Correction of parameters in "Computing Optimal Ate Pairings on Elliptic Curves with Embedding Degree 9, 15 and 27"

Walid Haddaji[1,2]
[1]Science and Technology for Defense Lab (LR19DN01),
Center for Military Research, Military Academy,
Tunis, Tunisia
[2]Mathematics Department, Faculty of Sciences,
University of Monastir, 5019 Monastir, Tunisia
haddajiwalid95@gmail.com

Abstract

We correct two errors in Section 8 of the above-mentioned paper concerning the seed parameters proposed for BLS27 elliptic curves (embedding degree $k = 27$) at the 256-bit and 192-bit security levels. In both instances, the disclosed seeds produce a composite $r(x)$, violating the primality condition essential for constructing pairing-friendly curves. Additionally, for the 192-bit seed, the characteristic $p(x)$ is also composite. We provide verified corrected seeds for each security level, obtained by exhaustive search, and confirm with SageMath that both $p(x)$ and $r(x)$ are prime in each case. Furthermore, we correct the formula for the final exponentiation cost that was adopted from Zhang et al. in the original paper.

Keywords: BLS27 curves, pairing friendly curves, bilinear pairings, seed correction, SageMath.

1 Background and Notation

The BLS27 family of pairing-friendly elliptic curves [2] is parametrised by an integer x via the polynomials

$$p(x) = \tfrac{1}{3}(x-1)^2\big(x^{18} + x^9 + 1\big) + x, \tag{1}$$

$$r(x) = \tfrac{1}{3}\big(x^{18} + x^9 + 1\big), \tag{2}$$

$$t(x) = x + 1, \tag{3}$$

where p is the characteristic of the base field, r is the order of the pairing-friendly subgroup, and t is the Frobenius trace [6]. For the curve $E/\mathbb{F}_p$ defined by these polynomials to yield a valid pairing-friendly instance it is *necessary* that:

1. $p(x)$ is prime (the base field characteristic);
2. $r(x)$ is prime (the subgroup order);
3. $x \equiv 1 \pmod 3$ so that $3 \mid (x^{18} + x^9 + 1)$ and $r(x)$ is an integer.

A composite $r(x)$ admits small-subgroup attacks [8] and invalidates the hardness assumption underlying every pairing-based protocol built on the curve [3, 4].
For resistance against the SexTNFS discrete-logarithm algorithm, Barbulescu–Duquesne [1] and Scott–Guillevic [9] require $\log_2(p^{27}) \geq 27\,410$ at the AES-256 level and $\log_2(p^{27}) \geq 12\,871$ at the AES-192 level (Table 4 of [5]). Since $\deg p = 20$ and $\deg r = 18$ in x, one has $\log_2 p \approx (20/18)\log_2 r$ (the ρ-value is $10/9$).

Throughout, M_1, S_1, I_1 denote the costs of a multiplication, squaring and inversion in $\mathbb{F}_p$, and $I_{G_{\phi_3(p^9)}}$ denotes inversion in the relevant cyclotomic subgroup, following the notation of [5].

In the rest of this paper, all computations are performed using SageMath version 10.4 (released on July 19, 2024).

2 Error at the 256-Bit Security Level (Section 8.3)

In Section 8.3 of [5], the seed proposed for the 256-bit security level is

$$x_{\text{old}}^{(256)} = 2^{51} + 2^{42} + 2^{28} + 2^9 + 1. \tag{4}$$

Proposition 1. *$r\left(x_{\text{old}}^{(256)}\right)$ is composite. Hence $x_{\text{old}}^{(256)}$ does not define a valid pairing-friendly curve. The characteristic $p\left(x_{\text{old}}^{(256)}\right)$ is, however, prime.*

Proof. The following SageMath [10] session verifies both claims:

```
sage: x0 = 2^51 + 2^42 + 2^28 + 2^9 + 1
sage: R.<u> = PolynomialRing(QQ)
sage: r(u) = (u^18 + u^9 + 1) / 3
sage: p(u) = ((u - 1)^2) * r(u) + u
sage: is_prime(r(x0))
False
sage: is_prime(p(x0))
True
```

□

Corrected seed. We replace (4) with

$$x_{\text{new}}^{(256)} = 2^{51} + 2^{39} + 2^{33} + 2^{25} + 2^6 + 1. \tag{5}$$

Proposition 2. *The seed $x_{\text{new}}^{(256)}$ defined by (5) is valid. Specifically:*

