# On cycles of pairing-friendly abelian varieties

Maria Corte-Real Santos[1]*, Craig Costello[2], and Michael Naehrig[2]

[1] University College London, London, UK
maria.santos.20@ucl.ac.uk
[2] Microsoft Research, Redmond, USA
{craigco,mnaehrig}@microsoft.com

**Abstract.** One of the most promising avenues for realising scalable proof systems relies on the existence of 2-cycles of pairing-friendly elliptic curves. Such a cycle consists of two elliptic curves $\mathcal{E}/\mathbb{F}_p$ and $\mathcal{E}'/\mathbb{F}_q$ that both have a low embedding degree and also satisfy $q = \#\mathcal{E}(\mathbb{F}_p)$ and $p = \#\mathcal{E}'(\mathbb{F}_q)$. These constraints turn out to be rather restrictive; in the decade that has passed since 2-cycles were first proposed for use in proof systems, no new constructions of 2-cycles have been found.

In this paper, we generalise the notion of cycles of pairing-friendly elliptic curves to study cycles of pairing-friendly *abelian varieties*, with a view towards realising more efficient pairing-based SNARKs. We show that considering abelian varieties of dimension larger than 1 unlocks a number of interesting possibilities for finding pairing-friendly cycles, and we give several new constructions that can be instantiated at any security level.

**Keywords:** Zero-knowledge proofs, SNARKs, recursive proof composition, abelian varieties, supersingular curves, trace zero varieties.

## 1 Introduction

**Pairing-based proof systems.** Non-interactive zero-knowledge proofs are powerful cryptographic primitives that offer an array of applications (see [60] for a comprehensive, up-to-date survey). Beginning with the works of Groth, Ostrovsky and Sahai [30,27,31], a large body of research has focussed on constructing instances of these proofs that additionally achieve the *succinctness* property. *Zero-knowledge succinct non-interactive arguments of knowledge* (zk-SNARKs) provide a computationally sound proof that is both cheap to verify and small in size compared to the circuit describing the statement. Groth's breakthrough zk-SNARK constructions were the first of their kind that achieved constant proof sizes [28,29]. Prior proposals gave proofs whose size depended on the size of the circuit, but Groth was able to overcome this dependency by utilising the power of bilinear pairings. Groth's pairing-based proof systems are now among the most popular instantiations of SNARKs, both in theory and in practice [60].

**Recursive SNARK composition via MNT cycles.** In 2014, Ben-Sasson, Chiesa, Tromer and Virza [6] realised efficient pairing-based zk-SNARKs via a new approach. They built on prior works proposing the *recursive composition* of proofs [61,8] to give the first implementation of a zk-SNARK that achieves such recursive proof composition at scale. The core ingredient was a *2-cycle* of *pairing-friendly* elliptic curves, i.e., $\mathcal{E}/\mathbb{F}_p$ and $\mathcal{E}'/\mathbb{F}_q$, where $q = \#\mathcal{E}(\mathbb{F}_p)$, $p = \#\mathcal{E}'(\mathbb{F}_q)$, and both $\mathcal{E}$ and $\mathcal{E}'$ have low embedding degrees. At that time, only one such pairing-friendly cycle was known in the literature: the 2-cycle of Miyaji, Nakabayashi and Takano (MNT) curves [45] that was pointed out by Karabina and Teske [39, Proposition 1]. Indeed, in [6], the authors used an instance of the MNT 2-cycle with $p \approx q \approx 2^{298}$ to bring their recursive proof composition to life.

*Supported by EPSRC grant EP/S022503/1. Part of this work was done while Maria was an intern at Microsoft Research.

While the elliptic curve discrete logarithm problem (ECDLP) on a well-chosen elliptic curve with a prime order of around $2^{298}$ is conjectured to offer around 150 bits of security, the implementation of the MNT cycle in [6] could only claim a security level of around 80 bits. The reason for this discrepancy is that both $\mathcal{E}/\mathbb{F}_p$ and $\mathcal{E}'/\mathbb{F}_q$ are pairing-friendly, meaning that the ECDLP on both curves can instead be solved more efficiently as a finite field discrete logarithm problem (DLP) in $\mathbb{F}_{p^k}^\times$ or $\mathbb{F}_{q^{k'}}^\times$, where $k$ and $k'$ are small, positive integers [44,21]. The MNT cycle has $(k, k') = (4, 6)$, so the easiest place to solve discrete logarithms is in $\mathbb{F}_{p^4}^\times$; in [6], the authors argued that $p \approx 2^{298}$ was enough to ensure that the DLP in $\mathbb{F}_{p^4}^\times$ offered around 80 bits of security. However, when scaling up to the modern standard of 128-bit security, Guillevic [33] analysed the state-of-the-art in algorithms for the finite field DLP and concluded that the MNT cycle must have $p \approx q \approx 2^{1000}$. In other words, $p$ and $q$ are around four times the bitlength they would need to be (to achieve $2^{128}$ ECDLP security) if cycles with larger embedding degrees were known. Working with such large $p$ and $q$ dramatically hampers the efficiency of recursive composition [60, §18].

**The search for new cycles.** Due to the inherent drawbacks of the MNT cycle, it is desirable to find alternative constructions of pairing-friendly 2-cycles. Unfortunately, the papers in the literature that investigate this possibility have been unable to find any new such 2-cycles, and have almost exclusively presented impossibility results. The 2019 paper by Chiesa, Chua and Weidner [16] showed that pairing-friendly 2-cycles with $(k, k')$ in the set $\{(5, 10), (8, 8), (12, 12)\}$ do not exist, and that cycles within the Freeman [18] and Barreto-Naehrig [4] families also do not exist. The 2023 paper by Bellés-Muñoz, Jiménez Urroz and Silva [5] extended this work and addressed some of the open problems posed in [16]. For example, they proved that no curve from *any* of the known pairing-friendly families can be in a 2-cycle in which the other curve has an embedding degree $k \leq 22$.

The failure to find any new 2-cycles has caused authors and designers of SNARK protocols to relax the cycle requirement and instead look for 2-*chains* of pairing-friendly curves; i.e., two pairing-friendly curves $\mathcal{E}/\mathbb{F}_p$ and $\mathcal{E}'/\mathbb{F}_q$ with $p \mid \#\mathcal{E}'(\mathbb{F}_q)$ (rather than $p = \#\mathcal{E}'(\mathbb{F}_q)$ and $q = \#\mathcal{E}(\mathbb{F}_p)$ as in a 2-cycle). The 2022 paper by El Housni and Guillevic [35] classifies the state-of-the-art in the direction of efficient 2-chains, and it includes parameterised families of 2-chains that link well-known families into 2-chains of pairing-friendly curves. With a chain of pairing-friendly curves, however, the corresponding SNARKs cannot perform the *unbounded* recursive composition of proofs envisioned by Ben-Sasson, Chiesa, Tromer and Virza [6]. Instead, they can only perform a bounded proof bootstrapping, as was first implemented in Geppetto [17], a zero-knowledge SNARK built for verifiable computations.

