mathbf{m_{\frac{k}{3},\xi}}$, $\mathbf{a_{\frac{k}{3},1}}$, $\mathbf{h_{\frac{k}{3}}}$, $\mathbf{A'_{\frac{k}{3}}}$, and $\mathbf{A_{\frac{k}{3}}}$ represent the costs of a multiplication by ξ, an addition by 1, a shift operation, a multiplication by 2, and an addition in $\mathbb{F}_{p^{\frac{k}{3}}}$, respectively.
The additions and shift operations are often neglected, leading to the following cost:

$$\mathbf{C_{c_k}} = 5\mathbf{M_{\frac{k}{3}}} + 4\mathbf{S_{\frac{k}{3}}} + 3\mathbf{m_{\frac{k}{3},\xi}}.$$

Similar to the costs of multiplication and squaring in $\mathbb{F}_{p^k}$, the cost of cyclotomic cubing depends on the multiplication by ξ. We can choose to either include or neglect this multiplication. If included, the costs of cyclotomic cubing in $\mathbb{F}_{p^{15}}$ and $\mathbb{F}_{p^{27}}$ are as follows:

$$\mathbf{C_{c_{15}}} = \mathbf{5M_5} + \mathbf{4S_5} + \mathbf{3m_{5,\xi}} \quad \text{and} \quad \mathbf{C_{c_{27}}} = \mathbf{5M_9} + \mathbf{4S_9} + \mathbf{3m_{9,\xi}}.$$

If neglected, the costs are as follows:

$$\mathbf{C_{c_{15}}} = \mathbf{5M_5} + \mathbf{4S_5} \quad \text{and} \quad \mathbf{C_{c_{27}}} = \mathbf{5M_9} + \mathbf{4S_9}.$$

We will disregard multiplications by ξ throughout this paper for the following reasons:

- Several works, including those of Aranha et al. [1], overlook multiplications by ξ when assessing multiplication and squaring costs in $\mathbb{F}_{p^k}$. They use costs derived from previous real implementations.
- In the context of computational efficiency, cyclotomic cubing in $\mathbb{F}_{p^k}$ is comparable to both squaring and multiplication. Therefore, we propose that the most balanced approach is to impose the same constraints on all three operations, particularly with respect to multiplication by ξ.
- In practical applications, there exists $\xi \in \mathbb{F}_{p^{\frac{k}{3}}}$ such that multiplication by ξ incurs a low cost.

In the following Table 1 we provide a summary of operations in $\mathbb{F}_{p^3}$, $\mathbb{F}_{p^9}$, $\mathbb{F}_{p^{15}}$ and $\mathbb{F}_{p^{27}}$.

Fields	Operations	Costs
$\mathbb{F}_{p^3}$	Multiplication $\mathbf{M_3}$	$6\mathbf{M_1}$
	Squaring $\mathbf{S_3}$	$5\mathbf{S_1}$
	Inversion $\mathbf{I_3}$	$37\mathbf{M_1}$
	Fronenius $\mathbf{F_3}$	$2\mathbf{M_1}$
$\mathbb{F}_{p^5}$	Multiplication $\mathbf{M_5}$	$13\mathbf{M_1}$
	Squaring $\mathbf{S_5}$	$13\mathbf{S_1}$
	Inversion $\mathbf{I_5}$	$73\mathbf{M_1}$
	Fronenius $\mathbf{F_5}$	$4\mathbf{M_1}$
$\mathbb{F}_{p^9}$	Multiplication $\mathbf{M_9}$	$36\mathbf{M_1}$
	Squaring $\mathbf{S_9}$	$27\mathbf{M_1}$
	Inversion $\mathbf{I_9}$	$106\mathbf{M_1}$
	Fronenius $\mathbf{F_9}$	$8\mathbf{M_1}$
	Cyclotomic inversion $\mathbf{I_{c_9}}$	$3 \times 6\mathbf{M_1} + 3 \times (2\mathbf{M_1} + 3\mathbf{S_1}) \approx 33\mathbf{M_1}$
	Cyclotomic cubing $\mathbf{C_{c_9}}$	$5 \times 6\mathbf{M_1} + 4 \times 5\mathbf{S_1} \approx 50\mathbf{M_1}$
$\mathbb{F}_{p^{15}}$	Multiplication $\mathbf{M_{15}}$	$78\mathbf{M_1}$
	Squaring $\mathbf{S_{15}}$	$65\mathbf{M_1}$
	Inversion $\mathbf{I_{15}}$	$229\mathbf{M_1}$
	Fronenius $\mathbf{F_{15}}$	$14\mathbf{M_1}$
	Cyclotomic inversion $\mathbf{I_{c_{15}}}$	$3 \times 13\mathbf{M_1} + 3 \times 13\mathbf{S_1} \approx 78\mathbf{M_1}$
	Cyclotomic cubing $\mathbf{C_{c_{15}}}$	$5 \times 13\mathbf{M_1} + 4 \times 13\mathbf{S_1} \approx 117\mathbf{M_1}$
$\mathbb{F}_{p^{27}}$	Multiplication $\mathbf{M_{27}}$	$216\mathbf{M_1}$
	Squaring $\mathbf{S_{27}}$	$153\mathbf{M_1}$
	Inversion $\mathbf{I_{27}}$	$536\mathbf{M_1}$
	Fronenius $\mathbf{F_{27}}$	$26\mathbf{M_1}$
	Cyclotomic inversion $\mathbf{I_{c_{27}}}$	$3 \times 36\mathbf{M_1} + 3 \times (18\mathbf{M_1} + 9\mathbf{S_1}) \approx 189\mathbf{M_1}$
	Cyclotomic cubing $\mathbf{C_{c_{27}}}$	$5 \times 36\mathbf{M_1} + 4 \times (18\mathbf{M_1} + 9\mathbf{S_1}) \approx 288\mathbf{M_1}$

Table 1: The costs of all operations in extension fields $\mathbb{F}_{p^i}$, for $i \in \{3, 5, 9, 15, 27\}$.

