Families of prime-order endomorphism-equipped embedded curves on pairing-friendly curves

Antonio Sanso[1] and Youssef El Housni[2]

[1] Ethereum Foundation
[2] Linea

Abstract. This paper presents a procedure to construct parameterized families of prime-order endomorphism-equipped elliptic curves that are defined over the scalar field of pairing-friendly elliptic curve families such as Barreto–Lynn–Scott (BLS), Barreto–Naehrig (BN) and Kachisa–Schaefer–Scott (KSS), providing general formulas derived from the curves' seeds. These so-called "embedded curves" are of major interest in SNARK applications that prove statements involving elliptic curve arithmetic i.e. digital signatures. In this paper, the mathematical groundwork is laid, and advantages of these embeddings are discussed. Additionally, practical examples in the case of BN and BLS families are included and impossibility results regarding KSS families are explained.

Keywords: elliptic curves · bilinear pairings · complex multiplication · zero-knowledge proofs

1 Introduction

A pairing-friendly curve E is an elliptic curve that admits an efficiently computable bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, where $\mathbb{G}_1, \mathbb{G}_2$ are prime-order r subgroups of E, and $\mathbb{G}_T \subset \mathbb{F}_{q^k}$ of the same order r. Nowadays, one of the main applications of pairings 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 systems. 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, one adds 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. In pairing-based (zk)-SNARKs, the first step is to "arithmetize" the statement to be proved, that is writing the statement over the scalar field $\mathbb{F}_r$. This issue is exacerbated when the statement involves elliptic curve arithmetic such as proving a signature verification i.e. ECDSA [Ame05] and EdDSA [BDL+12] or pre-image knowledge of curve-based hash function i.e. Bowe-Hopwood Pedersen hash [HBHW]. This is of tremendous interest for zero-knowledge rollups [1] and privacy-reserving cryptocurrencies (e.g. zcash [HBHW]).

To mitigate this challenge, one approach is to select *embedded curves* (see definition 1). These are elliptic curves characterized by parameter selection that aligns its base field characteristic with the group order of the pairing-friendly curve.

E-mail: asanso@ethereum.org (Antonio Sanso), youssef.elhousni@consensys.net (Youssef El Housni)

[1] https://ethereum.org/en/developers/docs/scaling/zk-rollups

Definition 1. An *embedded curve* E_e is an elliptic curve defined over $\mathbb{F}_r$ where r is the subgroup prime-order of a distinct elliptic curve E. If, in addition, E_e admits an fast non-trivial endomorphism, we call it an *endomorphism-equipped embedded curve.*

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 an embedded elliptic curve designed for the efficient execution of the necessary operation in key exchanges, namely, scalar multiplication (see Fig. 1).

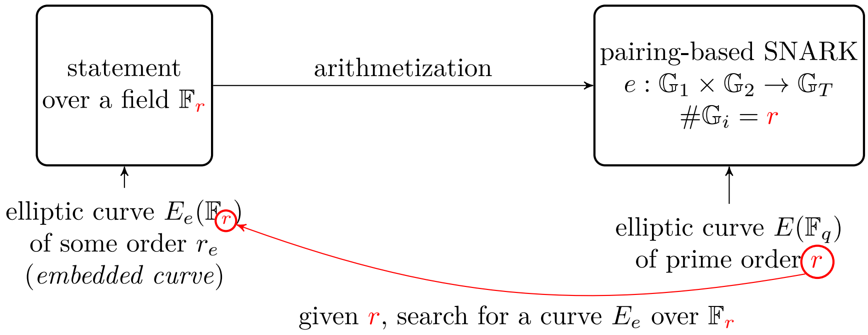
statement
over a field $\mathbb{F}_r$
arithmetization
pairing-based SNARK
$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$
$\#\mathbb{G}_i = r$
elliptic curve $E_e(\mathbb{F}_r)$
of some order r_e
(*embedded curve*)
elliptic curve $E(\mathbb{F}_q)$
of prime order r
given r, search for a curve E_e over $\mathbb{F}_r$

Figure 1: Kosba et al. construction [KZM+15]

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, Filecoin, Anoma, Skale, Algorand, Dfinity, Chia, and various others.

Building on CØCØ, the Zcash team introduced the JubJub curve [Zca] which is an embedded curve over BLS12-381. This curve allowed Zcash to efficiently implement a collision-resistant variant of Pedersen hash inside a SNARK, the now so-called Bowe-Hopwood Pedersen hash. In 2021 Masson, Sanso and Zhang presented Bandersnatch [MSZ21]: the first endomorphism-equipped embedded curve over the BLS12-381. It allowed a fast scalar multiplication algorithm which 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. An exhaustive search shows that a similar embedded curve to Bandersnatch is unlikely to be found by luck for other SNARK curves of interest. For more details about embedded curves and elliptic curves for proof systems in general can be found in [AHG23].

The motivation behind the writing of this paper was sparked by the observation that Bandersnatch is defined over the scalar field $\mathbb{F}_r$ of the BLS12 curve, with the seed u = `-0xd201000000010000`. The first 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 [MSZ21, Table 2] (partially presented here as Table 1)[2]. Existing curves like Jubjub and Bandersnatch are commonly represented in the Montgomery or Edwards form. Historically,

[2] In the paper, we use subscripts q_n to indicate an n-bit number not necessarily prime.

the trend was to favor Montgomery and Edwards curves. However, thanks to complete formulas provided by [RCB16] and optimized Weierstrass scalar multiplication SNARK circuits (e.g. gnark [BPH+23] and Halo2 [zc]), we now possess the ability to efficiently and securely work with prime order curves out-circuit and in-circuit. 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. Hence, a natural question aries:

can we construct *families* of prime-order endomorphism-equipped embedded curves?