There are a number of SNARKs based around elliptic curve cycles where the pairing-friendly requirement has been relaxed on one or both of the curves. For example, the Halo proof system of Bowe, Grigg and Hopwood [12] avoids the trusted setup that is inherent to pairing-based SNARKs and instead uses a 2-cycle of non-pairing-friendly curves. The work of Silverman and Stange [55] shows that these cycles are plentiful, and in practice we find they are therefore much easier to construct than cycles where both curves are pairing-friendly. Even in the case where only one of the curves in the 2-cycle needs to be pairing-friendly, this relaxation allows for relatively straightforward constructions, e.g. one can partner a non-pairing-friendly curve with a pairing-friendly curve from any one of the MNT, Freeman and BN families. We refer to the survey paper by Aranha, El Housni and Guillevic [1] for more examples of 2-chains or non-pairing-friendly cycles that can be found in the wild.

**This work.** Motivated by the lack of performant pairing-friendly cycles of *elliptic curves*, we initiate the search for pairing-friendly cycles of *abelian varieties*[3]. We say (see Definition 1) that two pairing-friendly abelian varieties $\mathcal{A}/\mathbb{F}_{p^u}$ and $\mathcal{B}/\mathbb{F}_{q^v}$ are a *cycle*, denoted $\mathcal{A} \rightleftharpoons \mathcal{B}$, if $p \mid \#\mathcal{B}(\mathbb{F}_{q^v})$ and $q \mid \#\mathcal{A}(\mathbb{F}_{p^u})$. In contrast to the cycles of pairing-friendly elliptic curves $\mathcal{E}/\mathbb{F}_p$ and $\mathcal{E}'/\mathbb{F}_q$ with

[3] Abelian varieties are a generalisations of elliptic curves, which are themselves the most simple instances of abelian varieties used in cryptography: an elliptic curve is an abelian variety of dimension 1.

$p = \#\mathcal{E}'(\mathbb{F}_q)$ and $q = \#\mathcal{E}(\mathbb{F}_p)$ that were proposed in [6] and studied in [16,5], our definition has three relaxations:

(i) $\mathcal{A}$ and $\mathcal{B}$ can be abelian varieties of any dimension;
(ii) $\mathcal{A}$ and $\mathcal{B}$ can be defined over extension fields; and
(iii) $p$ and $q$ need only divide the respective group orders of $\mathcal{B}$ and $\mathcal{A}$, not be equal to them.

To our knowledge, this paper is the first to explore (i) and (ii). In the original paper proposing cycles for proof systems, it is already mentioned that the generalisation in (iii) is permitted [6, §3.1], but the authors did not need to allow for it since they were using the prime order MNT construction. In the search for more pairing-friendly cycles of elliptic curves defined over prime fields, Chiesa, Chua and Weidner [16] also considered (iii) by allowing for either curves in the cycle to have composite order. However, they went on to prove that such cycles cannot exist when the elliptic curves $\mathcal{E}$ and $\mathcal{E}'$ are defined over prime fields.

All three relaxations above have their own benefits and drawbacks. As we show in this paper, the main benefit of the loosened requirements in (i), (ii) and (iii) is that they open up a wide range of possibilities for finding cycles. It is worth pointing out that we do not need to exploit all three relaxations simultaneously in order to find cycles of pairing-friendly curves. For example, the combination of (ii) and (iii) already allows us to define a new cycle of pairing-friendly elliptic curves $\mathcal{E}/\mathbb{F}_{p^2} \rightleftharpoons \mathcal{E}'/\mathbb{F}_q$, which have $p^2 = \#\mathcal{E}'(\mathbb{F}_q)$ and $q = \#\mathcal{E}(\mathbb{F}_{p^2})$. In this case, however, the *cryptographic exponents*[4] of $\mathcal{E}$ and $\mathcal{E}'$ are even smaller than the embedding degrees of the MNT cycle. It is only when we allow (i), and consider higher dimensional abelian varieties, that we are able to find cycles containing cryptographic exponents larger than 6 and present possibilities that may pique the interest of practitioners.

The *ideal scenario* for implementing a recursive SNARK is a 2-cycle of two prime order elliptic curves, both of which have (the same) small embedding degree that perfectly balances the ECDLP and DLP securities in all groups involved. The relaxations (i), (ii) and (iii) are all suboptimal compared to this ideal scenario. For example, the relaxation given by (i) is not as appealing as in the classical context of (hyper-)elliptic curve cryptography, where allowing higher-dimensional abelian varieties enables the use of smaller base fields for the same conjectured (H)ECDLP complexity. This presents interesting trade-offs between working with a more complex group law but over finite fields of smaller characteristic. Cycles for zk-SNARK applications, however, require the field characteristics to correspond to (sub)group sizes. To keep the DLP in these groups hard enough, the characteristics are forced to be at least $2\lambda$ bits to achieve $\lambda$ bits of security against Pollard's $\rho$ algorithm [48]. Despite these drawbacks, we hope that the relaxations above can pave the way to more performant cycles than the suboptimal MNT cycle, in particular since cycles realising the above ideal scenario have shown to be elusive and may not exist at all [5].

As we discuss at length in Section 3, the generalisation to abelian varieties opens up a vast number of options for obtaining cycles. In §3.1 we make four choices that narrow the scope of our search. On the one hand, they allow us to explore a meaningful fraction of this uncharted territory within a framework that produces a variety of new pairing-friendly cycles. On the other hand, these restrictions each come with their own drawbacks. The most significant of these imposes that all of our constructions have $\mathcal{B}/\mathbb{F}_{q^v}$ as an elliptic curve with cryptographic exponent 1. Unlike the case where the curves are defined over prime fields, however, this does not force $q$ to be large; the main goal of Section 5 is to pursue constructions where $v$ is as large as possible so that the size of $q$ can be made smaller at the same security level. We start there by giving two constructions for $\mathcal{B}$ that form cycles with all of the constructions for $\mathcal{A}$ we present in this paper: the first has $\mathcal{B}$ as an ordinary elliptic curve with $v = 1$, the second has $\mathcal{B}$ as a supersingular curve with $v = 2$. We then move to ordinary curves $\mathcal{B}$ that are paired with a specific construction of $\mathcal{A}$, starting with $v = 3$ before describing a more general construction for all $v \in 2\mathbb{N}$.

We explore multiple options for $\mathcal{A}/\mathbb{F}_{p^u}$, all of which are supersingular. This begins with two elliptic curve constructions in Section 4 for which the cryptographic exponents are $3/2$ and 3,

[4] For pairing-friendly abelian varieties defined over extension fields, the field of definition of the pairing can be a proper subfield of the field extension given by the embedding degree. The cryptographic exponent is the ratio of the sizes of this field and the field of definition of the variety.

respectively. In Section 6, we move into dimension 2 and present two constructions where $\mathcal{A}/\mathbb{F}_{p^u}$ is a supersingular abelian surface; these have cryptographic exponents 3 and 6, respectively. In Section 7 we present our main construction using the work of Rubin and Silverberg [49] to find cycles where $\mathcal{A}/\mathbb{F}_{p^u}$ can be of arbitrarily high dimension $g = 2^\ell$ for $\ell \geq 0$, and of arbitrarily high cryptographic exponent $3 \cdot 2^{g-1}$. In §7.2 we give a number of cryptographically sized examples that illustrate the potential of $\mathcal{A}$ being able to have arbitrarily high cryptographic exponent. The last example is geared towards the 128-bit security level: it uses a 256-bit $p$ and a genus 4 abelian variety $\mathcal{A}/\mathbb{F}_{p^2}$ with cryptographic exponent 24 to give comparable security to an MNT cycle with 992-bit $p$ and $q$.