2.2 Pairings

Let E be an elliptic curve defined over $\mathbb{F}_p$, r be a large prime factor of $\#E(\mathbb{F}_p)$ and k be the smallest positive integer such that $r \mid (p^k - 1)$. Let $P \in E(\mathbb{F}_p)[r]$ be of order r, and let $f_{r,P}$ be the rational function with the following divisor (for details about divisors, see [22]):

$$Div(f_{r,P}) = r(P) - r(P_\infty).$$

Let $Q \in E(\mathbb{F}_{p^k})[r]$ of order r, and let μ_r denote the group of r-th roots of unity in $\mathbb{F}_{p^k}^*$. The optimal Ate pairing is defined by:

$$\begin{aligned} e_o : \mathbb{G}_2 \times \mathbb{G}_1 &\longrightarrow \mathbb{G}_3 \\ (Q, P) &\longmapsto f_{t-1,Q}(P)^{\frac{p^k-1}{r}} \end{aligned}$$

and it can be computed in $\frac{\log_2(r)}{\varphi(k)} + \epsilon(k)$ basic Miller iterations, where

- $\epsilon(k) \leq \log_2(k)$.
- π_p is the Frobenius map that is defined by:

$$\begin{aligned} \pi_p : E(\overline{\mathbb{F}_p}) &\to E(\overline{\mathbb{F}_p}) \\ (x, y) &\longmapsto \pi_p(x, y) = (x^p, y^p) \end{aligned}$$

- $\mathbb{G}_1 = E(\overline{\mathbb{F}_p})[r] \cap Ker(\pi_p - 1) = E(\mathbb{F}_p)[r]$.
- $\mathbb{G}_2 = E(\overline{\mathbb{F}_p})[r] \cap Ker(\pi_p - p)$.
- $\mathbb{G}_3 = \{\mu \in \mathbb{F}_{p^k} \mid \mu^r = 1\}$.
- t is the trace of π_p.

The computation of pairing consists of two stages. The first stage involves calculating the function $f_{t-1,Q}(P)$ using the Miller algorithm [24]. The second stage, known as the final exponentiation, involves raising $f_{t-1,Q}(P)$ to the power of $\frac{p^k-1}{r}$. It consists of two phases: the easy part and the hard part. The easy part is straightforward to compute, whereas the hard part is more complex and demanding. Several methods have been proposed for performing this calculation [11, 12, 14, 15, 26]. In particular, Zhang et al. [29] used a recursion relation to expand $\frac{\phi_k(p)}{r}$ in base p and compute the hard part of the final exponentiation for $k = 27$. Hayashida et al. generalized the method of Zhang et al. to arbitrary embedding degrees using a homogeneous cyclotomic polynomial constructed from a cyclotomic polynomial. In the next section, we will focus on calculating the optimal Ate pairing over elliptic curves with embedding degrees 15 and 27.

2.3 Optimal Ate pairing over $BLS15$ and $BLS27$

A BLS curve is a pairing-friendly elliptic curve over a finite field $\mathbb{F}_p$ defined by the equation $y^2 = x^3 + b$, where $b \in \mathbb{F}_p$ is a nonzero constant.

BLS15

The $BLS15$ family consists of parametrized elliptic curves with an embedding degree of 15, defined in [10] by the following parameters:

$$\begin{cases} p = \frac{u^{12}-2u^{11}+u^{10}+u^7-2u^6+u^5+u^2+u+1}{3}, \\ r = u^8 - u^7 + u^5 - u^4 + u^3 - u + 1, \\ t = u + 1, \end{cases}$$

where the seed u is chosen so that p and r are both prime integers, ensuring a secure and efficient $BLS15$ elliptic curve for pairing. The optimal Ate pairing over $BLS15$ is given by:

$$\begin{aligned} e_o \colon \mathbb{G}_2 \times \mathbb{G}_1 &\longrightarrow \mathbb{G}_3 \\ (Q, P) &\longmapsto f_{u,Q}(P)^{\frac{p^{15}-1}{r}}, \end{aligned}$$

where the elevation of Miller's result to the power $(p^5 - 1)(p^2 + p + 1)$ is called the easy part of the final exponentiation. However, the result of the easy part power $\frac{\Phi_{15}(p)}{r}$ is called the hard part of the final exponentiation. In [17], for efficiency reasons, they proposed to use a multiple of the hard part of final exponentiation instead of considering the final exponentiation. Note that, that an exponent of pairing is a pairing. In this context, they considered $3.\frac{\Phi_{15}(p)}{r}$, where it is developed as follows:

$$3.\frac{\Phi_{15}(p)}{r} = (u-1)^2(u^2+u+1) + \sum_{i=0}^{7} \lambda_i(u)p^i(u) + 3,$$

where $\lambda_7 = 1$, $\lambda_6 = u\lambda_7 - 1$, $\lambda_5 = u\lambda_6$, $\lambda_4 = u\lambda_5 + 1$, $\lambda_3 = u\lambda_4 - 1$, $\lambda_2 = u\lambda_3 + 1$, $\lambda_1 = u\lambda_2$, and $\lambda_0 = u\lambda_1 - 1$.

BLS27

The $BLS27$ family consists of parametrized elliptic curves with an embedding degree of 27, as described in [29] by the following parameters:

$$\begin{cases} r(u) = \frac{u^{18}+u^9+1}{3}, \\ p(u) = (u-1)^2 r(u) + u, \\ t(u) = u + 1. \end{cases}$$

The seed u is selected to guarantee that p and r are prime integers, providing a secure and efficient $BLS27$ elliptic curve for pairing. The optimal Ate pairing over $BLS15$ is given by:

$$\begin{aligned} e_o \colon \mathbb{G}_2 \times \mathbb{G}_1 &\longrightarrow \mathbb{G}_3 \\ (Q, P) &\longmapsto f_{u,Q}(P)^{\frac{p^{27}-1}{r}}, \end{aligned}$$

Raising Miller's result to the power $(p^9 - 1)$ is known as the easy part of the final exponentiation. However, the elevation the easy part by $\frac{\Phi_{27}(p)}{r}$ defines the hard part of the final exponentiation and it is developed as follows:

$$(u-1)^2(u^2+pu+p^2)(u^6+p^3u^3+p^6)(u^9+p^9+1) + 3.$$

3 Applying cyclotomic cubing in final exponentiation computation

This section demonstrates the applicability of cyclotomic cubing for final exponentiation in two cases: a seed-independent case and a seed-dependent binary representation case.