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

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

Our contribution. We present parameterized families of fast prime-order endomorphism-equipped embedded curves on BLS [BLS03], and BN [BN06] families of pairing-friendly elliptic curves. We derive generic formulas, in terms of the pairing-friendly curves seeds u and give concrete examples. We also investigate the case of KSS [**?**] curves and give impossibility results for the particular KSS16 and KSS18 families.

Outline. This paper is organized as follows. In Section 2, we give the mathematical foundations for understanding the concepts employed in the manuscript. In Section 3, we present relevant families of pairing-friendly elliptic curves on which our embedded curves will be constructed. Section 4 offers a detailed description of the constructions and formulas. In Section 5, the main focus of the paper, we apply our algorithm to construct embedded curves on BLS, BN and KSS pairing-friendly curves. Finally in section 6, we propose new instantiations of pairing-friendly curves and their endomorphism-equipped embedded curves. Finally, we draw conclusions in Section 7.

2 Preliminaries

We present a short background on pairing-friendly elliptic curves and complex multiplication (CM) method [AM93]. Let E be an elliptic curve defined over the finite field $\mathbb{F}_q$. Let its order be:

$$\#E(\mathbb{F}_q) = n = h \cdot r \ ,$$

where r is the largest prime divisor of n. For any elliptic curve E defined over $\mathbb{F}_q$ 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 q and n through the equation $n = q + 1 - t$, is constrained within the range $|t| \leq 2\sqrt{q}$. Both the curve E and its quadratic twist, denoted E^t, exhibit an isomorphism over the field $\mathbb{F}_{q^2}$, and their orders over $\mathbb{F}_q$ are linked to the trace t, as expressed by the following formulas:

$$\#E(\mathbb{F}_q) = q + 1 - t \tag{1}$$
$$\#E^t(\mathbb{F}_q) = q + 1 + t \ .$$

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

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

The r-torsion subgroup of E is denoted $E[r] = \{P \in E(\overline{\mathbb{F}_q}), [r]P = \mathcal{O}\}$ 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:

$$e : E[r] \times E[r] \to \mu_r \subset \mathbb{F}_{q^k} \ .$$

To determine the hierarchy among families sharing the same k, the *ρ-value* is established as the ratio between the sizes of q and r ($\rho = \log q / \log r$), measuring the base field size relative to the size of the prime-order subgroup on the curve. Because $r \mid q + 1 - t$, we have then $\rho \geq 1$. 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 satisfy the condition $t \not\equiv 0 \pmod{q}$. The endomorphism ring of these curves have a particular structure: $\mathrm{End}(E)$ is an order of the imaginary quadratic field $\mathbb{Q}(\sqrt{t^2 - 4q})$. From now, we denote $-D$ to be the discriminant of $\mathrm{End}(E)$, and $\{\mathrm{Id}, \psi\}$ a basis of the endomorphism ring. The fundamental discriminant corresponds to the discriminant of the maximal order containing $\mathrm{End}(E)$. 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 Vélu'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, q, 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:

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

It's important to note that when arbitrary selections of q 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 $q + 1 - \frac{(\pm 3V - t)}{2}$ points, and two sextic twists with $q + 1 - \frac{(\pm 3V + t)}{2}$ points, where $V = \sqrt{\frac{4q - t^2}{3}}$. Analogously, when $D = 4$ there are two quartic twists with $q + 1 \pm 2V$ points, where $V = \sqrt{\frac{4q - t^2}{4}}$.

3 Pairing-friendly curves

From a broad perspective, there are two approaches to obtaining (non-supersingular) pairing-friendly curves [FST10]:

- **Generic algorithms** that take parameters k and r as inputs and outputs (if it exists) an elliptic curve defined over a field $\mathbb{F}_q$ with an embedding degree k relative to a subgroup of prime order r over $\mathbb{F}_q$. Among these algorithms, the Cocks–Pinch method [CP01] stands out as the most flexible.

- **Parameterized families** that involve specifying a seed u along with polynomials $q(u)$, $t(u)$ and $r(u)$ that define the curve. This setup ensures the existence of an elliptic curve E over $\mathbb{F}_{q(u)}$ with a subgroup of order $r(u)$, and exhibits an embedding degree k with respect to $r(u)$.

In this work, we focus our attention on parameterized families. 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*. In order to construct such curves is needed to redefine equation 2 in terms of polynomial and find integers V and u satisfying:

$$DV^2 = 4q(u) - t(u)^2 \ , \tag{3}$$

for some fixed positive integer D and polynomials $q(u)$ and $t(u)$.

We are interested in "complete" families of interest in SNARK systems. That is, families for which equation 3 may be satisfied for any u, and in fact we can write V as a polynomial in u and the equation gives an equality of polynomials. Example of these complete families are BLS [BLS03], BN [BN06] and KSS [KSS08].

BLS. Barreto, Lynn and Scott [BLS03] generalized the Cocks–Pinch method by parameterizing t, r and q as polynomials. They constructed families by taking the polynomial $r(u)$ defining the number field $K = \mathbb{Q}[u]/(r(u))$ to be the k-th cyclotomic polynomial $\Phi_k(u)$, choosing the k-th root of unity to be $\xi_k \mapsto u$ in K (so $t(u) = 1 + u$), and using the fact that if $3 \mid k$ then $\sqrt{-3} \in K$. Particular choices for $k = 12$ and $k = 24$ yield two families of curves with good security/performance trade-offs, denoted respectively BLS12 and BLS24. The parameters are given in Table 2. Particular examples of curves proposed in SNARK contexts are BLS12-381 [Bow17], BLS12-377 [BCG+20], BLS24-315 and BLS24-317 [AHG23].