(i) *$r\left(x_{\text{new}}^{(256)}\right)$ is a prime of* **917** *bits;*

(ii) *$p\left(x_{\text{new}}^{(256)}\right)$ is a prime of* **1019** *bits;*

(iii) *$\log_2\left(p^{27}\right) = 27\,497.4 \geq 27\,410$, satisfying the SexTNFS resistance bound of [1, 9];*

(iv) *$x_{\text{new}}^{(256)} \equiv 1 \pmod 3$;*

(v) *The Hamming weight of $x_{\text{new}}^{(256)}$ is 6, one more than that of $x_{\text{old}}^{(256)}$, resulting in one additional addition step in the Miller loop.*

Proof.
```
sage: x_new = 2^51 + 2^39 + 2^33 + 2^25 + 2^6 + 1
sage: is_prime(r(x_new)),  is_prime(p(x_new))
(True, True)
sage: int(r(x_new)).bit_length(),int(p(x_new)).bit_length()
(917, 1019)
sage: log(int(p(x_new))^27, 2).n()
27497.3991710550
sage: x_new % 3
1
sage: bin(x_new).count('1')
6
```

□

3 Error at the 192-Bit Security Level (Section 8.2)

In Section 8.2 of [5], the seed proposed for the 192-bit security level is

$$x_{\text{old}}^{(192)} = 2^{25} + 2^{17} + 2^{14} + 2^4 + 1. \tag{6}$$

Proposition 3. *Both* $r\left(x_{\text{old}}^{(192)}\right)$ *and* $p\left(x_{\text{old}}^{(192)}\right)$ *are composite.*

Proof.
```
sage: x1 = 2^25 + 2^17 + 2^14 + 2^4 + 1
sage: is_prime(r(x1)),is_prime(p(x1))
(False, False)
```

□

Corrected seed. We replace (6) with

$$x_{\text{new}}^{(192)} = 2^{24} + 2^{23} + 2^{20} + 2^{11} + 1. \tag{7}$$

This corrected seed was previously presented in [7].

Proposition 4. *The seed* $x_{\text{new}}^{(192)}$ *defined by* (7) *is valid. Specifically:*

(i) $r\left(x_{\text{new}}^{(192)}\right)$ *is a prime of* **443** *bits;*

(ii) $p\left(x_{\text{new}}^{(192)}\right)$ *is a prime of* **492** *bits;*

(iii) $\log_2\left(p^{27}\right) = 13\,264.9 \geq 12\,871$*, satisfying the SexTNFS resistance bound of [1, 9];*

(iv) $x_{\text{new}}^{(192)} \equiv 1 \pmod 3$*;*

(v) *The Hamming weight of* $x_{\text{new}}^{(192)}$ *is* 5*, the same as that of* $x_{\text{old}}^{(192)}$*.*

Proof.
```
sage: x_new2 = 2^24 + 2^23 + 2^20 + 2^11 + 1
sage: is_prime(r(x_new2)),  is_prime(p(x_new2))
(True, True)
sage: int(r(x_new2)).bit_length(),int(p(x_new2)).bit_length()
(443, 492)
sage: log(int(p(x_new2))^27, 2).n()
13264.9492430232
sage: x_new2 % 3
1
sage: bin(x_new2).count('1')
5
```

□

Table 1 summarises the erroneous and corrected parameter sets, together with their primality status and security properties.

Table 1: Erroneous and corrected BLS27 seeds. "✗" denotes composite and "✓" denotes prime.

Security Level	Seed x	$nbits(r)$	$nbits(p)$	$\log_2(p^{27})$	r prime	p prime	HW
256-bit	$2^{51}+2^{42}+2^{28}+2^9+1$ (original)	917	1019	27 498.7	✗	✓	5
	$2^{51}+2^{39}+2^{33}+2^{25}+2^6+1$ (corrected)	917	1019	27 497.4	✓	✓	6
192-bit	$2^{25}+2^{17}+2^{14}+2^4+1$ (original)	449	499	13 460.6	✗	✗	5
	$2^{24}+2^{23}+2^{20}+2^{11}+1$ (corrected)	443	492	13 264.9	✓	✓	5

4 Costs using our new parameters

By analysing the present paper, we deduce the generic formulas for computing the costs of the Miller loop and the final exponentiation of the optimal Ate pairing on the BLS27 curves for a given seed. Let $x = \sum_{i=0}^{n} b_i 2^i$ with $b_i \in \{-1, 0, 1\}$, and let h_x denote its Hamming weight, i.e. the number of non-zero digits in its signed binary representation.