In Section 8, we survey the literature for optimisations that can accelerate SNARKs based on our cycles. These include optimisations for the pairings themselves, as well as hashing routines and exponentations in all three pairing groups. We also touch on optimisations that are specific to SNARKs, like those that can accelerate large multiscalar multiplications; finally, we show that (unlike the MNT cycle) our cycles can be instantiated on parameters with very large 2-*adicity* – see §8.4.

**Towards optimal 2-cycles.** An optimal cycle $\mathcal{A}/\mathbb{F}_{p^u} \rightleftharpoons \mathcal{B}/\mathbb{F}_{q^v}$ at the $\lambda$-bit security level would be one where $p \approx q \approx 2^{2\lambda}$, and where the $q$-Weil pairing of $\mathcal{A}$ and the $p$-Weil pairing of $\mathcal{B}$ both map into extension fields just large enough to achieve $\lambda$ bits of security against the state-of-the-art in DLP attacks. In this work we are able to give constructions of $\mathcal{A}$ where $p \approx 2^{2\lambda}$ is indeed as small as possible. If we were able to partner this with a $\mathcal{B}/\mathbb{F}_{q^v}$ for which $v$ can be arbitrarily large, then we could hope to obtain $p \approx 2^{2\lambda}$ and $q \approx 2^{4\lambda}$ ($q$ is at least as large as $p^2$ in our framework), but unfortunately the only values of $v$ for which we managed to construct such a $\mathcal{B}$ are $v = 1$ and $v = 2$. However, we feel it is worth pointing out that cycles with arbitrarily large values of $v$ do *exist* within our framework; the only reason we have been so far unable to construct them is because our attempts have produced a CM equation with a discriminant that is too large, which makes computing the curve coefficients of cryptographically sized instances infeasible (see Section 2). Nevertheless, contrary to the negative results that exist for 2-cycles of ordinary elliptic curves [16,5], it is encouraging to know that cycles where $p$ and $q$ can be much closer to optimal (irrespective of the security level) are out there.

## 2 Preliminaries

In this section, we provide some relevant background about elliptic curves and abelian varieties. We assume basic knowledge about elliptic curves and their use in cryptography. For a more general exposition we refer to Silverman [54].

Throughout this paper, for a prime number $p$ we let $\mathbb{F}_{p^k}$ denote the finite field with $p^k$ elements, where $k \in \mathbb{N}$. We let $\overline{\mathbb{F}}_{p^k}$ denote its algebraic closure.

**Elliptic curves.** Let $p > 3$ be prime and $u \in \mathbb{N}$. An elliptic curve $\mathcal{E}/\mathbb{F}_{p^u}$ is *supersingular* if $\mathcal{E}(\overline{\mathbb{F}}_{p^u})$ has no points of order $p$, otherwise it is *ordinary*. The number of $\mathbb{F}_{p^u}$-rational points on $\mathcal{E}$ is $\#\mathcal{E}(\mathbb{F}_{p^u}) = p^u + 1 - t$, where $t$ is the *trace of Frobenius* and $|t| \leq 2\sqrt{p^u}$ according to Hasse's theorem.

The following theorem (due to Waterhouse [63]) tells us precisely which values of the *trace* $t$ correspond to $\mathcal{E}$ being supersingular.

**Theorem 1 ([63]).** *There exists a supersingular curve over $\mathbb{F}_{p^u}$ with trace $t$ if and only if $t$ satisfies one of the following conditions:*

- *$u$ is even and*
  - *(i)* $t = \pm 2\sqrt{p^u}$,
  - *(ii)* $t = \pm\sqrt{p^u}$ *and* $p \not\equiv 1 \bmod 3$,
  - *(iii)* $t = 0$ *and* $p \not\equiv 1 \bmod 4$;

– *$u$ is odd and*

*(iv)* $t = 0$.

Over a given finite field $\mathbb{F}_{p^u}$, we can take any $t$ that satisfies one of the conditions in Theorem 1, and input it alongside $p$ and $u$ into Bröker's algorithm [13] to obtain a supersingular elliptic curve with trace $t$.

For any $t$ with $|t| \leq 2\sqrt{p^u}$ that does not satisfy the conditions above, there exists an ordinary elliptic curve over $\mathbb{F}_{p^u}$ with trace $t$. If we wish to construct it, we can attempt to use the theory of *complex multiplication* (CM), which proceeds by taking $D$ as the largest squarefree divisor of $4p^u - t^2$, i.e., setting

$$DV^2 = 4p^u - t^2, \tag{1}$$

where $D$ is the squarefree integer commonly referred to as the CM *discriminant.* If $D$ is not too large, we can compute the *Hilbert class polynomial* $H_D(x) \in \mathbb{F}_{p^u}[x]$ corresponding to $D$ [57]. The roots of $H_D(x)$ are the $j$-invariants of curves with trace $t$, so we can take any such root $j$. If $j = 0$, the curve we seek is $\mathcal{E}\colon y^2 = x^3 + 1$ or one of its sextic twists; if $j = 1728$, it is $\mathcal{E}\colon y^2 = x^3 + x$ or one of its quartic twists, otherwise we can output the curve $\mathcal{E}\colon y^2 = x^3 + ax - a$ with $a = -27j/(4(j - 1728))$ or its quadratic twist [14].

**Abelian varieties.** The natural generalisation of elliptic curves to higher dimensions are principally polarised (p.p.) abelian varieties. Let $\mathcal{A}/\mathbb{F}_{p^u}$ be a p.p. abelian variety. We say that $\mathcal{A}$ is *simple* if it is not $\mathbb{F}_{p^u}$-isogenous to a product of lower dimensional abelian varieties, and is *supersingular* if it is $\overline{\mathbb{F}}_{p^u}$-isogenous to a product of supersingular elliptic curves.[5] From this point onwards, we will assume our abelian varieties come equipped with a principal polarisation, and drop the 'p.p.' for clarity.

The following result concerning supersingular abelian varities over $\mathbb{F}_{p^u}$ will prove useful when we arrive at §7 and construct cycles involving such $\mathcal{A}$. Before stating the result, we define a *supersingular $p^u$-Weil number* to be a complex number of the form $\sqrt{p^u}\zeta$, where $\zeta$ is a root of unity [49, §1].

**Theorem 2 ([49,34,58,64]).** *Let $\mathcal{A}/\mathbb{F}_{p^u}$ be a simple supersingular abelian variety and let $P(x)$ be the characteristic polynomial of the $p^u$-power Frobenius endomorphism of $\mathcal{A}$. Then:*

*(i)* $P(x) = G(x)^e$*, where* $G(x) \in \mathbb{Z}[x]$ *is a monic irreducible polynomial and* $e \in \{1, 2\}$*;*

*(ii) the roots of $G$ are supersingular $p^u$-Weil numbers;*

*(iii)* $\mathcal{A}(\mathbb{F}_{p^u}) \cong (\mathbb{Z}_{G(1)})^e$*, unless $p^u$ is non-square and either*

*(a)* $p \equiv 3 \bmod 4$*,* $\dim(\mathcal{A}) = 1$*, and* $G(x) = x^2 + p^u$*, or*

*(b)* $p \equiv 1 \bmod 4$*,* $\dim(\mathcal{A}) = 2$*, and* $G(x) = x^2 - p^u$*;*

*in these exceptional cases,* $\mathcal{A}(\mathbb{F}_{p^u}) \cong (\mathbb{Z}_{G(1)})^a \times (\mathbb{Z}_{\frac{G(1)}{2}} \times \mathbb{Z}_2)^b$ *with non-negative integers $a$ and $b$ such that $a + b = e$;*

*(iv)* $\#\mathcal{A}(\mathbb{F}_{p^u}) = P(1)$.