BN. Barreto and Naehrig presented a family of prime-order pairing-friendly elliptic curves with $k = 12$ and $D = 3$ (cf. Table 2). The construction is based on a result from [GMV07] and a lucky try in which the right-hand side of the CM equation happens to be a constant times a perfect square polynomial. However, it was suggested in [FST10, Example 6.8] that the BN construction can be viewed as a complete family on its own where $r(u)$ divides $\Phi_k(t(u) - 1)$. Particular examples of curves proposed in SNARK contexts are BN254 [BCTV14], BN383 [AHG23] and Pluto [Hop21].

KSS. Another strategy to build pairing-friendly constructions is to pick random small elements and take their minimal polynomials as the subgroup order polynomial $r(u)$. It is a non-cyclotomic polynomial such that K is isomorphic to the cyclotomic field $\mathbb{Q}(\xi_k)$. For well chosen embedding degrees $k = 16$ and $k = 18$, this yields the KSS16 and KSS18 families with $\rho = 5/4$ and $\rho = 4/3$ respectively (cf. Table 2). These families are well defined ($t(u)$ represents integers, $r(u)$ and $q(u)$ primes) only when $u \equiv \pm 25 \mod 70$ for KSS16 and $u \equiv 14 \mod 42$ for KSS18. Particular examples of curves proposed in SNARK contexts are KSS16-329 and KSS18-345 [AHG23].

4 Embedded curves

While SNARKs allow proving general-purpose computations, in many applications these computations revolve around proving some cryptographic operations such as hashings, encryptions, key exchanges or signatures. Many of these operations use elliptic curves distincts from the pairing-friendly curve used to instantiate the SNARK. As motivated in

Table 2: Polynomial parameters of BN, BLS12, BLS24, KSS16 and KSS18 families.

Family	k	D	ρ	$r(u)$	$q(u)$	$t(u)$
BN	12	-3	1	$36u^4+36u^3+18u^2+6u+1$	$36u^4+36u^3+24u^2+6u+1$	$6u^2+1$
BLS12	12	-3	$3/2$	u^4-u^2+1	$(u-1)^2r(u)/3+u$	$u+1$
BLS24	24	-3	$5/4$	u^8-u^4+1	$(u-1)^2r(u)/3+u$	$u+1$
KSS16	16	-1	$5/4$	$(u^8+48u^4+625)/61550$	$(u^{10}+2u^9+5u^8+48u^6+152u^5+$ $240u^4+625u^2+2398u+3125)/980$	$(2u^5+41u+35)/35$
KSS18	18	-3	$4/3$	$(u^6+37u^3+343)/343$	$(u^8+5u^7+7u^6+37u^5+188u^4+$ $259u^3+343u^2+1763u+2401)/21$	$(u^4+16u+7)/7$

the introduction, an embedded curve is required to express these computations natively. In other words, the modulo operations required during these 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.

To distinguish the polynomial parameters of the pairing-friendly curve $q(u), r(u)$ and $t(u)$ from those of the embedded curve, we will denote the parameters of the latter with the subscript "e" as in $q(u)_e, r(u)_e$ and $t(u)_e$.

To construct families of embedded curves one needs to construct simultaneously the pairing-friendly family (BLS, BN and KSS) curve $E/\mathbb{F}_{q(u)}$ of order $r(u)$ and the the embedded curve family curve $E_e/\mathbb{F}_{r(u)}$. Otherwise, once the seed is fixed for E nothing guarantees $r_e(u)$ to be a prime when evaluated in the same seed. This involves adding the extra constraints needed for the embedded curves and solving the CM equation 3.

4.1 Solving the CM equation

The approach for generating families of endomorphism-equipped curves requires solving the CM equation $DV^2 = 4q - t^2$, and then using the CM method to compute the curve equation coefficients. In our case, the CM equation takes on the following form:

$$DV_e(u)^2 = 4q_e(u) - t_e(u)^2 = 4r(u) - t_e(u)^2 \ . \tag{4}$$

There is currently no general method known for solving the Diophantine equations like 4 when the degree of $r(u)$ exceeds 4 (see also [BLS03, MNT01]). However, it is possible to leverage some of the known structure of $r(u)$ to derive a generic procedure. By construction of the parameterized families of pairing-friendly elliptic curves, we have $r(u) \in \mathbb{Z}[u]$ as an irreducible polynomial, such that $K \cong \mathbb{Q}[u]/(r(u))$ forms a number field. The success of our method for solving equation 4 depends heavily on the number field K. For example, if K is set to be the cyclotomic field $\mathbb{Q}(\xi_k)$ and $r(u)$ to be the k-th cyclotomic polynomial $\Phi_k(u)$ (as in BLS curves) or derived from it (as in BN and KSS curves), it is a standard result of the theory of cyclotomic fields that K contains $\sqrt{-1}$ if $4 \mid k$, $\sqrt{-2}$ if $8 \mid k$, and $\sqrt{\left(\frac{-1}{p}\right)p}$ for any odd prime p dividing k. More generically, $r(u) \in \mathbb{Z}[u]$ is an irreducible polynomial with a positive leading coefficient, such that K forms a number field containing $\sqrt{-D}$ and the cyclotomic field $\mathbb{Q}(\xi_k)$, as in the cases of Brezing–Weng curves [BW05]. At this point, we can utilize the fact that $r(u) = 0$ in K to rewrite equation 4 as:

$$DV_e(u)^2 + t_e(u)^2 = 0 \pmod{r(u)} \ . \tag{5}$$

Now, since K contains a square root of $-D$, there is at least one solution in polynomial form for equation 5. That is, there exists some polynomial $W_e(u)$ such that

$$W_e(u)^2 = -D \pmod{r(u)} \ .$$

At this point we have all the ingredients to generically solve equation 5. To find the $t_e(u)$ and $V_e(u)$ polynomials one can use the half-GCD algorithm by performing roughly half the Euclidean algorithm for computing the greatest common divisor.