4.1 Generic formulas

Miller Algorithm. The original paper assumes that the addition step and the doubling step share the same cost. For this reason, each doubling or addition step is referred to as a *Miller step*, and its cost is given by:

$$C_{\text{step}} = 9M_1 + I_9 + 2S_9 + 3M_9.$$

The Miller loop consists of n doubling steps and $h_x - 1$ addition steps, giving

$$(n + h_x - 1)\, C_{\text{step}}$$

for the step part. The f-updates contribute

$$(n-1)S_{27} + (n + h_x - 3)M_{27}.$$

Therefore, the total Miller-loop cost is

$$\begin{aligned} C_{\text{Miller}} = {} & (n + h_x - 1)I_9 + 9(n + h_x - 1)M_1 + 2(n + h_x - 1)S_9 \\ & + 3(n + h_x - 1)M_9 + (n-1)S_{27} + (n + h_x - 3)M_{27}, \end{aligned} \tag{8}$$

together with some full inversions in $\mathbb{F}_{p^{27}}$, if the signed binary representation of the seed x contains negative digits, which is mentioned in Remark 6.1 in [5].

Final exponentiation. According to the original paper, the final exponentiation costs

$$I_{27} + 2\big(nS_{27} + (h_x - 2)M_{27}\big) + 17\big(nS_{27} + (h_x - 1)M_{27}\big) + 11M_{27} + 2I_{G_{\phi_3(p^9)}}$$

together with the Frobenius maps $p, p^2, p^3, p^4, p^5, p^6, p^7, p^8, 2p^9$. The authors of the original paper used the work of Zhang et al. [11], where the final exponentiation of the Ate pairing factors as

$$(p^{27} - 1)/r = (p^9 - 1)(p^{18} + p^9 + 1)/r = (p^9 - 1) \cdot d.$$

The power of d is referred to as the hard part. According to [11] (Section 4.3), it can be expanded in base p as follows:

$$d = (p^{18} + p^9 + 1)/r = (x-1)^2 \cdot (p^9 + x^9 + 1) \cdot (p^8 + x \cdot p^7 + \cdots + x^7 \cdot p + x^8) + 3.$$

For the Miller loop output $f \in \mathbb{F}_{p^{27}}$, we first compute the easy part $M = f^{(p^9-1)}$. Then, we compute the hard part as follows:

$$M_1 = M^{p^8} \cdot M^{xp^7} \cdot M^{x^2p^6} \cdot M^{x^3p^5} \cdot M^{x^4p^4} \cdot M^{x^5p^3} \cdot M^{x^6p^2} \cdot M^{x^7p} \cdot M^{x^8},$$
$$M_2 = M_1^{(x-1)^2}, \quad M_3 = M_2^{x^9} \cdot M_2^{p^9} \cdot M_2, \quad M_4 = M^3 \cdot M_3.$$

Note that the hard part computation is performed in the cyclotomic subgroup $G_{\Phi_{27}(p)}$. Zhang et al. stated in [11] that the cost of the final exponentiation is

$$I_{27} + 2E_{x-1} + 17E_x + 11M_{27}$$

together with the Frobenius maps $p, p^2, p^3, p^4, p^5, p^6, p^7, p^8, 2p^9$. They also claimed that the cost for computing M^3 is included in computing M^x. However, we remark that the formula given in [11] is not fully correct for the following reasons:

1. The easy part is $M = f^{(p^9-1)} = f^{p^9} \cdot f^{-1}$. This step requires one inversion in $\mathbb{F}_{p^{27}}$, one multiplication in $\mathbb{F}_{p^{27}}$, and a p^9-Frobenius map.
2. The computation of M^3 is included in the computation of M^x only if the two most significant bits of the seed x verify the following property:

$$b_n = b_{n-1} = 1. \tag{9}$$

   This property is verified by the seed $x = 2^{28} + 2^{27} + 2^{25} + 2^8 - 2^3$ proposed by Zhang et al. in [11]. For this specific seed, computing M^3 is indeed free. However, if property (9) does not hold, the inclusion is invalid; in this case, only the calculation of M^2 is precomputed in M^x. Consequently, M^3 requires one additional multiplication in $\mathbb{F}_{p^{27}}$.