The roots of $G$ are called the *$p^u$-Weil numbers for $\mathcal{A}$.* The dimension of $\mathcal{A}$ is $\dim(\mathcal{A}) = \deg(P)/2 = e \cdot \deg(G)/2$.

**The cryptographic exponent.** Let $p$ be prime and let $\mathcal{A}/\mathbb{F}_{p^u}$ be an abelian variety. Since we are interested in scenarios where $\mathcal{A}$ is pairing-friendly, it is important (for the sake of MOV security [44]) to know the minimum degree of the extension field of $\mathbb{F}_p$ where the Weil pairing is defined. If $\ell \mid \#\mathcal{A}(\mathbb{F}_{p^u})$ for some prime $\ell > 5$, then we typically define the *embedding degree* of $\mathcal{A}$ with respect to $\ell$ as the smallest natural number $k$ such that $\ell \mid (p^u)^k - 1$. Rubin and Silverberg additionally define the *cryptographic exponent* $c_{\mathcal{A}}$ of $\mathcal{A}$ [49, Definition 3], which (for large enough

[5] Here, we emphasise that 'isogenous' should be understood in the context of abstract abelian varieties, i.e., discarding their principal polarisation.

$\ell$, as will be the case in this work) is such that $(p^u)^{c_\mathcal{A}} = p^r$ [49, Theorem 7], where $r$ is the smallest integer such that $\ell \mid p^r - 1$. For abelian varieties that are defined over extension fields, the cryptographic exponent therefore captures the ratio between the field of definition of $\mathcal{A}$ and the field where the $\ell$-Weil pairing is defined. Note that if $u > 1$, $r$ can be smaller than $uk$.

**The theorem of Rubin and Silverberg.** Supersingular elliptic curves $\mathcal{E}/\mathbb{F}_{p^u}$ will play a fundamental role in the constructions we present, but when $p > 3$ they can only have cryptographic exponents $c_\mathcal{E} \leq 3$. In Section 7, we will use the following theorem (due to Rubin and Silverberg [49, Theorem 17]) to produce higher dimensional abelian varieties $\mathcal{A}/\mathbb{F}_{p^u}$ whose cryptographic exponents are much larger. The larger the cryptographic exponent is, the smaller $p^u$ can be chosen, making arithmetic in the field of definition more efficient while still guaranteeing high enough DLP security in the finite field group.

**Theorem 3 ([49]).** *Let $\mathcal{E}/\mathbb{F}_{p^u}$ be a supersingular elliptic curve, $\pi$ be a $p^u$-Weil number for $\mathcal{E}$ that is not a rational number. Fix $r \in \mathbb{N}$ with $\gcd(r, 2pc_\mathcal{E}) = 1$. Then there is a supersingular abelian variety $\mathcal{A}/\mathbb{F}_{p^u}$ such that:*

*(i)* $\dim(\mathcal{A}) = \varphi(r)$*;*
*(ii) for every primitive $r$-th root of unity $\zeta$, $\pi\zeta$ is a $p^u$-Weil number for $\mathcal{A}$;*
*(iii) $c_A = rc_\mathcal{E}$; and*
*(iv) there is a natural identification of $\mathcal{A}(\mathbb{F}_{p^u})$ with the subgroup of $\mathcal{E}(\mathbb{F}_{p^{ur}})$*

$$\{Q \in \mathcal{E}(\mathbb{F}_{p^{ur}}) \colon \mathrm{Tr}_{\mathbb{F}_{p^{ur}}/\mathbb{F}_{p^{ur/\ell}}}(Q) = \mathcal{O} \quad \textit{for every prime } \ell \mid r\}.$$

# 3 The high-level strategy

We start this section by formalising our generalisation of cycles to abelian varieties in Definition 1. As we discussed in Section 1, this opens up a large number of possibilities for obtaining such cycles. In §3.1 we discuss the restrictions that are imposed throughout the rest of the paper. These choices allow us to explore a meaningful fraction of this uncharted territory whilst adhering to a consistent framework that produces a variety of new pairing-friendly cycles. Nevertheless, we believe it is highly likely that the most performant cycles of pairing-friendly abelian varieties are yet to be discovered, so we endeavour to point out the drawbacks of our restrictions by shedding light on what is lost by adhering to them. We conclude this section in §3.2 with a high-level discussion on the security of our approach.

**Definition 1.** *Two abelian varieties $\mathcal{A}/\mathbb{F}_{p^u}$ and $\mathcal{B}/\mathbb{F}_{q^v}$ are a* pairing-friendly cycle*, denoted $\mathcal{A} \rightleftharpoons \mathcal{B}$, if and only if*

*(i) $p \mid \#\mathcal{B}(\mathbb{F}_{q^v})$;*
*(ii) $q \mid \#\mathcal{A}(\mathbb{F}_{p^u})$;*
*(iii) $\mathcal{A}$ is pairing-friendly with respect to $q$; and*
*(iv) $\mathcal{B}$ is pairing-friendly with respect to $p$.*

The use of the term "pairing-friendly" in (iii) and (iv) refers to $\mathcal{A}$ and $\mathcal{B}$ having small cryptographic exponents, e.g. $c_\mathcal{A}, c_\mathcal{B} \leq 50$.

## 3.1 Choices and restrictions

The framework within which we search for cycles of pairing-friendly abelian varieties is based on the following four choices:

1. **$\mathcal{A}$ and $\mathcal{B}$ are simple.** In other words, $\mathcal{A}$ (resp. $\mathcal{B}$) is not $\mathbb{F}_{p^u}$-isogenous (resp. $\mathbb{F}_{q^v}$-isogenous) to a product of lower dimensional abelian varieties. We argue that this is a natural restriction: if $\mathcal{A} \rightleftharpoons \mathcal{B}$ and $\mathcal{A}$ was $\mathbb{F}_{p^u}$-isogenous to $\mathcal{A}_1 \times \mathcal{A}_2$, then it must be that at least one of $\mathcal{A}_1$ and $\mathcal{A}_2$ is pairing-friendly with respect to $q$, so (without loss of generality) assume that this is $\mathcal{A}_1$. Then we could instead take our cycle to be $\mathcal{A}_1 \rightleftharpoons \mathcal{B}$, rather than $\mathcal{A} \rightleftharpoons \mathcal{B}$, without losing anything. Note, however, that we do not insist that either is *absolutely simple*; in fact, our restriction below in 2 necessarily says that $\mathcal{A}$ is $\overline{\mathbb{F}}_{p^u}$-isogenous (as an abstract variety) to a product of lower-dimensional abelian varieties.