5 Constructions

This section presents the families of embedded curves for BLS (in particular BLS12 and BLS24) and BN. It also gives some impossibility results related to KSS (in particular KSS16 and KSS18). All parameters and formulas are expressed in the form of polynomials with respect to the variable u.

First, we need to express $\sqrt{-D} \mod r(u)$ as a polynomial. From equation 5, we know that $(t_e/V_e)(u) = \sqrt{-D} \mod r(u)$. To recover $t_e(u)$ and $V_e(u)$, we need to express the polynomial $\sqrt{-D} \mod r(u)$ as a rational fraction of two polynomials of degree $\leq \deg(r)/2$. This can be done using the half-GCD algorithm. Next, we know from equation 1 that $r_e(u) = q_e(u) + 1 - t_e(u)$ and from equation 4 that $q_e(u) = (DV_e(u)^2 + t_e(u)^2)/4$. Hence the group order of the embedded family is

$$\begin{aligned} r_e(u) &= \frac{(DV_e(u)^2 + (t_e(u) - 2)^2)}{4} \quad , \quad \text{or simply} \\ r_e(u) &= r(u) + 1 - t_e(u). \end{aligned} \tag{6}$$

Finally, we check that the polynomial $r_e(u)$ is irreducible to give raise of a prime-order endomorphism-equipped embedded curves family [3]. If not, we test with the available twists. That is replacing $r_e(u)$ by the respective twists orders given in the end of the preliminaries section (see Sec. 2). We focus on the cases where $D = 3$ whenever they are available as they give an efficient endomorphism for the GLV technique. But we presents also other cases to expose the completeness of our approach.

5.1 BLS12

The BLS12 family has an order $r(u) = \Phi_{12}(u) = u^4 - u^2 + 1$. The quadratic subfields of $r(u)$ are $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{3})$.

Case $D = 3$. Equation 4 becomes $3V_e(u)^2 = 4\Phi_{12}(u) - t_e(u)^2$. Using SageMath [4], one is able to express $\sqrt{-3} \mod r(u)$ as the polynomial $2u^2 - 1$ and reconstruct $t_e(u)$ and $V_e(u)$ through the half-GCD algorithm as $2u^2 - 1$ and 1 respectively, which satisfies $t_e(u)^2 + 3V_e(u)^2 = 4r(u)$. Finally, equation 6 gives the family of order $r_e(u) = u^4 - 3u^2 + 3$ which is an irreducible polynomial.

Case $D = 4$. Similarly, $\sqrt{-4} \mod r(u)$ is the polynomial $2u^3$ and we can reconstruct $t_e(u) = -2u^2 + 2$ and $V_e(u) = -u$ which satisfy the equation $t_e(u)^2 + 4V_e(u)^2 = 4r(u)$. Finally, equation 6 sets the order to be $r_e(u) = u^4 + u^2$ which is a reducible polynomial. Luckily, among the quadratic and the two quartic twists, the quadratic one gives an irreducible polynomial $r_e(u) = u^4 - 3u^2 + 4$ that gives raise to a prime-order family.

5.2 BLS24

The BLS24 family has an order $r(u) = \Phi_{24}(u) = u^8 - u^4 + 1$ and has many quadratic subfields of $r(u)$. We give some examples with $D = 2, 3, 4$ and $D = 6$.

[3] so that $r_e(u)$ satisfies the Bunyakovsky conjecture, which states that such a polynomial produces infinitely many primes for infinitely many integers.

[4] https://www.sagemath.org/

Cases $D = 3$ and $D = 4$. These cases give similar results to the BLS12-based families with curves of prime orders $u^8 - 3u^4 + 3$ when $D = 3$ and $u^8 - 3u^4 + 4$ when $D = 4$.

Case $D = 2$. The polynomial $\sqrt{-2}$ mod $r(u)$ is $u^5 + u^3 - u$ and $t_e(u)$ and $V_e(u)$ can be either $u^4 - u^2 + 1$ and $-u^3 + u$ respectively or $2u^3 - 2u$ and $u^4 - u^2 + 1$ respectively. The first choice satisfies $t_e(u)^2 + 2V_e(u)^2 = r_e(u)$ so we multiply $t_e(u)$ and $V_e(u)$ by 2, which is a square root in K, so that the right hand of the equation becomes $4r_e(u)$. The resulting polynomial order is $r_e(u)$ is $u^8 - 3u^4 + 2u^2$ which is reducible. However, the quadratic twist gives an irreducible polynomial $r_e(u) = u^8 + u^4 - 2u^2 + 4$.

Case $D = 6$. Following the procedure and considering the curve and its quadratic twist, we find the following polynomial orders $r_e(u)$:

- $u^8 - 3u^4 + 6u^2$,
- $u^8 - u^4 + 2\sqrt{6}u^3 - 2\sqrt{6}u + 2$,
- $u^8 + u^4 - 6u^2 + 4$,
- $u^8 - u^4 - 2\sqrt{6}u^3 + 2\sqrt{6}u + 2$.

None of these polynomials is irreducible and hence there is no prime-order embedded curves for the $D = 6$ case.

