

Family of embedded curves for BLS

Antonio Sanso 

Ethereum Foundation

Abstract. This paper presents embedded curves that stem from BLS elliptic curves, providing general formulas derived from the curve’s seed. The mathematical groundwork is laid, and advantages of these embeddings are discussed. Additionally, practical examples are included at the end of the paper.

1 Introduction

A pairing-friendly curve E has a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$, where $\mathbb{G}_1, \mathbb{G}_2$ are distinct prime-order r subgroups of E , and $\mathbb{G}_T \subset \mathbb{F}_{p^k}$ of the same order r . The current most efficient pairing-friendly elliptic curves are specific elliptic curves named after Barreto, Lynn, and Scott (BLS) [BLS03].

Nowadays, the main application of pairing in the field of cryptography is typically related to constructing Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge (zk-SNARKs), which are a specific type of cryptographic proof system. They allow one party to prove to another that a statement is true without revealing any information about the statement itself. A proof system involves a protocol in which one participant, known as the prover, endeavors to persuade another participant, known as the verifier, of the validity of a specific statement. In the context of zero-knowledge proofs, we add the condition that the proof must not disclose any information beyond the veracity of the statement. While verification of such proofs is typically rapid, generating such proofs can incur significant costs. This issue is exacerbated when there is involvement of elliptic curve arithmetic.

To mitigate this challenge in elliptic curve arithmetic, one approach is to select *embedded curves*. These are elliptic curves characterized by parameter selection that aligns its base field with the group order of the pairing curve, creating a correspondence with the modulus used in the arithmetic field. Embedded curves optimize the arithmetic operations within the proof of execution. In their work on CØCØ [KZM⁺15], Kosba, Zhao, Miller, Qian, Chan, Papamanthou and Pass introduced a collection of cryptographic primitives suitable for efficient verification using a SNARK. They achieved this by creating a novel (embedded) elliptic curve designed for the efficient execution of the necessary operation in key exchanges, namely, scalar multiplication.

BLS12-381 [Bow17], introduced by Sean Bowe in 2017 as a pairing-friendly curve, is presently in the midst of a standardization process led by the IRTF Crypto Forum Research Group. This curve has gained widespread adoption and is employed for digital signatures and zero-knowledge proofs in numerous projects within the blockchain ecosystem, including but not limited to Zcash, Ethereum 2.0, Anoma, Skale, Algorand, Dfinity, Chia, and various others.

Jubjub [ZCa] is an elliptic curve designed over the BLS12-381 scalar field \mathbb{F}_r by the ZCash team. In 2021 Masson, Sanso and Zhang presented Bandersnatch [MSZ21]: a fast elliptic curve built also over the BLS12-381 scalar field. Bandersnatch is equipped with an efficient endomorphism, allowing a fast scalar multiplication algorithm. As a result,

E-mail: asanso@ethereum.org (Antonio Sanso)



this enhancement has led to a 42% increase in the speed of scalar multiplication when compared to Jubjub. The GLV technique, as outlined in [GLV01], is a widely recognized approach to speeding up scalar multiplication on specific curves. In essence, it is applicable to elliptic curves where an efficient endomorphism can be calculated. The GLV method is particularly useful for curves with a j -invariant of $j = 0$ (or $j = 1728$) because it allows for the computation of a non-trivial automorphism with just a single modular multiplication. This method can also be adapted to work with other curves, even if the endomorphism is somewhat more computationally intensive. A survey of elliptic curves for proof systems can be found in [AHG22].

The motivation for further investigation and the writing of this paper was sparked by the observation that Bandersnatch is defined over the scalar field \mathbb{F}_r of the BLS curve, with the seed $u = -0xd20100000010000$. The author observed that the factorization of $u = -1 \cdot \mathbf{2^{16}} \cdot \mathbf{906349} \cdot \mathbf{254760293}$ overlaps significantly with some of the values found in the row of [MSZ21, Table 2] (partially presented here as Table 1).

Table 1: BLS12-381 embedded Curves for discriminants $-3 \geq -D \geq -4$.