2. **$\mathcal{A}$ is supersingular of dimension $g \geq 1$.** One restriction we make in this work is that we only allow the dimension of $\mathcal{A}$ (and not both $\mathcal{A}$ and $\mathcal{B}$) to be larger than 1 (more on this in 4 below). In terms of the myriad of pairing-friendly curves that existed prior to the interest in cycles, *ordinary* pairing-friendly abelian varieties of dimension larger than 1 were notoriously difficult to construct, and even the best examples (e.g. [19]) were ultimately not competitive with their genus 1 counterparts. On the other hand, explicit constructions of various *supersingular* pairing-friendly abelian varieties of dimension greater than 1 are readily found in the literature (e.g. [24]), and for our purposes they come with several advantages. While supersingular elliptic curves over large characteristic fields have cryptographic exponents of at most 3, the works of Galbraith [22] and Rubin-Silverberg [49] showed how the cryptographic exponents of supersingular abelian varieties grow steadily with the dimension. Moreover, crucial to our construction of pairing-friendly cycles is the fact that the coefficients in the $p^u$-Weil polynomial $P(x)$ of $\mathcal{A}/\mathbb{F}_{p^u}$ are all multiples of $p$ [22, Theorem 2], except for the leading coefficient which is 1. Together with Theorem 2(iv), this implies that $P(1) \equiv 1 \bmod p$, which (in conjunction with the choice we make in 3 below) allows us to define an abelian variety $\mathcal{B}$ that is pairing-friendly with respect to $p$ with ease.

3. **$\mathcal{A}$ is of prime order $q$.** This restriction is perhaps the most impactful one we impose, both in terms of the way it enables us to construct cycles in a straightforward way, and in terms of the optimality it sacrifices. Setting $q = \#\mathcal{A}(\mathbb{F}_{p^u})$ means $q \equiv 1 \bmod p$ (from 2), which in turn means that $\mathcal{B}$ will be pairing-friendly with respect to $p$. On the other hand, it forces the cryptographic exponent on this side to be $c_{\mathcal{B}} = 1$, which is the main cause of the suboptimality we mention above. The way we work towards overcoming the drawback of $c_{\mathcal{B}} = 1$ is to work with values of $v$ that are as large as possible, such that the $p$-torsion of $\mathcal{B}$ is defined over $\mathbb{F}_{q^v}$, i.e., $\mathcal{B}[p] \subseteq \mathcal{B}(\mathbb{F}_{q^v})$, but not over any smaller extension of $\mathbb{F}_q$. This in turn allows us to work with smaller values of $q$, which in some sense mimics what we would be able to do with a larger cryptographic exponent $c_{\mathcal{B}}$, but still comes with the drawback that *all* of the $p$-torsion is defined over $\mathbb{F}_{q^v}$. Moreover, all of the constructions in this paper have $\#A(\mathbb{F}_{p^u}) = P(1) = f(p)$, where $f$ is a polynomial of degree at least 2; thus, imposing that $q = P(1)$ means that $q$ will always have at least twice the bitlength of $p$.

4. **$\mathcal{B}$ has dimension 1.** Subject to 3 and the implication that $c_{\mathcal{B}} = 1$, having $\mathcal{B}$ as an elliptic curve allows for the most straightforward construction of a cycle and for the most efficient arithmetic. In Section 5 we give a variety of different possibilities for defining $\mathcal{B}/\mathbb{F}_{q^v}$; these include $\mathcal{B}$ being both ordinary and supersingular, and explicit constructions for $v = 1$, $v = 3$, as well as a construction that works for every $v \in 2\mathbb{N}$.

### 3.2 Security

We now give a preliminary discussion of the security of our constructions. From a high level, the security analysis of the pairing-friendly cycle $\mathcal{A} \rightleftharpoons \mathcal{B}$ can be conducted by independently analysing the security of the pairing-friendly constructions $\mathcal{A}$ and $\mathcal{B}$. In other words, to our knowledge there are no additional security concerns introduced by virtue of $\mathcal{A}$ and $\mathcal{B}$ being in a 2-cycle with one another.

**The security of supersingular varieties.** In terms of discrete logarithm based cryptosystems, the security story of supersingular elliptic curves has featured a number of highs and lows. Initially, they began as popular choices for instantiating ECC based on the ease of computing their cardinality and thus finding secure instances. In the early 1990's, however, the MOV/Frey-Rück attacks [44,21] used bilinear pairings to transport supersingular ECDLP instances into finite field DLP instances that were substantially easier to solve. Due to their low embedding degrees that enabled these attacks, supersingular curves were thought to be avoided at all costs, but this changed at the turn of the century with the birth of pairing-based cryptography [51,37,11]. Pairings were no longer entirely a destructive tool, and protocols that used their bilinearity property in a constructive way required small embedding degrees so that the pairings can be computed efficiently. Nevertheless, supersingular elliptic curves could still only achieve embedding degrees up to 6 [44], and researchers began noticing that this was too small to achieve optimal pairing-based cryptosystems. Subsequently, a number of constructions of ordinary pairing-friendly curves with higher embedding degrees began to emerge [3,4], and pairings based on supersingular curves soon became a suboptimal instantiation of the past. Nevertheless, as we discussed in §3.1 above, higher-dimensional supersingular varieties afford larger cryptographic exponents, which is what we exploit to find pairing-friendly cycles in this work. As long as the corresponding ECDLPs and finite field DLPs are conjecturally secure, and as long as the corresponding protocol does not require DDH to be hard (more on this below), there is no known drawback to using supersingular curves. Or, as Koblitz and Menezes [41, §7.1] put it: *"Despite the customary preference for nonsupersingular elliptic curves, there is no known reason why a nonsupersingular curve with small embedding degree k would have any security advantage over a supersingular curve with the same embedding degree"*.

**The security of high-dimensional abelian varieties.** Koblitz first proposed higher dimensional abelian varieties for discrete logarithm based cryptography in 1989 [40]. At that time, there was seemingly no difference in the asymptotic difficulty of two well-chosen prime order (H)ECDLP groups, regardless of the genus of the underlying abelian variety. Fast forwarding 25 years, the conventional wisdom nowadays is that only genus 1 and 2 varieties are safe for (H)ECC. The reason for avoiding genus 3 and above is that state-of-the-art index calculus attacks [26] on the HECDLP become asymptotically faster than generic algorithms like Pollard's $\rho$ algorithm [48]. This inference is based on the types of parameterisations and trade-offs that would be considered optimal for HECC. For example, the Jacobian variety corresponding to a well-chosen genus 3 curve $\mathcal{C}/\mathbb{F}_q$ of (almost) prime order $r$ will have $r = O(q^3)$. The attack of Gaudry, Thomé, Thériault and Diem [26] solves the HECDLP in the Jacobian group of any hyperelliptic curve with $g \geq 3$ in time $\tilde{O}(q^{2-2/g})$, so in this case would run in expected time $\tilde{O}(q^{4/3})$. This is a substantial improvement over the $\tilde{O}(q^{3/2})$ complexity of a generic attack like Pollard's $\rho$ algorithm.

In the case of the higher-dimensional varieties proposed in this paper, however, we are dealing with a rather different setup than that of optimised HECC instances. In particular, our varieties $\mathcal{A}/\mathbb{F}_{p^u}$ and $\mathcal{B}/\mathbb{F}_{q^v}$ being in a cycle forces us to choose both our field characteristics $p$ and $q$ to be large enough such that generic discrete logarithm attacks against the respective groups of these orders are hard. In other words, HECDLP index calculus algorithms like [26] will never be the best attack against our cycle constructions, because its respective complexities are always at least $\tilde{O}(p)$ and $\tilde{O}(q)$, which is much worse than the $\tilde{O}(p^{1/2})$ or $\tilde{O}(q^{1/2})$ Pollard-$\rho$ complexities.

