

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

Journal of Groups, Complexity, Cryptology,

Vol. 12, Issue 1, 2020, pp. 3:1–3:25

Walid Haddaji^{1,2}

¹Science and Technology for Defense Lab (LR19DN01),
Center for Military Research, Military Academy,
Tunis, Tunisia

²Mathematics Department, Faculty of Sciences,
University of Monastir, 5019 Monastir, Tunisia
haddajiwali95@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. All other results of the original paper remain valid.

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

$$p(x) = \frac{1}{3}(x-1)^2(x^{18} + x^9 + 1) + x, \quad (1)$$

$$r(x) = \frac{1}{3}(x^{18} + x^9 + 1), \quad (2)$$

$$t(x) = x + 1, \quad (3)$$

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_{cyc} denotes inversion in the relevant cyclotomic subgroup, following the notation of [5].

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

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

Proposition 1. $r(x_{\text{old}}^{(256)})$ is composite. Hence $x_{\text{old}}^{(256)}$ does not define a valid pairing-friendly curve. The characteristic $p(x_{\text{old}}^{(256)})$ 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.<x> = ZZ[]
sage: r = (x^18 + x^9 + 1) // 3
sage: p = ((x-1)^2*(x^18+x^9+1))/3 + x
sage: r(x0).is_prime()
False
sage: p(x0).is_prime()
True
```

□

Corrected seed. We replace (4) with

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

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

- (i) $r(x_{\text{new}}^{(256)})$ is a prime of **917** bits;
- (ii) $p(x_{\text{new}}^{(256)})$ is a prime of **1019** bits;
- (iii) $\log_2(p^{27}) = 27497.4 \geq 27410$, 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: r(x_new).is_prime(), p(x_new).is_prime()
(True, True)
sage: r(x_new).nbits(), p(x_new).nbits()
(917, 1019)
sage: 27 * p(x_new).nbits()
27513
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

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

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

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

□

Corrected seed. We replace (6) with

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

This corrected seed was previously presented in [7].

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

- (i) $r(x_{\text{new}}^{(192)})$ is a prime of **443** bits;
- (ii) $p(x_{\text{new}}^{(192)})$ is a prime of **492** bits;
- (iii) $\log_2(p^{27}) = 13\,264.9 \geq 12\,871$, 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: r(x_new2).is_prime(), p(x_new2).is_prime()
(True, True)
sage: r(x_new2).nbits(), p(x_new2).nbits()
(443, 492)
sage: 27 * p(x_new2).nbits()
13284
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. “ $\times$ ” denotes composite and “ $\checkmark$ ” 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	$\times$	$\checkmark$	5
	$2^{51} + 2^{39} + 2^{33} + 2^{25} + 2^6 + 1$ (corrected)	917	1019	27 497.4	$\checkmark$	$\checkmark$	6
192-bit	$2^{25} + 2^{17} + 2^{14} + 2^4 + 1$ (original)	449	499	13 460.6	$\times$	$\times$	5
	$2^{24} + 2^{23} + 2^{20} + 2^{11} + 1$ (corrected)	443	492	13 264.9	$\checkmark$	$\checkmark$	5

2 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

$$x = 2^n + \dots + 2^0,$$

where n is the highest exponent in the binary representation of x , and let h denote the Hamming weight of x , i.e. the number of non-zero bits in its binary expansion. We assume that the seed has no negative signed digits and that its least significant bit is 1, so that $x - 1$ also has no negative digits and its Hamming weight is $h - 1$. These assumptions are satisfied by the two seeds considered below.

2.1 Generic formulas

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 $h - 1$ addition steps, giving

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

for the step part. The f -updates contribute

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

Therefore, the total Miller-loop cost is

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

By deducing from the original paper, the final exponentiation costs

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

together with the Frobenius maps $p, p^2, p^3, p^4, p^5, p^6, p^7, p^8, 2p^9$. The term $2I_{G_{\phi_3(p^9)}}$ arises from the two exponentiations by $x - 1$ in the cyclotomic subgroup during the computation of the hard part of the final exponentiation. We however remark that for both their seeds and ours, the least significant bit is 1 and there are no negative digits. Hence $x - 1$ remains free of negative digits and no cyclotomic inversion is needed. Therefore, the corrected final exponentiation formula for this type of seed must *not* include the term $2I_{G_{\phi_3(p^9)}}$. Thus, for seeds with least significant bit 1 and no negative digits, the final exponentiation cost is

$$C_{\text{final}}(n, h) = I_{27} + 19n S_{27} + (19h - 10)M_{27} + 228M_1, \quad (9)$$

where $228M_1$ is the total cost of the Frobenius maps, based on Table 2 in the original paper.

2.2 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

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

Here $n = 51$ and $h = 6$, so there are 51 doubling steps and 5 addition steps.

Miller loop. Substituting $n = 51$ and $h = 6$ into (8), we obtain

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

Final exponentiation. Substituting $n = 51$ and $h = 6$ into (9), we obtain

$$\begin{aligned} C_{\text{final}}(51, 6) &= I_{27} + 19 \cdot 51 S_{27} + (19 \cdot 6 - 10)M_{27} + 228M_1 \\ &= I_{27} + 969S_{27} + (114 - 10)M_{27} + 228M_1 \\ &= I_{27} + 969S_{27} + 104M_{27} + 228M_1 \\ &= I_1 + 23079M_1 + 121187S_1. \end{aligned}$$

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

Consider the seed

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

Here $n = 24$ and $h = 5$, so there are 24 doubling steps and 4 addition steps.

Miller loop. Substituting $n = 24$ and $h = 5$ into (8), we obtain

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

Final exponentiation. Substituting $n = 24$ and $h = 5$ into (9), we obtain

$$\begin{aligned} C_{\text{final}}(24, 5) &= I_{27} + 19 \cdot 24 S_{27} + (19 \cdot 5 - 10)M_{27} + 228M_1 \\ &= I_{27} + 456S_{27} + (95 - 10)M_{27} + 228M_1 \\ &= I_{27} + 456S_{27} + 85M_{27} + 228M_1 \\ &= I_1 + 18975M_1 + 57062S_1 \end{aligned}$$

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 ($x_{\text{new}}^{(256)}$)	$56I_1 + 21\,744M_1 + 9\,722S_1$	$I_1 + 23\,079M_1 + 121\,187S_1$
192-bit	Original [5] (invalid)	$29I_1 + 11\,052M_1 + 4\,798S_1$	$I_1 + 19\,191M_1 + 59\,587S_1$
	Corrected ($x_{\text{new}}^{(192)}$)	$28I_1 + 10\,656M_1 + 4\,611S_1$	$I_1 + 18\,975M_1 + 57\,062S_1$

3 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.