3.1 Direct application

Description

Inspired by the work of Nanjo et al. [25], we apply cyclotomic cubing to compute the hard part of the final exponentiation in the BLS family. In fact, for all BLS curves, $\frac{\phi_k(p)}{r}$ is given in [17] in the form $\psi_{k,p,u}+3$, where $\psi_{k,p,u} \in \mathbb{Z}$. Let $\alpha \in G_{\Phi_k(p)}$, the computation of the hard part simplifies to $\alpha^{\psi_{k,p,u}+3} = \alpha^{\psi_{k,p,u}}\alpha^{\mathbf{3}}$. The computation of $\alpha^{\mathbf{3}}$ consists in cyclotomic cubing instead of a multiplication and squaring. This results in a fixed computational gain expressed as $(\mathbf{M_k}+\mathbf{S_k})-\mathbf{C_{c_k}}$.

Application

The computation of α^3 using cyclotomic cubing allows us to save few operations in $\mathbb{F}_p$. Indeed;

- for $BLS15$; α^3 costs $\mathbf{C_{c_{15}}}$ instead of $\mathbf{M_{15}}+\mathbf{S_{15}}$, therefore, we gain

$$(\mathbf{M_{15}}+\mathbf{S_{15}})-\mathbf{C_{c_{15}}} \approx 26\mathbf{M_1},$$

- for $BLS27$; α^3 costs $\mathbf{C_{c_{27}}}$ instead of $\mathbf{M_{27}}+\mathbf{S_{27}}$, therefore, we gain

$$(\mathbf{M_{27}}+\mathbf{S_{27}})-\mathbf{C_{c_{27}}} \approx 81\mathbf{M_1}.$$

We consider the above gains when comparing the costs of the final exponentiation over $BLS15$ and $BLS27$ using the method **SM** and our upcoming methods. As outlined in [17], these costs are determined under **SM** as follows:

$$\mathbf{I_{15}}+19\times\mathbf{M_{15}}+\mathbf{S_{15}}+10\times\mathbf{F_{15}}+\mathbf{I_{c_{15}}}+2\times\mathbf{E_{u-1}}+9\times\mathbf{E_u}, \tag{2}$$

and

$$\mathbf{I_{27}}+9\times\mathbf{M_{27}}+\mathbf{S_{27}}+6\times\mathbf{F_{27}}+2\times\mathbf{E_{u-1}}+17\times\mathbf{E_u}. \tag{3}$$

These costs will be performed as follows under our upcoming methods:

$$\mathbf{I_{15}}+18\times\mathbf{M_{15}}+\mathbf{C_{c_{15}}}+10\times\mathbf{F_{15}}+\mathbf{I_{c_{15}}}+2\times\mathbf{E_{u-1}}+9\times\mathbf{E_u}, \tag{4}$$

and

$$\mathbf{I_{27}}+8\times\mathbf{M_{27}}+\mathbf{C_{c_{27}}}+6\times\mathbf{F_{27}}+2\times\mathbf{E_{u-1}}+17\times\mathbf{E_u} \tag{5}$$

In this section, we present a new method of applying the cyclotomic cubing called ”Two Consecutive Active Bits”.

3.2 Two Consecutive Active Bits (TCAB)

For some existing seeds in the literature, the binary representation contains two consecutive active bits with a particular form. This allows us to apply cyclotomic cubing in exponentiation within the cyclotomic subgroup. This form can occur in the least, middle, or most significant bits of the seed. Since the first two cases yield no gain, we focus exclusively on the last one.

This section explores possible seed forms suitable for **TCAB**, along with existing examples. We also generate new seeds that are useful for the **TCAB** method.

Description

Let h be the Hamming weight of the seed u. Then, u is expressed as:

$$u = 2^{s_1}+2^{s_2}+\cdots+2^{s_{h-1}}+2^{s_h},$$

where $s_1,\ldots,s_h \in \mathbb{N}$ satisfy $s_1 < s_2 < \cdots < s_{h-1} < s_h$. Based on the value of $s_h - s_{h-1}$, we identify two possible cases where we can apply cyclotomic cubing. The first case arises when $s_h - s_{h-1} = 1$, while the second occurs when $s_h - s_{h-1} = 3$. Consequently, the seed u can be expressed as follows:

$$u = 2^{s_1}+2^{s_2}+\cdots+2^{s_{h-2}}+2^{s_{h-1}}\times\mathbf{3^c},$$

where

$$c = \begin{cases} 1, \text{ if } s_h - s_{h-1} = 1, \\ 2, \text{ if } s_h - s_{h-1} = 3. \end{cases}$$

This leads to the following expression for $\alpha \in G_{\phi_k(p)}$:

$$\alpha^u = \alpha^{2^{s_1}+2^{s_2}+\cdots+2^{s_{h-2}}} (\alpha^{\mathbf{2^{s_{h-1}}}})^{\mathbf{3^c}}.$$

Using the current method, computing α^u costs:

$$s_{h-1}\mathbf{S_k} + (h-2)\mathbf{M_k} + c\mathbf{C_{c_k}},$$

whereas using (**SM**) method incurs:

$$s_h\mathbf{S_k} + (h-1)\mathbf{M_k}.$$

Table 2 presents the gains from using **TCAB** over **SM**.