Therefore, the corrected cost of the final exponentiation is

$$I_{27} + 2E_{x-1} + 17E_x + 228M_1 + (12 + \mathbf{1}_{\{b_n \neq 1 \text{ or } b_{n-1} \neq 1\}})M_{27},$$

where $228M_1$ is the total cost of the Frobenius maps, based on Table 2 in the original paper, and $\mathbf{1}_{\{\mathcal{C}\}}$ denotes the indicator function, which equals 1 if condition $\mathcal{C}$ is true and 0 otherwise. The costs E_x and E_{x-1} are given by:

$$E_x = nS_{27} + (h_x - 1)M_{27} + \delta \cdot I_{G_{\phi_3(p^9)}}, \quad E_{x-1} = nS_{27} + (h_{x-1} - 1)M_{27} + \delta' \cdot I_{G_{\phi_3(p^9)}},$$

where

$$\delta = \mathbf{1}_{\{x \text{ contains a negative digit}\}}, \quad \delta' = \mathbf{1}_{\{x-1 \text{ contains a negative digit}\}}.$$

Consequently, substituting E_x and E_{x-1} into the final exponentiation cost, we obtain:

$$\begin{aligned} C_{\text{final}} = I_{27} + 19nS_{27} &+ \big(17h_x + 2h_{x-1} - 7 + \mathbf{1}_{\{b_n \neq 1 \text{ or } b_{n-1} \neq 1\}}\big)M_{27} \\ &+ \big(17\delta + 2\delta'\big)I_{G_{\phi_3(p^9)}} + 228M_1. \end{aligned} \tag{10}$$

4.2 Application to $x_{\text{new}}^{(256)}$

In this section, we use the arithmetic operations costs given in Table 2 in the original paper. Consider the seed

$$x_{\text{new}}^{(256)} = 2^{51} + 2^{39} + 2^{33} + 2^{25} + 2^6 + 1.$$

Subtracting one yields

$$x_{\text{new}}^{(256)} - 1 = 2^{51} + 2^{39} + 2^{33} + 2^{25} + 2^6,$$

and $h_{x_{\text{new}}^{(256)}} = 6$ and $h_{x_{\text{new}}^{(256)}-1} = 5$. Consequently, neither the signed binary representation of $x_{\text{new}}^{(256)}$ nor that of $x_{\text{new}}^{(256)} - 1$ contains any negative digits. Therefore, neither the full inversion in $\mathbb{F}_{p^{27}}$ during the Miller loop nor the cyclotomic inversion in the final exponentiation are required. Furthermore, the seed $x_{\text{new}}^{(256)}$ does not satisfy property (9). Ultimately, this yields $\mathbf{1}_{\{b_{51} \neq 1 \text{ or } b_{50} \neq 1\}} = 1$ and $\delta = \delta' = 0$.

Miller loop. Applying the formula (8), we obtain

$$\begin{aligned}C_{\text{Miller}} &= (51+6-1)I_9 + 9\times(51+6-1)M_1 + 2\times(51+6-1)S_9 + 3\times(51+6-1)M_9\\ &\quad + (51-1)S_{27} + (51+6-3)M_{27}\\ &= 56I_9 + 9\times 56\,M_1 + 2\times 56\,S_9 + 3\times 56\,M_9 + 50S_{27} + 54M_{27}\\ &= 56I_9 + 504M_1 + 112S_9 + 168M_9 + 50S_{27} + 54M_{27}.\\ &= 56I_1 + 21744M_1 + 9722S_1.\end{aligned}$$

Final exponentiation. Applying the formula (10), we obtain

$$\begin{aligned}C_{\text{final}} &= I_{27} + 19\times 51S_{27} + \big(17\times 6 + 2\times 5 - 7 + 1\big)M_{27} + \big(17\times 0 + 2\times 0\big)I_{G_{\phi_3(p^9)}} + 228M_1\\ &= I_{27} + 969S_{27} + (112-6)M_{27} + 228M_1\\ &= I_{27} + 969S_{27} + 106M_{27} + 228M_1\\ &= I_1 + 23511M_1 + 121187S_1.\end{aligned}$$

4.3 Application to $x_{\text{new}}^{(192)}$

Consider the seed

$$x_{\text{new}}^{(192)} = 2^{24} + 2^{23} + 2^{20} + 2^{11} + 1.$$

Since $x_{\text{new}}^{(192)} - 1 = 2^{24} + 2^{23} + 2^{20} + 2^{11}$, we have $h_{x_{\text{new}}^{(192)}} = 5$ and $h_{x_{\text{new}}^{(192)}-1} = 4$. Thus, neither $x_{\text{new}}^{(192)}$ nor $x_{\text{new}}^{(192)} - 1$ has negative digits in its signed binary representation, eliminating the need for full inversions in the Miller loop and cyclotomic inversions in the final exponentiation. Moreover, the seed satisfies $b_{24} = b_{23} = 1$ (verifying property (9)). This gives $\mathbf{1}_{\{b_{24}\neq 1 \text{ or } b_{23}\neq 1\}} = 0$ and $\delta = \delta' = 0$.