**Security within SNARK ecosystems.** A note of caution is warranted when using supersingular varieties for proof systems and zk-SNARKs. Supersingular elliptic curves have distortion maps, meaning the Weil pairing can be used as a Diffie-Hellman oracle resulting in the decisional Diffie-Hellman problem (DDH) being efficiently solvable [62]. This is problematic, for instance, for the inner pairing product commitment of the Dory polynomial commitment scheme [42], which relies on the hardness of DDH in both pairing argument groups. Many other constructions, including the line of pairing-based SNARKs following Groth's constructions [28,29] are unaffected by the symmetric pairing.

The assumption that underpins the security of pairing-based SNARKs is typically (a variant of) the $Q$-DLog assumption: for an asymmetric pairing $e\colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, it asks to find the scalar $x$ given the tuples

$$(P_1, [x]P_1, \ldots, [x^Q]P_1) \in \mathbb{G}_1^{Q+1} \quad \text{and} \quad (P_2, [x]P_2, \ldots, [x^Q]P_2) \in \mathbb{G}_2^{Q+1}.$$

For a symmetric pairing $e\colon \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$, it asks to find the scalar $x$ given the tuple

$$(P, [x]P, \ldots, [x^Q]P) \in \mathbb{G}^{Q+1}.$$

In both cases one can use the pairing to produce the tuple of elements

$$(z, z^x, z^{x^2}, \ldots, z^{x^{2Q}}) \in \mathbb{G}_T^{2Q+1},$$

where $z = e(P_1, P_2)$ in the asymmetric case and $z = e(P, P)$ in the symmetric case. Thus, any known security issues posed by, say, Cheon's attack [15], apply equivalently to both the ordinary and supersingular scenarios.

### 3.3 Roadmap

The remainder of the paper is organised as follows. We start in Section 4 by presenting our simplest construction for $\mathcal{A}$: a supersingular elliptic curve. In Section 5 we present multiple possibilities for constructing $\mathcal{B}$, which include both ordinary and supersingular elliptic curves. We then return to $\mathcal{A}$ in the next two sections: Section 6 gives constructions where $\mathcal{A}$ is a supersingular abelian surface that is the Jacobian of a genus-2 curve, and Section 7 exploits the theorem of Rubin and Silverberg to increase the cryptographic exponents of $\mathcal{A}$ by working in the trace zero subvarieties of supersingular elliptic curves over larger extension fields.[6] Finally, in Section 8 we point readers to a number of optimisations from the literature that can be used to accelerate SNARKs based on our new cycles.

## 4 $\mathcal{A}$ is a supersingular elliptic curve

We begin describing our construction of cycles with our simplest option for $\mathcal{A}$: a supersingular elliptic curve. Proposition 1 in §4.1 gives a construction for $c_{\mathcal{A}} = 3/2$ and Proposition 2 in §4.2 gives a construction with $c_{\mathcal{A}} = 3$. Together, they form the basis for the remainder of the constructions of $\mathcal{A}$ in the paper.

Recall from Restriction 3 in §3.1 that we seek $\mathcal{A}/\mathbb{F}_{p^u}$ such that $\#\mathcal{A}(\mathbb{F}_{p^u})$ is prime. Over fields of large prime characteristic $p$, the only possibility for supersingular elliptic curves to have prime order arise as Category (ii) of Theorem 1, which excludes $p \equiv 1 \bmod 3$. For the remainder of this paper, we impose that $p \equiv 2 \bmod 3$.

Both constructions work over $\mathbb{F}_{p^u}$ for $u \in 2\mathbb{Z}$: the first involves curves of order $p^u + p^{u/2} + 1$ while the second produces curves of order $p^u - p^{u/2} + 1$. With $p \equiv 2 \bmod 3$, imposing that the order is prime means that $u \in 2\mathbb{Z}$ but $u \notin 4\mathbb{Z}$ in the first case, and $u \in 4\mathbb{Z}$ in the second case.

We immediately follow Proposition 1 with Example 1, which is continued through the rest of the paper. To find one small sized example that could continue through Sections 6 and 7, we chose the prime $p = 1373$ so that $p \equiv 2 \bmod 3$ and for which $p^2 + p + 1$, $p^4 - p^2 + 1$, and $p^8 - p^4 + 1$ are also prime (the reason for this will become clear once we arrive at Theorem 4).[7]

[6] The reason we jump from $\mathcal{A}$ to $\mathcal{B}$ and then back to $\mathcal{A}$ is so the reader does not have to wait past Section 5 to see constructions of cycles $\mathcal{A} \rightleftharpoons \mathcal{B}$.

[7] The first such odd prime was $p = 5$, so for the sake of taking something slightly larger (e.g. to avoid issues in dimensions larger than 1), we took the next one: $p = 1373$.

### 4.1 $\mathcal{A}$ has cryptographic exponent $c_{\mathcal{A}} = 3/2$

We are now ready to present our construction for $\mathcal{A}$ with cryptographic exponent $c_{\mathcal{A}} = 3/2$.

**Proposition 1.** *Let $p \equiv 2 \bmod 3$ be an odd prime and $u$ be twice an odd integer such that $q = p^u + p^{u/2} + 1$ is also prime. Let $\alpha$ be a primitive element of $\mathbb{F}_{p^u}$. The elliptic curve $\mathcal{A}/\mathbb{F}_{p^u}$ with trace $t = -p^{u/2}$ satisfies the following:*

1. *It has the form $\mathcal{A}/\mathbb{F}_{p^u} : y^2 = x^3 + a$, where $a \in \{\alpha, \alpha^5\}$;*
2. *is supersingular;*
3. *has order $\#\mathcal{A}(\mathbb{F}_{p^u}) = q$; and*
4. *has cryptographic exponent $c_{\mathcal{A}} = 3/2$ with respect to $q$.*

*Proof.* Claim 3 is immediate from $t = -p^{u/2}$, Claim 2 is due to Waterhouse [63, Theorem 4.1(3)], and Claim 4 is due to Galbraith [10, Theorem IX.20]. The form of the curve in Claim 1 is due to Morain [47], where $a \in \{\alpha, \alpha^5\}$ follows from $\mathcal{A}$ having prime order. □

*Example 1.* Let $p = 1373$ and $u = 2$, and observe that $q = p^2 + p + 1 = 1886503$ is prime. Write $\mathbb{F}_{p^2} = \mathbb{F}_p(\lambda)$ where $\lambda^2 = 2$. The element $\alpha = \lambda + 12$ is primitive in $\mathbb{F}_{p^2}$ and the curve $\mathcal{A}/\mathbb{F}_{p^2} : y^2 = x^3 + \alpha$ is supersingular with prime order $q = \#\mathcal{A}(\mathbb{F}_{p^2})$. The cryptographic exponent of $\mathcal{A}$ with respect to $q$ is $c_{\mathcal{A}} = 3/2$, meaning the order-$q$ Weil pairing maps to a subgroup of $\mathbb{F}_{p^3}^{\times}$.