$\mathbf{s_h - s_{h-1}}$	1	3
Gain	$\mathbf{S_k + M_k - C_{c_k}}$	$\mathbf{3S_k + M_k - 2C_{c_k}}$

Table 2: The gain of using **TCAB** instead of **SM**.

Examples

We examine literature seeds where **TCAB** applies to $BLS15$ and $BLS27$ and identify the following ones:

- For $BLS15$, the found seed is

$$u_{e_{15.190}} = 2^6 + 2^{59} + 2^{62} + \mathbf{2^{73}} + \mathbf{2^{74}},$$

which is proposed in [1] and corresponds to the 190-bit security level. The costs of **TCAB** and **SM** applied to $u_{e_{15.190}}$ are

$$3\mathbf{M_{15}} + 73\mathbf{S_{15}} + \mathbf{C_{c_{15}}} = 5096\mathbf{M_1} \quad \text{and} \quad 4\mathbf{M_{15}} + 74\mathbf{S_{15}} = 5122\mathbf{M_1}.$$

- For $BLS27$, the only identified seeds at the security levels 192 and 256 bits are

$$u_{e_{27.192}} = -2^5+2^8+2^{12}+2^{16}+\mathbf{2^{21}} + \mathbf{2^{22}} \quad \text{from [4]} \quad \text{and} \quad u_{e_{27.256}} = -2^3+2^8+2^{25}+\mathbf{2^{27}} + \mathbf{2^{28}} \quad \text{from [29]}.$$

The costs of **TCAB** and **SM** applied to the seeds $u_{e_{15.190}}$, $u_{e_{27.192}}$, and $u_{e_{27.256}}$, are given in Table 3.

Seeds	**Methods**	
	TCAB	**SM**
$u_{e_{15.190}}$	$3\mathbf{M_{15}} + 73\mathbf{S_{15}} + \mathbf{C_{c_{15}}} = 5096\mathbf{M_1}$	$4\mathbf{M_{15}} + 74\mathbf{S_{15}} = 5122\mathbf{M_1}$
$u_{e_{27.192}}$	$4\mathbf{M_{27}} + 21\mathbf{S_{27}} + \mathbf{C_{c_{27}}} + \mathbf{I_{c_{27}}} = 4554\mathbf{M_1}$	$5\mathbf{M_{27}} + 22\mathbf{S_{27}} + \mathbf{I_{c_{27}}} = 4635\mathbf{M_1}$
$u_{e_{27.256}}$	$3\mathbf{M_{27}} + 27\mathbf{S_{27}} + \mathbf{C_{c_{27}}} + \mathbf{I_{c_{27}}} = 5256\mathbf{M_1}$	$4\mathbf{M_{27}} + 28\mathbf{S_{27}} + \mathbf{I_{c_{27}}} = 5337\mathbf{M_1}$

Table 3: A cost comparison of **TCAB** and **SM** applied to the Seeds $u_{e_{15.190}}$, $u_{e_{27.192}}$, and $u_{e_{27.256}}$.

New seeds

We aimed to generate new seeds suitable for **TCAB** while adhering to the following constraints:

1. Following the recommendations of Barbulescu and Duquesne [2] for discrete logarithm computation over the field $\mathbb{F}_{p^k}$ concerning the size of p^k.
2. Generating binary seeds to avoid additional cyclotomic inversion costs.
3. Produce odd seeds or those whose least significant active bit is equal to 2, guaranteeing $\mathbf{E_{u-1}} \leq \mathbf{E_u}$.
4. Generate more efficient seeds considering the seed sizes from [4, 11].

- **New seed for TCAB at the $128-$bit security level**

  - **Case of $k = 15$**
    We generated the seed
    $$u = 2 + 2^{12} + 2^{26} + 2^{28} + 2^{29}$$
    which yields a prime p with 355 bits and a prime r with 238 bits. The cost of exponentiation in $G_{\Phi_{15}(p)}$ by this seed using **TCAB** is
    $$\mathbf{3M_{15} + 28S_{15} + C_{c_{15}} = 2171M_1}.$$
    Notably, the exponentiation in $G_{\Phi_{15}(p)}$ by $u-1$ incurs the same cost. Using expression (4), we apply **TCAB** to the seed u, demonstrating that the final exponentiation cost for the optimal Ate pairing over $BLS15$ is
    $$229\mathbf{M_1} + 18 \times (78\mathbf{M_1}) + 117\mathbf{M_1} + 10 \times (14\mathbf{M_1}) + 78\mathbf{M_1} + 2 \times (2171\mathbf{M_1}) + 9 \times (2171\mathbf{M_1}) = 25849\mathbf{M_1}$$

  - **Case of $k = 27$**
    We generated the seed
    $$u = 2 + 2^{9} + 2^{12} + 2^{15},$$
    resulting in a 303-bit prime p and a 272-bit prime r. Using **TCAB**, the cost of exponentiation by u or $u-1$ in $G_{\Phi_{27}(p)}$ is
    $$\mathbf{2M_{27} + 12S_{27} + 2C_{c_{27}} = 2844M_1}.$$
    Applying **TCAB** to the current seed and using the expression (5), the final exponentiation over $BLS27$ is
    $$536\mathbf{M_1} + 8 \times (216\mathbf{M_1}) + 288\mathbf{M_1} + 6 \times (26\mathbf{M_1}) + 2 \times (2844\mathbf{M_1}) + 17 \times (2844\mathbf{M_1}) = 56744\mathbf{M_1}.$$