$-D$	Curve sec.	Curve order
-3	65-bit	$2^2 \cdot 3 \cdot 97 \cdot 19829809 \cdot 2514214987 \cdot 423384683867248993 \cdot p_{131}$
	14-bit	$\mathbf{2^{64}} \cdot \mathbf{906349^4} \cdot \mathbf{p_{28}^4}$
	77-bit	$7 \cdot 43 \cdot 1993 \cdot 2137 \cdot 43558993 \cdot 69032539613749 \cdot p_{154}$
	41-bit	$3 \cdot 7 \cdot 13 \cdot 79 \cdot 2557 \cdot 33811 \cdot 1645861201 \cdot 75881076241177 \cdot 86906511869757553 \cdot p_{82}$
	13-bit	$3^2 \cdot 11^2 \cdot 19^2 \cdot 10177^2 \cdot 125527^2 \cdot 859267^2 \cdot 2508409^2 \cdot 2529403^2 \cdot p_{26}^2$
	118-bit	$836509 \cdot p_{236}$
-4	59-bit	$\mathbf{2^{32}} \cdot \mathbf{5} \cdot \mathbf{73} \cdot \mathbf{906349^2} \cdot \mathbf{254760293^2} \cdot \mathbf{p_{119}}$
	37-bit	$2^2 \cdot 29 \cdot 233 \cdot 34469 \cdot 1327789373 \cdot 19609848837063073 \cdot 159032890827948314857 \cdot p_{74}$
	37-bit	$2 \cdot 3^2 \cdot 11^2 \cdot 13 \cdot 1481 \cdot 10177^2 \cdot 859267^2 \cdot 52437899^2 \cdot 346160718017 \cdot p_{74}$
	57-bit	$2 \cdot 5 \cdot 19^2 \cdot 1709 \cdot 125527^2 \cdot 2508409^2 \cdot 2529403^2 \cdot p_{114}$

Outline. This paper is organized as follows. In Section 2, we give a mathematical foundation for understanding the concepts employed in the manuscript. Section 3, the main focus of the paper, offers a detailed description of the derivation of new formulas. Section 4 extends the algorithm from the original BLS paper to incorporate the new formulas. In Subsection 4.1, we will survey existing BLS curves while analyzing our new method retrospectively. In Subsection 4.2, we will propose a new BLS curve with an associated embedded curve of prime order, along with an efficient endomorphism. Finally, we draw conclusions in Section 5.

2 Preliminaries

We present a short background on pairing-friendly elliptic curves and complex multiplication (CM) method. Consider an elliptic curve denoted as E , defined over the finite field \mathbb{F}_p .

$$\#E(\mathbb{F}_p) = n = hr$$

where r is the largest prime divisor of n . For any elliptic curve E defined over \mathbb{F}_p with n points, Hasse's theorem [Sil92, V.1.1] applies. This theorem asserts that the trace t of the Frobenius endomorphism on E , linked to p and n through the equation $n = q + 1 - t$, is constrained within the range $|t| \leq 2\sqrt{p}$. Both the curve E and its quadratic twist, denoted as E^t , exhibit an isomorphism over the field \mathbb{F}_{p^2} , and their orders over \mathbb{F}_p are linked to the trace t , as expressed by the following formulas:

$$\#E(\mathbb{F}_p) = p + 1 - t \tag{1}$$

$$\#E^t(\mathbb{F}_p) = p + 1 + t.$$

Let's define the *embedding degree* to be the smallest positive integer k such that

$$r \mid p^k - 1$$

The r -torsion subgroup of E is denoted as $E[r] = \{P \in E(\overline{\mathbb{F}_p}) \mid [r]P = \mathcal{O}\}$ and has two subgroups of order r that are used for pairing applications. One can define several bilinear pairings, one of which is the Weil pairing defined as:

$$e : E[r] \times E[r] \rightarrow \mu_r \subset \mathbb{F}_{p^k}$$

For more formal definitions and details on elliptic curves over finite fields see [Sil92].