5.3 BLS generalization

So far, we have not looked all the cases because each time we found a prime-order family. However, it is easy to give the formulas for all the twists orders and it is also easy to generalize the formulas derived above for all $i, j \geq 1$ for $k = 2^i 3^j$ as shown in Table 3. We focus on the cases $D = 3$ and $D = 4$ which give efficient endomorphisms to implement the GLV technique.

Table 3: Parameters of BLS and embedded curves for $k = 2^i 3^j, i, j \geq 1, 18 \nmid k$. Irreducible $r_e(u)$ polynomials are given in **bold**.

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

The GLV technique. At different security levels, BLS curves with $k = 2^i 3^j, i, j \geq 1, 18 \nmid k$ and $D = 3$ are usually the most efficient. In SNARK context, BLS12 and BLS24 stand out particularly. These curves have an efficient endomorphism $\phi : E \to E$ defined by $(x, y) \mapsto (\omega x, y)$ (and $\mathcal{O} \mapsto \mathcal{O}$) which acts on a point $P \in E(\mathbb{F}_q)[r]$ as $\phi(P) = [\lambda]P$ where $\lambda = u^{k/6} - 1$ and ω an element of order 3 in $\mathbb{F}_q$.

The embedded curves on BLS can have a similar efficient endomorphism for the $D = 3$ case. We focus on the cases where $r_e(u)$ is irreducible (given in **bold**), which are the only cases that would imply a prime-order embedded families. These families have the following orders $r_e(u)$:

- "order 1": $u^{k/3} - 3u^{k/6} + 3$,
- "order 2": $u^{k/3} + 3$ and
- "order 3": $u^{k/3} - 2u^{k/6} + 4$.

They also have an efficient endomorphism $\phi_e : E_e \to E_e$ defined by $(x, y) \mapsto (\omega_e x, y)$ (and $\mathcal{O} \mapsto \mathcal{O}$) which acts on a point $Q \in E_e(\mathbb{F}_r)[r_e]$ as $\phi_e(Q) = [\lambda_e]Q$ where ω_e and λ_e can be nicely expressed as the following polynomials:

- For "order 1":
$$\begin{aligned} \omega_e &= u^{k/6} - 1 \ , \\ \lambda_e &= u^{k/6} - 2 \ . \end{aligned}$$
- For "order 2":
$$\begin{aligned} \omega_e &= u^{k/6} - 1 \ , \\ \lambda_e &= (u^{k/6} - 1)/2 \ . \end{aligned}$$
- For "order 3":
$$\begin{aligned} \omega_e &= u^{k/6} - 1 \ , \\ \lambda_e &= u^{k/6}/2 - 1 \ . \end{aligned}$$

5.4 BN

The BN family has an order $r(u) = 36u^4 + 36u^3 + 18u^2 + 6u + 1$, which is a factor of $36\Phi_{12}(6u^2)$ ($r(u)$ divides $\Phi_{12}(t(u) - 1)$). The quadratic subfields of $r(u)$ are $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{3})$. BN curves are known to form a hybrid cycle which is a generalization of definition 1 in the sense that the pairing-friendly E curve is also an embedded curve of the E_e. This happens when $D = 3$ [AHG23, Sec. 5.4]. For completeness, we look at the case $D = 1$. This forms an embedded family but not a hybrid cycle family.

Case $D = 3$. The CM equation of the BN family is $t(u)^2 + 3V(u)^2 = 4q(u)$ with $t(u) = 6u^2 + 1$, $V(u) = 6u^2 + 4u + 1$ and $q(u) = r(u) + t(u) - 1$. It is a known result that the BN family forms a hybrid cycle and that the equation $(t(u) - 2)^2 + 3V(u)^2 = 4r(u)$ is satisfied. It turns out immediately that $t_e(u) = t(u) - 2 = 6u^2 - 1$, $V_e(u) = V(u) = 6u^2 + 4u + 1$ and $r_e(u) = q(u) = 36u^4 + 36u^3 + 12u^2 + 6u + 3$. E has an efficient endomorphism ϕ with $\lambda(u) = 36u^3 + 18u^2 + 6u + 1$ and $\omega(u) = 18u^3 + 18u^2 + 9u + 1$, and E_e has an efficient endomorphism ϕ_e with $\lambda_e = \omega$ and $\omega_e = \lambda$.

Case $D = 4$. Considering the curve, the quadratic twist and the two quartic twists, there are four possible orders $r_e(u)$:

- $36u^4 + 36u^3 + 30u^2 + 12u + 2$,
- $36u^4 + 36u^3 + 6u^2 + 2$,
- $36u^4 + 36u^3 + 18u^2 + 12u + 4$,
- $36u^4 + 36u^3 + 18u^2$.

All polynomials are irreducible except the quartic twist order $36u^4 + 36u^3 + 18u^2$. This case $D = 4$ yields to three prime-order families but they are more difficult to construct and less efficient compared to the straightforward $D = 3$ case.

5.5 KSS16

This family has an order $r(u) = (u^8 + 48u^4 + 625)/61250$. It is a non-cyclotomic polynomial such that K is isomorphic to the cyclotomic field $\mathbb{Q}(\xi_k)$. It can be computed as the minimal polynomial of a randomly chosen element of $\mathbb{Q}(\xi_k)$. The are many quadratic subfields of $r(u)$ with $D = 2, 8, -8, 16$ but none gives a prime-order embedded family. We explicit the case $D = 2$ as an example but the procedure remains the same for all cases to show the impossibility result.