### 4.2 $\mathcal{A}$ has cryptographic exponent $c_{\mathcal{A}} = 3$

To obtain a larger cryptographic exponent, we look to find $\mathcal{A}/\mathbb{F}_{p^u}$ with group order $p^u - p^{u/2} + 1$. This leads us to the following proposition.

**Proposition 2.** *Let $p \equiv 2 \bmod 3$ be an odd prime and $u$ be twice an even integer such that $q = p^u - p^{u/2} + 1$ is also prime. Let $\alpha$ be a primitive element of $\mathbb{F}_{p^u}$. The elliptic curve $\mathcal{A}/\mathbb{F}_{p^u}$ with trace $t = p^{u/2}$ satisfies the following:*

1. *It has the form $\mathcal{A}/\mathbb{F}_{p^u} : y^2 = x^3 + a$, where $a \in \{\alpha, \alpha^5\}$;*
2. *is supersingular;*
3. *has order $\#\mathcal{A}(\mathbb{F}_{p^u}) = q$; and*
4. *has cryptographic exponent $c_{\mathcal{A}} = 3$ with respect to $q$.*

*Proof.* The proof is identical to that of Proposition 1, except for Claim 4 which is also due to Galbraith [10, Theorem IX.20]. □

*Example 1 (continued).* Let $p = 1373$ and take $u = 4$. Observe that $q = p^4 - p^2 + 1 = 3553709461513$ is prime. Write $\mathbb{F}_{p^2} = \mathbb{F}_p(\lambda)$ with $\lambda^2 = 2$ and $\mathbb{F}_{p^4} = \mathbb{F}_{p^2}(\mu)$ with $\mu^2 = \lambda$. The element $\alpha = (788\lambda + 1236)\mu + (740\lambda + 183)$ is primitive in $\mathbb{F}_{p^4}$ and the curve $\mathcal{A}/\mathbb{F}_{p^4} : y^2 = x^3 + \alpha$ is supersingular with prime order $q = \#\mathcal{A}(\mathbb{F}_{p^4})$. The cryptographic exponent of $\mathcal{A}$ with respect to $q$ is $c_{\mathcal{A}} = 3$, meaning the order-$q$ Weil pairing maps to a subgroup of $\mathbb{F}_{p^{12}}^{\times}$.

## 5 $\mathcal{B}$ is an elliptic curve of cryptographic exponent $c_{\mathcal{B}} = 1$

We now turn to exploring several options for instantiating $\mathcal{B}/\mathbb{F}_{q^v}$ for $v \geq 1$. These will be used to form cycles with the options for $\mathcal{A}/\mathbb{F}_{p^u}$ already presented in Section 4, as well as those that will come in Sections 6 and 7. Recall from §3.1(4) that we restrict $\mathcal{B}$ to have dimension 1 in this paper, i.e., $\mathcal{B}$ is an elliptic curve.

All of the $\mathcal{A}/\mathbb{F}_{p^u}$ in Sections 4, 6 and 7 have $\#\mathcal{A}(\mathbb{F}_{p^u}) = p^u \pm p^{u/2} + 1$ with $u \in 2\mathbb{N}$. Recall from §3.1(3) that we will set $q = p^u \pm p^{u/2} + 1$, which immediately implies that $c_{\mathcal{B}} = 1$. If $v = 1$, this means that $q$ must be large enough that discrete logarithms in $\mathbb{F}_q^{\times}$ are hard. The way we work towards overcoming this drawback and decrease the size of $q$ is to try to increase $v$, i.e., increase the field over which (the $p$-torsion of) $\mathcal{B}$ is minimally defined. In the case of $q = p^u \pm p^{u/2} + 1$ with arbitrary $u$, we find constructions with $v = 1$ such that $\mathcal{B}/\mathbb{F}_q$ is ordinary (§5.1) and with $v = 2$ such that $\mathcal{B}/\mathbb{F}_{q^2}$ is supersingular (§5.2). When $q = p^2 + p + 1$ (i.e., $u = 2$), we find a construction for $v = 3$ where $\mathcal{B}/\mathbb{F}_{q^3}$ is ordinary (§5.3), and a general construction that works for any even $v$ (§5.4).

We note that cycles between $\mathcal{A}/\mathbb{F}_{p^u}$ and ordinary curves $\mathcal{B}/\mathbb{F}_{q^v}$ exist for $q = p^u + p^{u/2} + 1$ with arbitrary $u \in 2 + 4\mathbb{Z}$ and arbitrary $v \in 2\mathbb{Z}$. However, the key of our methods is to ensure $\mathcal{B}/\mathbb{F}_{q^v}$ has small CM discriminant. In this way, we can exploit the CM method to obtain an *explicit* construction of the elliptic curve, which cannot be guaranteed for $v > 2$.

### 5.1 $\mathcal{B}$ is ordinary and defined over $\mathbb{F}_q$

We start with a construction for an ordinary elliptic curve $\mathcal{B}/\mathbb{F}_q$ that can be used to form a cycle with any of the $\mathcal{A}$ constructions in this paper.

**Proposition 3.** *Let $p \equiv 2 \bmod 3$ be an odd prime and $u$ be an even integer such that $q = p^u \pm p^{u/2} + 1$ is also prime, and let $\beta$ be a primitive element of $\mathbb{F}_q$. The elliptic curve $\mathcal{B}/\mathbb{F}_q$ with trace $t = \pm p^{u/2} + 2$*

1. *has the form $\mathcal{B}/\mathbb{F}_q \colon y^2 = x^3 + b$, where $b \in \{\beta, \beta^5\}$;*
2. *is ordinary;*
3. *has order $\#\mathcal{B}(\mathbb{F}_q) = p^u$;*
4. *has cryptographic exponent $c_{\mathcal{B}} = 1$ with respect to $p$; and*
5. *is in a cycle $\mathcal{A}/\mathbb{F}_{p^u} \rightleftharpoons \mathcal{B}/\mathbb{F}_q$,
where $\mathcal{A}/\mathbb{F}_{p^u}$ is the curve from Proposition 1 if $q = p^u + p^{u/2} + 1$,
and $\mathcal{A}/\mathbb{F}_{p^u}$ is the curve from Proposition 2 if $q = p^u - p^{u/2} + 1$.*

*Proof.* Claims 2 and 3 follow immediately from $t = \pm p^{u/2} + 2$, and 4 follows from observing that $q \equiv 1 \bmod p$. Substituting $q$ and $t$ into the CM equation $4q = t^2 + Dy^2$ yields $D = 3$ and $y = \pm p^u$. The six traces satisfying the CM equation with $q$, $D$ and $y$ as above are $\{\pm t, \pm(t{+}3y)/2, \pm(t{-}3y)/2\}$ [32, §A.14.2.3]. Direct substitution reveals that the only possible trace that gives a group of order divisible by $p^u$ is $t$. Now, since $2 \nmid \#\mathcal{B}(\mathbb{F}_q)$ (resp. $3 \nmid \#\mathcal{B}(\mathbb{F}_q)$), $b$ cannot be a cube (resp. square) in $\mathbb{F}_q$; thus, $b$ is precisely one of $\beta$ or $\beta^5$, which proves 1. Finally, Claim 5 follows from the respective group orders and cryptographic exponents of $\mathcal{A}/\mathbb{F}_{p^u}$ and $B/\mathbb{F}_q$, and Definition 1. □

*Example 1 (continued).* We continue with $p = 1373$, $u = 2$, and the prime $q = p^2 + p + 1 = 1886503$. The element $\beta = 3$ is primitive in $\mathbb{F}_q$ and the curve $\mathcal{B}/\mathbb{F}_q \colon y^2 = x^3 + b$ with $b = \beta^5 = 243$ has trace $p + 2 = 1375$ and group order $\#\mathcal{B}(\mathbb{F}_q) = p^2$. In particular, $\mathcal{B}(\mathbb{F}_q) \cong \mathbb{Z}_p \times \mathbb{Z}_p$, and the order-$p$ Weil pairing maps to a subgroup of $\mathbb{F}_q^\times$.