- **New seeds for TCAB at the $192-$bit security level**

  - **Case of $k = 15$**
    We determined the seed
    $$u = 1 + 2^{9} + 2^{16} + 2^{68} + 2^{71},$$
    leading to an 853-bit prime p and a 570-bit prime r. Using **TCAB**, the costs of exponentiation in $G_{\Phi_{15}(p)}$ by u and $u-1$ are
    $$\mathbf{3M_{15} + 68S_{15} + 2C_{c_{15}} = 4888M_1} \quad \text{and} \quad \mathbf{2M_{15} + 68S_{15} + 2C_{c_{15}} = 4810M_1}.$$
    Applying **TCAB** to the seed u and using the expression (4), the cost of the final exponentiation of optimal Ate pairing over the $BLS15$ curve is
    $$229\mathbf{M_1} + 18 \times (78\mathbf{M_1}) + 117\mathbf{M_1} + 10 \times (14\mathbf{M_1}) + 78\mathbf{M_1} + 2 \times (4810\mathbf{M_1}) + 9 \times (4888\mathbf{M_1}) = 55580\mathbf{M_1}.$$

  - **Case of $k = 27$**
    We found the seed
    $$u = 1 + 2^{11} + 2^{20} + 2^{23} + 2^{24},$$
    resulting in a 492-bit prime p and a 443-bit prime r. This seed results in an exponentiation in $G_{\Phi_{27}(p)}$ with the following cost:
    $$\mathbf{3M_{27} + 23S_{27} + C_{c_{27}} = 4455M_1}.$$
    The exponentiation by $u-1$ in $G_{\Phi_{27}(p)}$ costs $4239\mathbf{M_1}$. Using the expression (5) and applying **TCAB** to the current seed, the cost of the final exponentiation of optimal Ate pairing over the $BLS27$ curve is
    $$536\mathbf{M_1} + 8 \times (216\mathbf{M_1}) + 288\mathbf{M_1} + 2 \times (4239\mathbf{M_1}) + 17 \times (4455\mathbf{M_1}) + 6 \times (26\mathbf{M_1}) = 86921\mathbf{M_1}.$$

- **New seeds for TCAB at the $256-$bit security level ($k = 27$)**
  We generated the seed
  $$u = 2 + 2^{41} + 2^{45} + 2^{48}$$
  which results in a 963-bit prime p and an 866-bit prime r. Applying **TCAB**, the cost of exponentiation in $G_{\Phi_{27}(p)}$ by u or $u-1$ is
  $$\mathbf{2M_{27} + 45S_{27} + 2C_{c_{27}} = 7893M_1}.$$

Based on the expression (5), the cost of the final exponentiation of optimal Ate pairing over the curve $BLS27$ by applying **TCAB** to the seed u is

$$536\mathbf{M_1} + 8 \times (216\mathbf{M_1}) + 288\mathbf{M_1} + 2 \times (7893\mathbf{M_1}) + 17 \times (7893\mathbf{M_1}) + 6 \times (26\mathbf{M_1}) = 152675\mathbf{M_1}.$$

Table 4 presents all newly generated seeds, including the curve embedding degree, the prime p size, the security level, and the curve equation coefficient b.

Seed	**k**	**Size(p)**	**Size(p^k)**	**Sec-level**	**b**	**DL algorithm**
$2 + 2^{12} + 2^{26} + 2^{28} + 2^{29}$	15	355	5323	128	16	SexTNFS
$2 + 2^{9} + 2^{12} + 2^{15}$	27	303	8160	128	16	SexTNFS
$1 + 2^{9} + 2^{16} + 2^{68} + 2^{71}$	15	853	12787	192	1	exTNFS
$1 + 2^{11} + 2^{20} + 2^{23} + 2^{24}$	27	492	13265	192	2	SexTNFS
$2 + 2^{41} + 2^{45} + 2^{48}$	27	963	25975	256	3	exTNFS

Table 4: New valid seeds for **TCAB** use.

Comparison

We evaluate **TCAB** and **SM** on new seeds, emphasizing **TCAB**'s benefits. Table 5 compares final exponentiation complexity for optimal Ate pairing on $BLS15$ and $BLS27$ using both methods, computed via (4) and (5) for **TCAB**, and (2) and (3) for **SM**.

Seed	**k**	**Method**	**Complexity**					
			$\mathbf{I_k}$	$\mathbf{M_k}$	$\mathbf{S_k}$	$\mathbf{C_{c_k}}$	$\mathbf{I_{c_k}}$	$\mathbf{F_k}$
$2 + 2^{41} + 2^{45} + 2^{48}$	27	**TCAB**	1	46	855	39	0	6
		SM	1	66	913	0	0	6
$1 + 2^{11} + 2^{20} + 2^{23} + 2^{24}$	27	**TCAB**	1	63	437	20	0	6
		SM	1	83	457	0	0	6
$1 + 2^{9} + 2^{16} + 2^{68} + 2^{71}$	15	**TCAB**	1	49	748	23	1	10
		SM	1	61	782	0	1	10
$2 + 2^{9} + 2^{12} + 2^{15}$	27	**TCAB**	1	46	228	39	0	6
		SM	1	66	286	0	0	6
$2 + 2^{12} + 2^{26} + 2^{28} + 2^{29}$	15	**TCAB**	1	51	308	12	1	10
		SM	1	63	320	0	1	10

Table 5: Comparison of the final exponentiation complexity over $BLS15$ and $BLS27$ using **TCAB** and **SM** applied to the new seeds.

We compare the final exponentiation cost over $BLS15$ and $BLS27$ elliptic curves in Table 6 when applying **TCAB** and **SM** using Tables 1 and 5. Additionally, we evaluate **TCAB**'s gain over **SM**.

Seed	**k**	**Method**	**Cost**	**Gain (TCAB/SM)**
$2 + 2^{41} + 2^{45} + 2^{48}$	27	**TCAB**	$152675\mathbf{M_1}$	$1962\mathbf{M_1}$
		SM	$154637\mathbf{M_1}$	
$1 + 2^{11} + 2^{20} + 2^{23} + 2^{24}$	27	**TCAB**	$86921\mathbf{M_1}$	$1085\mathbf{M_1}$
		SM	$88006\mathbf{M_1}$	
$1 + 2^{9} + 2^{16} + 2^{68} + 2^{71}$	15	**TCAB**	$55580\mathbf{M_1}$	$377\mathbf{M_1}$
		SM	$55957\mathbf{M_1}$	
$2 + 2^{9} + 2^{12} + 2^{15}$	27	**TCAB**	$56744\mathbf{M_1}$	$1962\mathbf{M_1}$
		SM	$58706\mathbf{M_1}$	
$2 + 2^{12} + 2^{26} + 2^{28} + 2^{29}$	15	**TCAB**	$25849\mathbf{M_1}$	$312\mathbf{M_1}$
		SM	$26161\mathbf{M_1}$	

Table 6: Comparison of the cost of the final exponentiation for pairings over $BLS15$ and $BLS27$ using **TCAB** and **SM** with new seeds.