In this work, our focus revolves around cryptographic applications grounded in ordinary elliptic curves, implying that we seek values of t that do not satisfy the condition $t \not\equiv 0 \pmod{p}$. The endomorphism ring of these curves have a particular structure: $\text{End}(E)$ is an order of the imaginary quadratic field $\mathbb{Q}(\sqrt{t^2 - 4p})$. From now, we denote $-D$ to be the discriminant of $\text{End}(E)$, and $\{\text{Id}, \psi\}$ a basis of the endomorphism ring. The fundamental discriminant corresponds to the discriminant of the maximal order containing $\text{End}(E)$. This way, ψ is of degree $\frac{D+1}{4}$ or $D/4$ depending on the value of D modulo 4, and ψ can be defined using polynomials of degree $O(D)$ thanks to the Vélú's formulas [Vél71]. Thus, the evaluation of ψ is efficient only for curves of small discriminant. The complex multiplication (CM) technique is used to identify an elliptic curve characterized by a specified modulus, p , and a given trace, t . The method is successful when a solution can be identified for the CM equation with relatively modest values of D , represented by:

$$DV^2 = 4p - t^2 \tag{2}$$

It's important to note that when arbitrary selections of p and t are made while adhering to the Hasse condition (ensuring that the right-hand side is non-negative), the non-square component D may become significantly large. Nevertheless, the practicality of the CM method hinges on obtaining solutions that result in smaller values for D .

When $D = 3$, there are two cubic twists with $p + 1 - \frac{(\pm 3V - t)}{2}$ points, and two sextic twists with $p + 1 - \frac{(\pm 3V + t)}{2}$ points, where $V = \sqrt{\frac{4p - t^2}{3}}$. Analogously, when $D = 4$ there are two quartic twists with $p + 1 \pm 2V$ points, where $V = \sqrt{\frac{4p - t^2}{4}}$.

2.1 Barreto–Lynn–Scott (BLS) curves

BLS curves were introduced in [BLS03] Barreto, Lynn and Scott. These are a collection of elliptic curves suitable for pairings, specifically chosen with an embedding degree denoted as k , which is a multiple of 3 but not a multiple of 18. Various well-established families exist where these curves can be found with values of k such as 9, 12, 24, 27, and 48. The curves share common characteristics, with a j -invariant of 0 and a discriminant of $-D$, which equals -3 . Each family is characterized by polynomial parameters $q(u)$, $r(u)$, and $t(u)$. These parameters correspond to distinct aspects of the curve, respectively its characteristic, the subgroup order linked to the embedding degree k , and the trace. Notably, the subgroup order is defined by $r(u)$ as $\Phi_k(u)$, where $\Phi_k(u)$ is the k -th cyclotomic polynomial. The trace is straightforwardly expressed as $t(u) = u + 1$. The order of the curve is calculated as $q(u) + 1 - t(u)$, and the CM equation can be represented as $Dy(u)^2 = 4q(u) - t(u)^2$.

3 Embedded curves

In the context of elliptic curve arithmetic, it becomes necessary to perform a modulo operation using the order of the field over which the curve is defined, denoted as p . This

presents a clever opportunity: ensuring that the order of the field defining our elliptic curve perfectly aligns with the modulus used in our zkSNARK arithmetic. In simpler terms, both fields should share the same p value.

This notion forms the basis for the concept of an embedded curve. An embedded curve is essentially an elliptic curve where the parameters have been carefully chosen so that the underlying prime field \mathbb{F}_p matches the group order of a hosting curve, and hence, it corresponds to the modulus used in the arithmetic field.

Consequently, when performing elliptic curve operations on an embedded curve, they essentially reduce to prime field arithmetic, utilizing the native modulo p operations of the field. In other words, the modulo operations required during elliptic curve computations become seamless, as the formula for point addition simplifies to a few multiplications and additions due to the alignment of moduli. This efficiency in embedded curve operations is what makes them highly effective within the realm of SNARK

This section presents the families of embedded curves for BLS12 and a generalization for all BLS curves. All parameters and formulas are expressed in the form of polynomials with respect to the variable u .

3.1 BLS embedded curves

The approach for creating embedded curves appears relatively simple. This involves extending the BLS curve generation, as described in [BLS03], adding the extra constraints needed for embedded curves and solve for the CM discriminant D (and for V) the CM equation $DV^2 = 4p - t^2$ and use the CM method to compute the curve equation coefficients. To distinguish the polynomial parameters of the hosting curve $(q(u), r(u), t(u))$ from those of the embedded curve, we will denote the parameters of the latter with the letter 'e' $(q(u)_e, r(u)_e, t(u)_e)$.