Case $D = 2$. This gives the following families of irreducible polynomial orders $r_e(u)$: $(u^8 + 48u^4 - 4900u^2 + 61875)/61250$ and $(u^8 + 48u^4 + 4900u^2 + 61875)/61250$. The latter polynomial does not give integers when $u \equiv \pm 25 \mod 70$ (which is a requirement for KSS16 family definition) and the former does not give primes since in this case $r_e(u) \equiv 48 \mod 70$ which means the order is even.

5.6 KSS18

This family has an order $r(u) = (u^6 + 37u^3 + 343)/343$. The only quadratic subfield of $r(u)$ is $\mathbb{Q}(\sqrt{-3})$.

Case $D = 3$. The polynomial $\sqrt{-3} \mod r(u)$ is $-2u^3 - 37$ and the half-GCD gives $t_e(u) = 2u^3 + 37$ and $V_e(u) = 1$ or $t_e(u) = 3/1372$ and $V_e(u) = (u^3 + 37/2)/686$. These polynomials satisfy $t_e(u)^2 + 3V_e(u)^2 = 7r_e(u)$ but 7 is not a square in K. Thus, there is no embedded family that can be constructed on KSS18.

6 Examples

To demonstrate the feasibility of the method outlined in this paper, we present a new BLS12 curve, a new BLS24 curve and their prime-order endomorphism-equipped embedded curve. The new BLS12 and BLS24 curves satisfy the state-of-the-art criteria for efficiency and security, as per [AHG23], for pairing-based SNARK applications.

As explained in Section 4, one needs to construct simultaneously the pairing-friendly curve and the embedded curve so that the same seed results in $r(u)$, $q(u)$ and $r_e(u)$ primes. For already existing pairing-friendly curves (with an already fixed seed) it is unlikely that $r_e(u)$ is a prime.

We also give an example of a BN curve and its embedded curve (hybrid cycle) from the literature, which falls in the family framework that we presented. Unfortunately, KSS16 and KSS18 do not give prime-order families.

Remark 1. We conducted a retrospective analysis of our new method while examining the landscape of all existing pairing-friendly curves within the SNARK context and none has a prime-order endomorphism-equipped embedded curve. However, among the curves we examined, it appears that two of them (specifically, BLS12-440 and BLS12-442 as defined in [BD17]) have endomorphism-equipped embedded curves but with a composite order. BLS12-440 has a 292-bit r_e, while BLS12-442 has a 294-bit r_e both with a cofactor of 4, indicating that these curves can be expressed in Montgomery form. The comprehensive analysis and findings can be succinctly summarized and presented in the form of Table 4 in Appendix A.

A new BLS12-380 and its embedded curve. Both the BLS12 curve and its embedded curve have $D = 3$, the seed $u =$ `0xb504f33499580000` and the following parameters:

$$\begin{aligned} r &= \texttt{0x40000000e18820ac7e4ae010935bb29483628260db62ef544865b1c000000001} \\ q &= \texttt{0xaaaaaaae30cb2d5ddbe0944aad1b96788db962bb21454db5c12fca0d6c205a32} \\ &\quad \texttt{71689e66595fc8a55ac51118872aaab} \\ r_e &= \texttt{0x40000000e18820ac7e4ae010935bb2938362825f1852adfcd931154000000003} \\ q_e &= r \ . \end{aligned}$$

Here r is a 255-bit prime, q a 380-bit prime and r_e a 255-bit prime. The curves can be expressed in the Weierstrass model as

$$(E/\mathbb{F}_q) : y^2 = x^3 - 3 \ ,$$
$$(E_e/\mathbb{F}_r) : y^2 = x^3 + 11 \ .$$

E is efficient for large SNARK circuits because r has a high 2-adicity of 38, i.e. $2^{38} \mid r-1$ which makes Fast Fourier Transforms (FFT) very efficiently implementable over $\mathbb{F}_r$. E has also a $D = 3$ endomorphism ϕ with

$$\begin{aligned} &\lambda = u^2 - 1 = \texttt{0x80000000e18820abb79a4e3ffffffff} \\ &\omega = u^5 - 3u^4 + 3u^3 - u + 1 = \texttt{0x2d413ccdc5cf9b7c45bf2ad1a0852992a147ae13d27b2c} \\ &\quad \texttt{a95d0a9add9261c06cbcfb0ccb66a80001} \ . \end{aligned}$$

The embedded curve belongs to the family of order $u^4 - 3u^2 + 3$ from Section 5.1 (case $D = 3$). It also has a $D = 3$ endomorphism ϕ_e with

$$\begin{aligned} \lambda_e &= u^2 - 2 = \texttt{0x80000000e18820abb79a4e3fffffffe} \\ \omega_e &= \lambda = u^2 - 1 \ . \end{aligned}$$

A new BLS24-315 and its embedded curve. Both the BLS24 curve and its embedded curve have have a discriminant $D = 3$, the seed $u =$ `0xc5e03c00` and the following parameters:

$$\begin{aligned} r &= \texttt{0x209e54cfb3769a02a5b094de5d4faa86d42cb747e87cff8dcb1a3f0000000001} \\ q &= \texttt{0x67efc38cff28a453d57fe137cf351bea1f46dfcb855b607c0c3d1496948c72e9} \\ &\quad \texttt{781b5409bfabeab} \\ r_e &= \texttt{0x209e54cfb3769a02a5b094de5d4faa872f8e089adb810000000000000000000003} \\ q_e &= r \ . \end{aligned}$$

Here r is a 254-bit prime, q a 315-bit prime and r_e a 254-bit prime. The curves can be expressed in the Weierstrass model as

$$(E/\mathbb{F}_q) : y^2 = x^3 + 4 \ ,$$
$$(E_e/\mathbb{F}_r) : y^2 = x^3 + 11 \ .$$

E is efficient for large SNARK circuits because r has a high 2-adicity of 40. E has also an efficient endomorphism ϕ with

$\lambda = u^4 - 1 =$ `0x5b615152f304007234e5c0ffffffffff`
$\omega = u^9 - 3u^8 + 4u^7 - 4u^6 + 3u^5 - 2u^3 + 2u^2 - u + 1 =$ `0x19366972c4dcfbec26534fd271`
`efec374522fab7fe5e11aa7f2ec18fd2c206e9d63fc401` .