We compare, Table 7, final exponentiation costs for optimal Ate pairing on $BLS15$ and $BLS27$, applying **TCAB** to new seeds and **SM** to existing ones [4, 11].

Seed	k	Sec-level	Complexity	Gain
$2+2^{12}+2^{26}+2^{28}+2^{29}$ (**This work**)	15	128	$\mathbf{I_{15}}+51\mathbf{M_{15}}+308\mathbf{S_{15}}+12\mathbf{C_{c_{15}}}+\mathbf{I_{c_{15}}}+10\mathbf{F_{15}}=25849\mathbf{M_1}$	$1040\mathbf{M_1}(3.9\%)$
$2^2+2^5+2^{19}+2^{31}$ [11]			$\mathbf{I_{15}}+54\mathbf{M_{15}}+342\mathbf{S_{15}}+\mathbf{I_{c_{15}}}+10\mathbf{F_{15}}=26889\mathbf{M_1}$	
$1+2^{11}+2^{20}+2^{23}+2^{24}$ (**This work**)	27	192	$\mathbf{I_{27}}+63\mathbf{M_{27}}+437\mathbf{S_{27}}+20\mathbf{C_{c_{27}}}+6\mathbf{F_{27}}=86921\mathbf{M_1}$	$4527\mathbf{M_1}(5\%)$
$1+2^4+2^{14}+2^{17}+2^{25}$ [11]			$\mathbf{I_{27}}+83\mathbf{M_{27}}+476\mathbf{S_{27}}+6\mathbf{F_{27}}=91448\mathbf{M_1}$	
$2+2^{41}+2^{45}+2^{48}$ (**This work**)	27	256	$\mathbf{I_{27}}+46\mathbf{M_{27}}+855\mathbf{S_{27}}+39\mathbf{C_{c_{27}}}+6\mathbf{F_{27}}=152675\mathbf{M_1}$	$14355\mathbf{M_1}(8.6\%)$
$1+2^9+2^{28}+2^{42}+2^{51}$ [11]			$\mathbf{I_{27}}+83\mathbf{M_{27}}+970\mathbf{S_{27}}+6\mathbf{F_{27}}=167030\mathbf{M_1}$	

Table 7: Comparison of our seeds and existing ones based on final exponentiation cost over $BLS15$ and $BLS27$.

Table 7 leads to the following findings:

- At the 256-bit security level, our seed outperforms [11] in efficiency while exhibiting slightly lower security.
- At the 128-bit and 192-bit security levels, our seed ensures both security and efficiency.

Despite modest gains, this section confirms cyclotomic cubing's applicability in final exponentiation with binary seeds. To improve them, the next section explores generating sparse ternary seeds.

4 Exponentiation using the sparse ternary representation

This section focuses on enhancing the computation of the final exponentiation of optimal Ate pairing by generating sparse ternary seeds and applying cyclotomic cubing.

4.1 Cubing and multiplication (CM)

To benefit from using ternary representation, we introduce an alternative to **SM** that replaces squaring with cubing. Given a seed u, its ternary representation is:

$$tern(u) = (t_0 t_1 \cdots t_{n-1})_3,$$

where $t_i \in \{0, 1, 2\}$, and

$$u = \sum_{i=0}^{n-1} t_i 3^i,$$

with n denoting its length. Let $k \in \mathbb{N}^*$ such that $3 \mid k$ and $\alpha \in G_{\Phi_k(p)} \subset \mathbb{F}_{p^k}$. To exploit cyclotomic cubing and ternary sparsity, α^u is computed using 'cubing and multiply' (**CM**), detailed in Algorithm 1. This method applies one cyclotomic cubing per digit and multiplies when the digit is nonzero.

Algorithm 1 CM (Cubing and multiplication)

Input: Parameter $u = (t_0, t_1, \cdots, t_n)_3$, $\alpha \in G_{\Phi_k(p)} \subset \mathbb{F}_{p^k}$
Output: α^u.

```
1. $r = 1$,
2. $\beta = \alpha^2$,//If the ternary representation of $u$ contains 2
3. for $j = n - 1$ down to 0 do
  3.1 $r \leftarrow r^3$,
  3.2 if $t_j = 1$ then $r \leftarrow r\alpha$,
  3.3 if $t_j = 2$ then $r \leftarrow r\beta$.
4. return $r$.
```

4.2 Generating new sparse ternary seeds

We aim to generate novel sparse ternary seeds while adhering to the following constraints:

1. Following the security requirements outlined in [2], which address the size of p^k,
2. Each new seed must have its least significant bit set to 1, ensuring the reduction of the cost associated with $\mathbf{E_{u-1}}$,
3. The newly proposed seeds should maintain competitiveness in terms of final exponentiation cost when compared to the seeds presented in [11].