Given that embedded curves are constructed using the scalar field, and the BLS scalar field corresponds to the k -th cyclotomic polynomial, denoted as $q_e(u) = r(u) = \Phi_k(u)$ (where k represents the embedded degree), the CM equations take on the following form:

$$DV^2 = 4\Phi_k(u) - t^2 \quad (3)$$

No general method is known for solving the Diophantine equations above with a degree $\deg(\Phi_k)$ greater than 4 (see also [BLS03, MNT01]). We describe how to find algebraic solution to equation 3 for the special cases $D = 3, 4$.

Case $D = 3, k = 12$ Let's focus first on the case $D = 3, k = 12$ first. Equation 3 becomes

$$3V^2 = 4\Phi_{12}(u) - t^2 \quad (4)$$

then

$$V^2 = \frac{4(u^4 - u^2 + 1) - t^2}{3}$$

When attempting to derive generic formulas in terms of the BLS12 curve seed u , it is easy to prove that the solution $t = 2u^2 - 1$ is valid for equation 4 over the integer.

Substitute $t = 2u^2 - 1$ into the equation:

$$\begin{aligned} 3V^2 &= 4(u^4 - u^2 + 1) - (2u^2 - 1)^2 \\ 3V^2 &= 4(u^4 - u^2 + 1) - (4u^4 - 4u^2 + 1) \\ 3V^2 &= 4u^4 - 4u^2 + 4 - 4u^4 + 4u^2 - 1 \end{aligned}$$

¹for the embedded curve this is the full order

$$3V^2 = 3$$

$$V^2 = 1$$

So, when $t = 2u^2 - 1$, the equation $3V^2 = 4(u^4 - u^2 + 1) - t^2$ holds true for integer solutions, with V taking the values of 1 and -1. This proves that $t = 2u^2 - 1$ is indeed a solution for the given equation over the integers. It is trivial to prove that $t = 2u^2 - 1$ respects the Hasse-Weil bound. Taking in account equation 1 we can parameterize the order of the embedded curve in terms of curve seed u :

$$r_e(u) = u^4 - 3u^2 + 3$$

Now, we are using the quadratic, cubic, and sextic twist formulas in Section 2 to derive the other solutions: $t = -(2u^2 - 1)$, $t = \pm(u^2 + 1)$ and $t = \pm(u^2 - 2)$ and the corresponding orders ($r_e(u) = u^4 + u^2 + 3$, $r_e(u) = u^4 - 2u^2 + 1$, $r_e(u) = u^4 + 3$, $r_e(u) = u^4 - 2u^2 + 4$, $r_e(u) = u^4$).

Case $D = 4, k = 12$ Let's shift our focus to the case where $D = 4$ and $k = 12$. Equation 3 then becomes

$$4V^2 = 4\Phi_{12}(u) - t^2 \tag{5}$$

then

$$V^2 = \frac{4(u^4 - u^2 + 1) - t^2}{4}$$

Also here it is straightforward to prove that the solution $t = 2u^2 - 2$ is valid for equation 5 over the integer. We begin by proving that the solution satisfies the Hasse-Weil bound. Starting with the original inequality:

$$\begin{aligned} 2u^2 - 2 &\leq 2\sqrt{u^4 - u^2 + 1} \\ (2u^2 - 2)^2 &\leq (2\sqrt{u^4 - u^2 + 1})^2 \\ 4u^4 - 8u^2 + 4 &\leq 4(u^4 - u^2 + 1) \\ 4u^4 - 8u^2 + 4 &\leq 4u^4 - 4u^2 + 4 \\ 4u^4 - 8u^2 + 4 &\leq 4u^4 - 4u^2 + 4 \\ -8u^2 &\leq -4u^2 \\ 2u^2 &\geq u^2 \\ u^2 &\geq 0 \end{aligned}$$

This inequality is true for all integers u because the square of any integer is always non-negative. So, the original inequality $2u^2 - 2 \leq 2\sqrt{u^4 - u^2 + 1}$ holds for all integer values of u . To prove that $t = 2u^2 - 2$ is a solution for the equation $4V^2 = 4(u^4 - u^2 + 1) - t^2$ over the integers, we can substitute this value for t and see if it holds true. Let's do that:

$$\begin{aligned} 4V^2 &= 4(u^4 - u^2 + 1) - t^2 \\ 4V^2 &= 4(u^4 - u^2 + 1) - (2u^2 - 2)^2 \\ 4V^2 &= 4(u^4 - u^2 + 1) - (4u^4 - 8u^2 + 4) \\ 4V^2 &= 4u^4 - 4u^2 + 4 - 4u^4 + 8u^2 - 4 \\ 4V^2 &= 4u^2 \\ V^2 &= u^2 \end{aligned}$$