The embedded curve belongs to the family of order $u^8 + 3$ from sub-section 5.3 (case $D = 3$). It also has an efficient endomorphism ϕ_e with

$\lambda_e = (u^4 - 1)/2 =$ `0x104f2a67d9bb4d0152d84a6f2ea7d543c577acf6e74280391a72e080`
`00000001`
$\omega_e = \lambda = u^4 - 1$.

A BN446 and its embedded curve (Pluto and Eris). As shown in Subsection 5.4, all BN curves form a hybrid cycle which is a generalization of embedded curves. Hence there is no need to construct new BN curves. Taking any BN curve from the literature, we are able to construct embedded curves following our appraoch. Examples include Pluto-Eris [Hop21]

$E/\mathbb{F}_q : y^2 = x^3 + 57$ is a BN curve of order r, called Pluto;
$E_e/\mathbb{F}_r : y^2 = x^3 + 57$ is an embedded curve of order $r_e = q$, called Eris, with
$q = 36u^4 + 36u^3 + 24u^2 + 6u + 1$ and
$r = 36u^4 + 36u^3 + 18u^2 + 6u + 1, \text{for } u = -(2^{110} + 2^{60} + 2^{39} + 2^{35} - 2^{31})$.

The field size of Pluto is 446 bits to target 128-bit security level and naturally leaves a larger security margin for Eris. Both curves have the high 2-adicity of 32 for r and are again equipped the fast endomorphisms ϕ and ϕ_e with:

$\lambda = \omega_e = 36u^3 + 18u^2 + 6u + 1 =$ `-0x9000000000006c000392a0001afee1c9500792ae`
`3039253e641ba35817a29ffaf50be000032cffffffff`
$\omega = \lambda_e = 18u^3 + 18u^2 + 9u + 1 =$ `-0x480000000000360001c950000d7ee0e4a803c956d`
`01c903d720dc8ad8b38dffaf50c100004c37ffffff` .

7 Conclusions

In this paper, we introduced a generic algorithm to construct families of prime-order endomorphism-equipped embedded curves. To our best knowledge, this led to the first embedded families. We used our algorithm to construct families over BLS and BN pairing-friendly curves and gave some impossibility results on constructing such families over the KSS16 and KSS18 curves. Moreover, to demonstrate the approach, we proposed new instantiations of BLS12 and BLS24 pairing-friendly curves alongside their prime-order endomorphism-equipped embedded curves. The new proposed curves meet the state-of-the-art requirements for efficient elliptic curves for proof systems.

However, the Bandersnatch curve found in the literature (embedded over BLS12-381) does not fall into any of the families we presented in this work. It has a discriminant $D = 8$ while the quadratic subfields of $r(u) = \phi_{12}(u)$ do not include $\mathbb{Q}(\sqrt{-8})$, hence its existence cannot be explained within our framework. We hope that this work will encourage the community to further investigate the odd existence of such an embedded curve and, likely, another embedded family into which it would fall.

Acknowledgments. We express our gratitude to the anonymous reviewers for their critical review of the manuscript and for providing detailed and insightful comments, particularly to the reviewer who pointed out a generic method to solve equation 4, which ultimately became a subsection of this manuscript. We would also like to thank Diego Aranha, Luca De Feo, Robert Granger, Aurore Guillevic, Gottfried Herold, Dimitri Koshelev, Simon Masson and Michael Scott for fruitful discussions.

A Embedded curves on existing curves

Table 4: Security of embedded curves on existing BLS curves.

Bitlength of the largest prime dividing r_e		
	$D = 3$	$D = 4$
BLS12-381 [Bow17]	236-bit 154-bit 130-bit	74-bit
BLS12-377 [BCG$^+$20]	126-bit 142-bit 130-bit	114-bit
BLS12-379 [EHG22]	130-bit 104 180-bit	132-bit
BLS12-440 [BD17]	? [†] 190-bit 244-bit	**292-bit**
BLS12-442 [BD17]	82-bit 238-bit 198-bit	**294-bit**
BLS12-446 [GS21]	128-bit 82-bit 114-bit	176-bit
BLS12-461 [BD17]	**272-bit** [*] ? [†] 110-bit	112-bit
BLS24-315 [EHG22]	120-bit 104-bit 170-bit	154-bit
BLS24-317 [EHG22]	76-bit 180-bit 82-bit	240-bit

References

[AHG23] Diego F. Aranha, Youssef El Housni, and Aurore Guillevic. A survey of elliptic curves for proof systems. *DCC*, 91(11):3333–3378, 2023. doi:10.1007/s10623-022-01135-y.

[AM93] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp*, 61:29–68, 1993.

[Ame05] American National Standards Institute, Inc. ANSI X9.62 public key cryptography for the financial services industry: the elliptic curve digital signature algorithm (ECDSA), November 16, 2005. URL: https://standards.globalspec.com/std/1955141/ANSI%20X9.62.

[*] While this curve is 128-bit secure it has a relatively large cofactor $c = 76635610837$.

[†] A prime factor of a hard to factorize composite number.

[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*, pages 947–964. IEEE Computer Society Press, May 2020. doi:10.1109/SP40000.2020.00050.