We denote our seeds by u_t and those of [11] by u_b. Let h_t and h_b be the ternary and binary Hamming weights of u_t and u_b. Exponentiation in $G_{\phi_k(p)}$ by u_t using **CM** costs:

$$c_t = (h_t - 1)\mathbf{M_k} + \mathbf{S_k} + (\log_3(u_t) - 1)\mathbf{C_{c_k}}.$$

With **SM**, exponentiation by u_b in $G_{\phi_k(p)}$ costs:

$$c_b = (h_b - 1)\mathbf{M_k} + (\log_2(u_b) - 1)\mathbf{S_k}.$$

For each security level, we construct sparse ternary seeds that ensure $c_t < c_b$. We have generated the following seeds:

- For 128-bit security with curve $BLS15$:

$$1 + 3^2 + 3^5 + 3^{10} + 3^{16}.$$

- For 192-bit security with curve $BLS27$:

$$1 + 2 \times 3^9 + 3^{11}.$$

- For 256-bit security with curve $BLS27$:

$$1 + 3 + 2 \times 3^{20} + 2 \times 3^{26}.$$

4.3 Comparison

In this section, we conduct the comparison as follows:

1. Table 8 highlights the security properties of our new ternary seeds versus those proposed in [11].

Seed	**Sec-level**	**Size(p)**	**Size(r)**	**Size($\mathbf{p^k}$)**	**DL Alg**
$1 + 3^2 + 3^5 + 3^{10} + 3^{16}$	128	303	203	4542	exTNFS
$2^2 + 2^5 + 2^{19} + 2^{31}$ [11]		371	249	5557	SexTNFS
$1 + 2 \times 3^9 + 3^{11}$	192	353	318	9529	exTNFS
$1 + 2^4 + 2^{14} + 2^{17} + 2^{25}$ [11]		511	410	13461	SexTNFS
$1 + 3 + 2 \times 3^{20} + 2 \times 3^{26}$	256	851	766	22976	exTNFS
$1 + 2^9 + 2^{28} + 2^{42} + 2^{51}$ [11]		1019	883	27499	SexTNFS

Table 8: Comparison of security properties of our ternary seeds with binary seeds in [11]. $k = 27$ for **Sec-level**$=$ 256 or 192 and $k = 15$ for **Sec-level**$=$ 128.

2. Table 9 compares the cost of exponentiation in $G_{\phi_{15}(p)}$ and $G_{\phi_{27}(p)}$ applying **CM** our new ternary seeds and **SM** to those proposed in [11].

Seed	k	Sec-level	Method	Cost	Gain
$1+3^2+3^5+3^{10}+3^{16}$	15	128	**CM**	$\mathbf{4M_{15}+16C_{c_{1}5}=2184M_1}$	$\mathbf{65M_1}$
$2^2+2^5+2^{19}+2^{31}$ [11]			**SM**	$\mathbf{3M_{15}+31S_{15}=2249M_1}$	
$1+2\times3^9+3^{11}$	27	192	**CM**	$\mathbf{2M_{27}+S_{27}+11C_{c_{27}}=3753M_1}$	$\mathbf{936M_1}$
$1+2^4+2^{14}+2^{17}+2^{25}$ [11]			**SM**	$\mathbf{4M_{27}+25S_{27}=4689M_1}$	
$1+3+2\times3^{20}+2\times3^{26}$	27	256	**CM**	$\mathbf{3M_{27}+S_{27}+26C_{c_{27}}=8289M_1}$	$\mathbf{378M_1}$
$1+2^9+2^{28}+2^{42}+2^{51}$ [11]			**SM**	$\mathbf{4M_{27}+51S_{27}=8667M_1}$	

Table 9: Comparison of the cost of exponentiation by the ternary seeds and the seeds of [11] in $G_{\phi_{15}(p)}$ and $G_{\phi_{27}(p)}$.

Since the gains are positive in Table 9, we extend the comparison to the final exponentiation cost of the optimal Ate pairing over $BLS15$ and $BLS27$. Applying **CM** to our seeds, we compute the final exponentiation costs as follows:

- At 128-bit security level, with the seed

  $$u = 1+3^2+3^5+3^{10}+3^{16},$$

  expression (2) gives the cost over $BLS15$:

  $$229\mathbf{M_1}+18\times(78\mathbf{M_1})+117\mathbf{M_1}+(78\mathbf{M_1})+10\times(14\mathbf{M_1})+2\times(2106\mathbf{M_1})+9\times(2184\mathbf{M_1})=25836\mathbf{M_1}.$$

- At 192-bit security level, with the seed

  $$u = 1+2\times3^9+3^{11},$$

  expression (5) yields the cost over $BLS27$:

  $$536\mathbf{M_1}+8\times(216\mathbf{M_1})+288\mathbf{M_1}+6\times(26\mathbf{M_1})+2\times(3537\mathbf{M_1})+17\times(3753\mathbf{M_1})=73583\mathbf{M_1}.$$

- At 256-bit security level, with the seed

  $$u = 1+3+2\times3^{20}+2\times3^{26}$$

  the cost over $BLS27$ amounts to:

  $$536\mathbf{M_1}+8\times(216\mathbf{M_1})+288\mathbf{M_1}+6\times(26\mathbf{M_1})+2\times(8073\mathbf{M_1})+17\times(8289\mathbf{M_1})=159767\mathbf{M_1}.$$

Table 10 compares the costs of our seeds with those from [11], highlighting their gains.

Seeds	k	Sec-level	Cost	Gain
$1+3^2+3^5+3^{10}+3^{16}$ **(This work)**	15	128	$25836\mathbf{M_1}$	$1053\mathbf{M_1}(3.9\%)$
$2^2+2^5+2^{19}+2^{31}$ [11]			$26889\mathbf{M_1}$	
$1+2\times3^9+3^{11}$ **(This work)**	27	192	$73583\mathbf{M_1}$	$17865\mathbf{M_1}(19.3\%)$
$1+2^4+2^{14}+2^{17}+2^{25}$ [11]			$91448\mathbf{M_1}$	
$1+3+2\times3^{20}+2\times3^{26}$ **(This work)**	27	256	$159767\mathbf{M_1}$	$7263\mathbf{M_1}(4.3\%)$
$1+2^9+2^{28}+2^{42}+2^{51}$ [11]			$167030\mathbf{M_1}$	

Table 10: Comparison of the final exponentiation costs and the gain offered by our seeds

Though slightly less secure than those in [11], our seeds are more efficient and remain exTNFS-secure.