Miller loop. We apply (8) to obtain

$$\begin{aligned}C_{\text{Miller}}(24,5) &= (24+5-1)I_9 + 9\times(24+5-1)M_1 + 2\times(24+5-1)S_9 + 3\times(24+5-1)M_9\\ &\quad + (24-1)S_{27} + (24+5-3)M_{27}\\ &= 28I_9 + 9\times 28\,M_1 + 2\times 28\,S_9 + 3\times 28\,M_9 + 23S_{27} + 26M_{27}\\ &= 28I_9 + 252M_1 + 56S_9 + 84M_9 + 23S_{27} + 26M_{27}.\\ &= 28I_1 + 10656M_1 + 4611S_1.\end{aligned}$$

Final exponentiation. We use (10), to get

$$\begin{aligned}C_{\text{final}} &= I_{27} + 19\times 24S_{27} + \big(17\times 5 + 2\times 4 - 7 + 0\big)M_{27} + \big(17\times 0 + 2\times 0\big)I_{G_{\phi_3(p^9)}} + 228M_1\\ &= I_{27} + 456S_{27} + (93-7)M_{27} + 228M_1\\ &= I_{27} + 456S_{27} + 86M_{27} + 228M_1\\ &= I_1 + 19191M_1 + 57062S_1.\end{aligned}$$

We summarise the costs of the Miller loop and the final exponentiation of the optimal Ate pairing on BLS27 curve in Table 2, and give the costs reported in the original paper.

Table 2: Corrected costs for the BLS27 optimal ate pairing.

Level		Miller loop	Final exponentiation
256-bit	Original [5] (invalid)	$55I_1 + 21\,348M_1 + 9\,660S_1$	$I_1 + 19\,191M_1 + 122\,337S_1$
	Corrected ($x_{\text{new}}^{(256)}$)	$56I_1 + 21744M_1 + 9722S_1$	$I_1 + 23511M_1 + 121187S_1$
192-bit	Original [5] (invalid)	$29I_1 + 11\,052M_1 + 4\,798S_1$	$I_1 + 19\,191M_1 + 59\,587S_1$
	Corrected ($x_{\text{new}}^{(192)}$)	$28I_1 + 10656M_1 + 4611S_1$	$I_1 + 19191M_1 + 57062S_1$

5 Conclusion

In this paper, we replaced the seeds associated with the parameters p and r of the BLS27 curve presented in [5], which do not yield prime values of p and r, with seeds that ensure this primality. We also observed that for seeds containing no negative digits and having a least significant bit equal to 1, the final exponentiation formula involves no cyclotomic inversion.

References

[1] R. Barbulescu and S. Duquesne. Updating key size estimations for pairings. *Journal of Cryptology*, 32:1298–1336, 2019.

[2] P. S. L. M. Barreto, B. Lynn, and M. Scott. Constructing elliptic curves with prescribed embedding degrees. In *SCN 2002*, LNCS 2576, pp. 257–267, 2002.

[3] D. Boneh and M. K. Franklin. Identity-based encryption from the Weil pairing. In *CRYPTO 2001*, LNCS 2139, pp. 213–229, 2001.

[4] D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. *Journal of Cryptology*, 17(4):297–319, 2004.

[5] E. Fouotsa, N. El Mrabet, and A. Pecha. Computing optimal ate pairings on elliptic curves with embedding degree 9, 15 and 27. *Journal of Groups, Complexity, Cryptology*, 12(1):3:1–3:25, 2020.

[6] D. Freeman, M. Scott, and E. Teske. A taxonomy of pairing friendly elliptic curves. *Journal of Cryptology*, 23(2):224–280, 2010.

[7] W. Haddaji, L. Ghammam, N. El Mrabet, and L. Ben Abdelghani. Efficient pairings final exponentiation using cyclotomic cubing for odd embedding degrees curves. *Cryptology ePrint Archive*, Report 2025/958, 2025.

[8] C. H. Lim and P. J. Lee. A key recovery attack on discrete log-based schemes using a prime order subgroup. In *CRYPTO 1997*, LNCS 1294, pp. 249–263, 1997.

[9] M. Scott and A. Guillevic. A new family of pairing friendly elliptic curves. Cryptology ePrint Archive, Report 2018/193, 2018.

[10] The Sage Developers. *SageMath, the Sage Mathematics Software System.* `https://www.sagemath.org`, 2024.

[11] X. Zhang and D. Lin. Analysis of optimum pairing products at high security levels. In *INDOCRYPT 2012*, LNCS 7668, pp. 412–430, 2012.