We have shown that if $t = 2u^2 - 2$, then the equation $4V^2 = 4(u^4 - u^2 + 1) - t^2$ simplifies to $V^2 = u^2$. This equation holds true for integer values of u and V . So, $t = 2u^2 - 2$ is indeed a solution to the given equation over the integers.

Now, we are using the quadratic and quartic twist formulas in Section 2 to derive the other solutions: $t = -(2u^2 - 2)$, and $t = \pm(2u)$ and the corresponding orders ($r_e(u) = u^4 - 3u^2 + 4$, $r_e(u) = u^4 + u^2$, $r_e(u) = u^4 - u^2 + 2u + 2$, $r_e(u) = u^4 - u^2 - 2u + 2$).

It is easy to show by induction that the formulas derived above can be generalized for all $i, j \geq 1$ for $k = 2^i 3^j$ as shown in Table 2 (analogous formulas could be derived for the less common $k = 3^j$ case).

Table 2: Parameters of BLS and embedded curves for $k = 2^i 3^j, i, j \geq 1, 18 \nmid k$

D	3	4
k	$2^i 3^j, i, j \geq 1 (6, 12, 24, 48, 96, \dots)$	
$t(u)$	$u + 1$	
$r(u) = q_e(u)$	$u^{k/3} - u^{k/6} + 1$	
$q(u)$	$\frac{r(u)(u-1)^2}{3} + u$	
$t_e(u)$	$2u^{k/6} - 1$ $-2u^{k/6} + 1$ $u^{k/6} + 1$ $-u^{k/6} - 1$ $u^{k/6} - 2$ $-u^{k/6} + 2$	$2u^{k/6} - 2$ $-2u^{k/6} + 2$ $2u^{k/12}$ $-2u^{k/12}$
$r_e(u)$	$u^{k/3} - 3u^{k/6} + 3$ $u^{k/3} + u^{k/6} + 1$ $u^{k/3} - 2u^{k/6} + 1$ $u^{k/3} + 3$ $u^{k/3} - 2u^{k/6} + 4$ $u^{k/3}$	$u^{k/3} - 3u^{k/6} + 4$ $u^{k/3} + u^{k/6}$ $u^{k/3} - u^{k/6} + 2u^{k/12} + 2$ $u^{k/3} - u^{k/6} - 2u^{k/12} + 2$

4 A general method

This section extends the algorithm outlined in [BLS03, Section 3.2] to accommodate the use of embedded curves. While the core structure of the algorithm remains unchanged, it incorporates an additional step: incrementing the seed until the generated $r(u)_e$ value is a prime number. The generated embedded curve will have a prime order with a discriminant of $D = 3$ or $D = 4$, allowing for the utilization of the non-trivial automorphism in implementing the GLV technique. Section 4.2 contains examples of this method. Existing curves like Jubjub and Bandersnatch are commonly represented in the Montgomery or Edwards form. Historically, the trend was to favor Montgomery and Edwards curves. However, thanks to recent advances in research, such as the closed-form formulas provided by [RCB16], we now possess the ability to efficiently and securely work with prime order curves. This enhanced knowledge has not only allowed us to design more robust interfaces for these curves, but it has also led to a deep appreciation of the inherent value of prime order curves, which remain immune to cofactor vulnerabilities. Nevertheless, for those who still prefer to use Montgomery or Edwards forms, it is possible to accommodate their choice by modifying the algorithm. One can simply stop when $r_e(u)$ takes on the form of $4p$ or $8p$, where p represents a prime number.

4.1 Existing BLS curves

In this Section we conducted a retrospective analysis of our new method while examining the landscape of existing BLS curves. The comprehensive analysis and findings can be succinctly summarized and presented in the form of Table 3. Among the curves we examined, it appears that two of them (specifically, BLS-440 and BLS-442 as defined in [BD19]) have the potential to host an appropriate embedded curve. BLS-440 has a p_{146} -order subgroup of the curve, while BLS-442 has a p_{147} -order subgroup, both with a cofactor of 4, indicating that these curves can be expressed in Montgomery form.