[BCTV14] Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, and Madars Virza. Succinct non-interactive zero knowledge for a von neumann architecture. In Kevin Fu and Jaeyeon Jung, editors, *USENIX Security 2014*, pages 781–796. USENIX Association, August 2014.

[BD17] Razvan Barbulescu and Sylvain Duquesne. Updating key size estimations for pairings. Cryptology ePrint Archive, Report 2017/334, 2017. https://eprint.iacr.org/2017/334.

[BDL+12] Daniel J. Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, and Bo-Yin Yang. High-speed high-security signatures. *Journal of Cryptographic Engineering*, 2(2):77–89, September 2012. doi:10.1007/s13389-012-0027-1.

[BLS03] Paulo S. L. M. Barreto, Ben Lynn, and Michael Scott. Constructing elliptic curves with prescribed embedding degrees. In Stelvio Cimato, Clemente Galdi, and Giuseppe Persiano, editors, *SCN 02*, volume 2576 of *LNCS*, pages 257–267. Springer, Heidelberg, September 2003. doi:10.1007/3-540-36413-7_19.

[BN06] Paulo S. L. M. Barreto and Michael Naehrig. Pairing-friendly elliptic curves of prime order. In Bart Preneel and Stafford Tavares, editors, *SAC 2005*, volume 3897 of *LNCS*, pages 319–331. Springer, Heidelberg, August 2006. doi:10.1007/11693383_22.

[Bow17] Sean Bowe. BLS12-381: New zk-SNARK elliptic curve construction, 2017. https://electriccoin.co/blog/new-snark-curve/.

[BPH+23] Gautam Botrel, Thomas Piellard, Youssef El Housni, Ivo Kubjas, and Arya Tabaie. Consensys/gnark: v0.9.0, February 2023. doi:10.5281/zenodo.5819104.

[BW05] Friederike Brezing and Annegret Weng. Elliptic curves suitable for pairing based cryptography. *DCC*, 37(1):133–141, 2005. doi:10.1007/s10623-004-3808-4.

[CP01] Clifford Cocks and RGE Pinch. Identity-based cryptosystems based on the weil pairing. *Unpublished manuscript*, 170, 2001.

[EHG22] Youssef El Housni and Aurore Guillevic. Families of SNARK-friendly 2-chains of elliptic curves. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part II*, volume 13276 of *LNCS*, pages 367–396. Springer, Heidelberg, May / June 2022. doi:10.1007/978-3-031-07085-3_13.

[FST10] David Freeman, Michael Scott, and Edlyn Teske. A taxonomy of pairing-friendly elliptic curves. *Journal of Cryptology*, 23(2):224–280, April 2010. doi:10.1007/s00145-009-9048-z.

[GLV01] Robert P. Gallant, Robert J. Lambert, and Scott A. Vanstone. Faster point multiplication on elliptic curves with efficient endomorphisms. In Joe Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 190–200. Springer, Heidelberg, August 2001. doi:10.1007/3-540-44647-8_11.

[GMV07] Steven D. Galbraith, James F. McKee, and P. C. Valença. Ordinary abelian varieties having small embedding degree. *Finite Fields Their Appl.*, 13(4):800–814, 2007. doi:10.1016/j.ffa.2007.02.003.

[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.

[HBHW] Daira Hopwood, Sean Bowe, Taylor Hornby, and Nathan Wilcox. Zcash protocol. https://zips.z.cash/protocol/protocol.pdf.

[Hop21] Daira Hopwood. Pluto-eris hybrid cycle of elliptic curves, 2021. https://github.com/daira/pluto-eris.

[KSS08] Ezekiel J. Kachisa, Edward F. Schaefer, and Michael Scott. Constructing Brezing-Weng pairing-friendly elliptic curves using elements in the cyclotomic field. In Steven D. Galbraith and Kenneth G. Paterson, editors, *PAIRING 2008*, volume 5209 of *LNCS*, pages 126–135. Springer, Heidelberg, September 2008. doi:10.1007/978-3-540-85538-5_9.

[KZM$^+$15] Ahmed Kosba, Zhichao Zhao, Andrew Miller, Yi Qian, Hubert Chan, Charalampos Papamanthou, Rafael Pass, abhi shelat, and Elaine Shi. C∅c∅: A framework for building composable zero-knowledge proofs. Cryptology ePrint Archive, Report 2015/1093, 2015. https://eprint.iacr.org/2015/1093.

[MNT01] Atsuko Miyaji, Masaki Nakabayashi, and Shunzo Takano. Characterization of elliptic curve traces under FR-reduction. In Dongho Won, editor, *ICISC 00*, volume 2015 of *LNCS*, pages 90–108. Springer, Heidelberg, December 2001.

[MSZ21] Simon Masson, Antonio Sanso, and Zhenfei Zhang. Bandersnatch: a fast elliptic curve built over the BLS12-381 scalar field. Cryptology ePrint Archive, Report 2021/1152, 2021. https://eprint.iacr.org/2021/1152.

[RCB16] Joost Renes, Craig Costello, and Lejla Batina. Complete addition formulas for prime order elliptic curves. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part I*, volume 9665 of *LNCS*, pages 403–428. Springer, Heidelberg, May 2016. doi: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 Vélu. Isogénies entre courbes elliptiques. *Comptes Rendus de l'Académie des Sciences de Paris*, 273:238–241, 1971.

[zc] zcash contributors. The halo2 zero-knowledge proving system. https://zcash.github.io/halo2/.

[Zca] Zcash. What is Jubjub? https://web.archive.org/web/20230201163714/https://z.cash/technology/jubjub/.