5 Conclusion

In this paper, we demonstrated the applicability of cyclotomic cubing for computing the final exponentiation of optimal Ate pairing through a two step approach. The first step involves a direct application, culminating in a formula to calculate the cost of the final exponentiation over $BLS15$ and $BLS27$. The second step introduces the **TCAB** method, which applies cyclotomic cubing using a particular structure in the seed's binary representation. To further explore the use of cyclotomic cubing in calculating the final exponentiation for $BLS15$ and $BLS27$, we endeavored to generate novel sparse ternary representation seeds. While these new seeds exhibit slightly lower security compared to existing ones, they offer enhanced efficiency. The challenge with sparse ternary representation seeds stems from the lack of sparsity in their binary representations, which undermines the efficiency of the Miller algorithm. Consequently, advancements in cyclotomic cubing and the finding of a ternary based alternative to the double and add method [9] are crucial to overcome this limitation.

References

[1] Aranha DF, Fotiadis G, Guillevic A (2024) A short-list of pairing-friendly curves resistant to the special tnfs algorithm at the 192-bit security level. Cryptology ePrint Archive Report 2024/294

[2] Barbulescu R, Duquesne S (2019) Updating key size estimations for pairings. Journal of cryptology 32:1298–1336

[3] Barbulescu R, Gaudry P, Guillevic A, et al (2015) Improving nfs for the discrete logarithm problem in non-prime finite fields. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, pp 129–155

[4] Barbulescu R, El Mrabet N, Ghammam L (2020) A taxonomy of pairings, their security, their complexity. HAL science ouverte

[5] Barreto PS, Naehrig M (2005) Pairing-friendly elliptic curves of prime order. In: International workshop on selected areas in cryptography, Springer, pp 319–331

[6] Barreto PS, Lynn B, Scott M (2003) Constructing elliptic curves with prescribed embedding degrees. In: Security in Communication Networks: Third International Conference, SCN 2002 Amalfi, Italy, September 11–13, 2002 Revised Papers 3, Springer, pp 257–267

[7] Boneh D, Franklin M (2001) Identity-based encryption from the weil pairing. In: Annual international cryptology conference, Springer, pp 213–229

[8] Boneh D, Lynn B, Shacham H (2001) Short signatures from the weil pairing. In: International conference on the theory and application of cryptology and information security, Springer, pp 514–532

[9] Coron JS (1999) Resistance against differential power analysis for elliptic curve cryptosystems pp 292–302

[10] Duan P, Cui S, Chan CW (2005) Special polynomial families for generating more suitable elliptic curves for pairing-based cryptosystems. Cryptology ePrint Archive

[11] Fouotsa E, El Mrabet N, Pecha A (2020) Optimal ate pairing on elliptic curves with embedding degree $9, 15$ and 27. Journal of groups, complexity, cryptology 12

[12] Fuentes-Castaneda L, Knapp E, Rodríguez-Henríquez F (2011) Faster hashing to. In: International workshop on selected areas in cryptography, Springer, pp 412–430

[13] Galbraith SD (2012) Mathematics of Public Key Cryptography, 1st edn. Cambridge University Press, Cambridge

[14] Ghammam L, Fouotsa E (2016) Adequate elliptic curves for computing the product of n pairings. In: International workshop on the arithmetic of finite fields, Springer, pp 36–53

[15] Ghammam L, Fouotsa E (2019) Improving the computation of the optimal ate pairing for a high security level. Journal of Applied Mathematics and Computing 59(1):21–36

[16] Granger R, Scott M (2010) Faster squaring in the cyclotomic subgroup of sixth degree extensions. In: International Workshop on Public Key Cryptography, Springer, pp 209–223

[17] Hayashida D, Hayasaka K, Teruya T (2020) Efficient final exponentiation via cyclotomic structure for pairings over families of elliptic curves. Cryptology ePrint Archive

[18] Hess F, Smart NP, Vercauteren F (2006) The eta pairing revisited. IEEE transactions on information theory 52(10):4595–4602

[19] Joux A (2004) A one round protocol for tripartite diffie–hellman. Journal of cryptology 17(4):263–276

[20] Kachisa EJ, Schaefer EF, Scott M (2008) Constructing brezing-weng pairing-friendly elliptic curves using elements in the cyclotomic field. In: International conference on pairing-based cryptography, Springer, pp 126–135

[21] Karabina K (2013) Squaring in cyclotomic subgroups. Mathematics of Computation 82(281):555–579

[22] Khamseh E (2021) The review on elliptic curves as cryptographic pairing groups. Mathematics and Computational Sciences 2(2):50–59

[23] Kim T, Barbulescu R (2016) Extended tower number field sieve: A new complexity for the medium prime case. In: Annual international cryptology conference, Springer, pp 543–571

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

[25] Nanjo Y, Shirase M, Kusaka T, et al (2020) An explicit formula of cyclotomic cubing available for pairings on elliptic curves with embedding degrees of multiple of three. In: 2020 35th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC), IEEE, pp 288–292

[26] Scott M, Benger N, Charlemagne M, et al (2009) On the final exponentiation for calculating pairings on ordinary elliptic curves. In: Pairing-Based Cryptography–Pairing 2009: Third International Conference Palo Alto, CA, USA, August 12-14, 2009 Proceedings 3, Springer, pp 78–88

[27] Stam M, Lenstra AK (2003) Efficient subgroup exponentiation in quadratic and sixth degree extensions. In: Cryptographic Hardware and Embedded Systems-CHES 2002: 4th International Workshop Redwood Shores, CA, USA, August 13–15, 2002 Revised Papers 4, Springer, pp 318–332

[28] Vercauteren F (2009) Optimal pairings. IEEE transactions on information theory 56(1):455–461

[29] Zhang X, Lin D (2012) Analysis of optimum pairing products at high security levels. In: Progress in Cryptology-INDOCRYPT 2012: 13th International Conference on Cryptology in India, Kolkata, India, December 9-12, 2012. Proceedings 13, Springer, pp 412–430