4.2 An example of the general construction

To demonstrate the feasibility of the method outlined in Section 4, we present a BLS12 curve that incorporates an embedded prime order curve. These curves can be built using the seed $u = -15132376222941635237$. This seed yields:

```
r = 52435875175126086317194268734274856590483579016894522447982524027249851530
39
q = 40024095552216554674225471656415571472778415993941077330341178057482976463
14110491974795389318365740812777421285127
```

Here r is a 255-bit prime, and q is a 381-bit prime. The associated BLS12 curve is quickly found as $E : y^2 = x^3 + 1$.

The associated embedded curve, denoted as E_e can be represented in the Weierstrass model using the equation $E_e : y^2 = x^3 + 15$. This curve is defined over the scalar field \mathbb{F}_r of the host curve and possesses a prime order of 52435875175126086317194268734274856590025601396589223746732046134954731438057. It's crucial to emphasize that the BLS curve presented here serves the sole purpose of demonstrating feasibility and does not meet all the criteria that a state-of-the-art pairing curve must adhere to, such as SNARK-friendliness, having a seed u with a low Hamming weight, and so on.

5 Conclusions

In this paper, we have introduced new formulas, extended existing algorithms, and proposed a novel BLS curve accompanied by an embedded curve of prime order and an efficient endomorphism. We have also conducted a comprehensive survey of existing BLS curves while concurrently performing a retrospective analysis of our new methodology.

The BLS curve presented in Subsection 4.2 includes an embedded curve of prime order along with an efficient endomorphism. However, it's important to acknowledge that the proposed curve may not fully satisfy all the necessary criteria. Therefore, we encourage readers to utilize the algorithm described in this paper to explore and address the challenge of enhancing the curve to meet additional criteria. This includes optimizing it for SNARK-friendliness, achieving a low Hamming weight for the seed u , and implementing other relevant improvements. This challenge remains an open problem and serves as an exercise for interested individuals to further investigate.

Acknowledgments. We would like to thank Diego Aranha, Luca De Feo, Youssef El Housni, Gottfried Herold, Dimitri Koshelev, Simon Masson and Michael Scott for fruitful discussions.

Table 3: Security of existing BLS embedded curves

Embedded curve security (Is Prime?)		
<i>D</i>	3	4
BLS12-381 [Bow17]	118-bit (N) 41-bit (N) 13-bit (N) 77-bit (N) 65-bit (N) 14-bit (N)	37-bit (N) 59-bit (N) 57-bit (N) 37-bit (N) - -
BLS12-377 [BCG+20]	63-bit (N) 40-bit (N) 30-bit (N) 71-bit (N) 65-bit (N) 32-bit (N)	57-bit (N) 32-bit (N) 38-bit (N) 40-bit (N) - -
BLS12-379 [EHG22]	65-bit (N) 34-bit (N) 14-bit (N) 52 (N) 90-bit (N) 27-bit (N)	66-bit (N) 58-bit (N) 33-bit (N) 36-bit (N) - -
BLS12-440 [BD19]	? (N) 61-bit (N) 25-bit (N) 95 (N) 122-bit (N) 10-bit (N)	146-bit (N) 58-bit (N) 43-bit (N) 36-bit (N) - -
BLS12-442 [BD19]	41-bit (N) ? (N) 16-bit (N) 119-bit (N) 99-bit (N) 29-bit (N)	147-bit (N) 65-bit (N) 39-bit (N) 59-bit (N) - -
BLS12-446 [GS21]	64-bit (N) 50-bit (N) 36-bit (N) 41-bit (N) 57-bit (N) 20-bit (N)	88-bit (N) 20-bit (N) 67-bit (N) 41-bit (N) - -
BLS12-461 [BD19]	136-bit (N) 50-bit (N) 36-bit (N) ? (N) 95-bit (N) 10-bit (N)	56-bit (N) 49-bit (N) 55-bit (N) 31-bit (N) - -
BLS24-315 [EHG22]	60-bit (N) 57-bit (N) 16-bit (N) 52-bit (N) 85-bit (N) 9-bit (N)	77-bit (N) 32-bit (N) 35-bit (N) 28-bit (N) - -
BLS24-317 [EHG22]	38-bit (N) 34-bit (N) 15-bit (N) 90-bit (N) 41-bit (N) 9-bit (N)	120-bit (N) 55-bit (N) 20-bit (N) 61-bit (N) - -

References

- [AHG22] Diego Aranha, Youssef Housni, and Aurore Guillevic. A survey of elliptic curves for proof systems. *Designs, Codes and Cryptography*, 12 2022. doi: [10.1007/s10623-022-01135-y](https://doi.org/10.1007/s10623-022-01135-y).
- [BCG⁺20] Sean Bowe, Alessandro Chiesa, Matthew Green, Ian Miers, Pratyush Mishra, and Howard Wu. Zexe: Enabling decentralized private computation. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 947–964, 2020. doi: [10.1109/SP40000.2020.00050](https://doi.org/10.1109/SP40000.2020.00050).
- [BD19] Razvan Barbulescu and Sylvain Duquesne. Updating key size estimations for pairings. *Journal of Cryptology*, 32(4):1298–1336, 2019.
- [BLS03] Paulo S. L. M. Barreto, Ben Lynn, and Michael Scott. Constructing elliptic curves with prescribed embedding degrees. In Stelvio Cimato, Giuseppe Persiano, and Clemente Galdi, editors, *Security in Communication Networks*, pages 257–267, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.
- [Bow17] Sean Bow. BLS12-381: New zk-SNARK elliptic curve constructio, 2017. <https://electriccoin.co/blog/new-snark-curve/>.
- [EHG22] Youssef El Housni and Aurore Guillevic. Families of snark-friendly 2-chains of elliptic curves. In Orr Dunkelman and Stefan Dziembowski, editors, *Advances in Cryptology – EUROCRYPT 2022*, pages 367–396, Cham, 2022. Springer International Publishing.
- [GLV01] Robert P. Gallant, Robert J. Lambert, and Scott A. Vanstone. Faster point multiplication on elliptic curves with efficient endomorphisms. pages 190–200, 2001. doi: [10.1007/3-540-44647-8_11](https://doi.org/10.1007/3-540-44647-8_11).
- [GS21] Aurore Guillevic and Shashank Singh. On the alpha value of polynomials in the tower number field sieve algorithm. *Mathematical Cryptology*, 1(1):1–39, Feb. 2021. URL: <https://journals.flvc.org/mathcryptology/article/view/125142>.
- [KZM⁺15] Ahmed Kosba, Zhichao Zhao, Andrew Miller, Yi Qian, Hubert Chan, Charalampos Papamanthou, Rafael Pass, abhi shelat, and Elaine Shi. C0c0: A framework for building composable zero-knowledge proofs. *Cryptology ePrint Archive*, Paper 2015/1093, 2015. <https://eprint.iacr.org/2015/1093>. URL: <https://eprint.iacr.org/2015/1093>.
- [MNT01] Atsuko Miyaji, Masaki Nakabayashi, and Shunzou Takano. New explicit conditions of elliptic curve traces for FR-reduction. *TIEICE: IEICE Transactions on Communications/Electronics/Information and Systems*, E84-A(5):1234–1243, 2001.
- [MSZ21] Simon Masson, Antonio Sanso, and Zhenfei Zhang. Bandersnatch: a fast elliptic curve built over the bls12-381 scalar field. *Cryptology ePrint Archive*, Paper 2021/1152, 2021. <https://eprint.iacr.org/2021/1152>. URL: <https://eprint.iacr.org/2021/1152>.
- [RCB16] Joost Renes, Craig Costello, and Lejla Batina. Complete addition formulas for prime order elliptic curves. pages 403–428, 2016. doi: [10.1007/978-3-662-49890-3_16](https://doi.org/10.1007/978-3-662-49890-3_16).
- [Sil92] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992.

- [Vél71] Jacques Vélú. Isogénies entre courbes elliptiques. *Comptes Rendus de l'Académie des Sciences de Paris*, 273:238–241, 1971.
- [ZCa] ZCash. What is Jubjub? <https://web.archive.org/web/20230201163714/https://z.cash/technology/jubjub/>.