When $q = p^u \pm p^{u/2} + 1$, there are other ordinary curves $\mathcal{B}'/\mathbb{F}_{q^v}$ with $v \in \{2, 3, 6\}$ that form cycles with the $\mathcal{A}$ from Section 4, and whose $p$-torsion only become rational over $\mathbb{F}_{q^v}$. Moreover, they are also (isomorphic to elliptic curves) of the form $y^2 = x^3 + b$, and since they have $v > 1$, it seems they would be preferable to the construction of $\mathcal{B}/\mathbb{F}_q$ above. However, as we show below, these all correspond to the twists of the $\mathcal{B}$ in Proposition 3. From a constructive point of view, this means that if we were to use any of them to construct a cycle $\mathcal{A}/\mathbb{F}_{p^u} \rightleftharpoons \mathcal{B}'/\mathbb{F}_{q^v}$, the $p$-Weil pairing would be a map $\mathcal{B}'(\mathbb{F}_{q^v})[p] \times \mathcal{B}'(\mathbb{F}_{q^v})[p] \to \mathbb{F}_{q^v}^\times$, which would seemingly give finite field discrete logarithm instances in $\mathbb{F}_{q^v}^\times$. However, an attacker could use the twisting morphism $\Psi \colon \mathcal{B}' \to \mathcal{B}$ to instead work with the $p$-Weil pairing $\mathcal{B}(\mathbb{F}_q)[p] \times \mathcal{B}(\mathbb{F}_q)[p] \to \mathbb{F}_q^\times$, and solve discrete logarithms in $\mathbb{F}_q^\times$. Thus, in terms of being able to decrease $q$, we do not gain anything in using one of the twists of $\mathcal{B}/\mathbb{F}_q$.

**Proposition 4.** *Let $\mathcal{B}_1/\mathbb{F}_q \colon y^2 = x^3 + b$ be the curve defined by Proposition 3. None of the five curves $\mathcal{B}_z/\mathbb{F}_q \colon y^2 = x^3 + b^z$ with $z \in \{2, 3, 4, 5, 6\}$ have $\mathbb{F}_q$-rational $p$-torsion, but are all $\overline{\mathbb{F}}_q$-isomorphic to $\mathcal{B}_1$. In particular, $\mathcal{B}_4$ is $\mathbb{F}_{q^2}$-isomorphic to $\mathcal{B}_1$; $\mathcal{B}_3$ and $\mathcal{B}_5$ are $\mathbb{F}_{q^3}$-isomorphic to $\mathcal{B}_1$; and, $\mathcal{B}_2$ and $\mathcal{B}_6$ are $\mathbb{F}_{q^6}$-isomorphic to $\mathcal{B}_1$.*

*Proof.* It follows from Silverman [54, Proposition X.5.4] that the curves $\mathcal{B}_1/\mathbb{F}_q$ and $\mathcal{B}_4/\mathbb{F}_q$ are quadratic twists of one another and are thus isomorphic over $\mathbb{F}_{q^2}$; the curves $\mathcal{B}_1/\mathbb{F}_q$, $\mathcal{B}_3/\mathbb{F}_q$ and $\mathcal{B}_5/\mathbb{F}_q$ are cubic twists of each other and are thus isomorphic over $\mathbb{F}_{q^3}$; and, all six curves $\mathcal{B}_z/\mathbb{F}_q$ with $z \in \{1, \ldots, 6\}$ are sextic twists of each other and thus become isomorphic over $\mathbb{F}_{q^6}$. □

*Example 1 (continued).* Take $q = 1886503$ and $b = 243$ as above. The curves $\mathcal{B}_z/\mathbb{F}_q \colon y^2 = x^3 + b^z$ with $z \in \{1, \ldots, 6\}$ are such that $\mathcal{B}_1(\mathbb{F}_q) \cong \mathbb{Z}_{1373} \times \mathbb{Z}_{1373}$, $\mathcal{B}_2(\mathbb{F}_q) \cong \mathbb{Z}_{1883757}$, $\mathcal{B}_3(\mathbb{F}_q) \cong \mathbb{Z}_2 \times \mathbb{Z}_{942566}$, $\mathcal{B}_4(\mathbb{F}_q) \cong \mathbb{Z}_{1887879}$, $\mathcal{B}_5(\mathbb{F}_q) \cong \mathbb{Z}_{1889251}$, and $\mathcal{B}_6(\mathbb{F}_q) \cong \mathbb{Z}_{1374} \times \mathbb{Z}_{1374}$. However, we have $\mathcal{B}_1(\mathbb{F}_{q^2}) \cong \mathcal{B}_4(\mathbb{F}_{q^2})$, $\mathcal{B}_1(\mathbb{F}_{q^3}) \cong \mathcal{B}_3(\mathbb{F}_{q^3}) \cong \mathcal{B}_5(\mathbb{F}_{q^3})$, and $\mathcal{B}_z(\mathbb{F}_{q^6}) \cong \mathcal{B}_{z'}(\mathbb{F}_{q^6})$ for all $z, z' \in \{1, \ldots, 6\}$.

### 5.2 $\mathcal{B}$ is supersingular and defined over $\mathbb{F}_{q^2}$

We now present the construction for a supersingular elliptic curve $\mathcal{B}/\mathbb{F}_{q^2}$ that can be used to form a cycle with our constructions for $\mathcal{A}$.

**Proposition 5.** *Let $p > 3$ be a prime and $u$ be an even integer such that $q = p^u \pm p^{u/2} + 1$ is also prime. The elliptic curve $\mathcal{B}/\mathbb{F}_{q^2}$ with trace $t = 2q$*

1. *is supersingular;*
2. *has group structure $\mathcal{B}(\mathbb{F}_{q^2}) \cong \mathbb{Z}_{p^{u/2}(p^{u/2}\pm 1)} \times \mathbb{Z}_{p^{u/2}(p^{u/2}\pm 1)}$;*
3. *has cryptographic exponent $c_{\mathcal{B}} = 1$ with respect to $p$; and*
4. *is in a cycle $\mathcal{A}/\mathbb{F}_{p^u} \rightleftharpoons \mathcal{B}/\mathbb{F}_q$,*
   *where $\mathcal{A}/\mathbb{F}_{p^u}$ is the curve from Proposition 1 if $q = p^u + p^{u/2} + 1$,*
   *and $\mathcal{A}/\mathbb{F}_{p^u}$ is the curve from Proposition 2 if $q = p^u - p^{u/2} + 1$.*

*Proof.* Refer to Galbraith [10, Theorem IX.20] for Claims 1, 2 and 3. Claim 4 follows from the respective group orders and cryptographic exponents of $\mathcal{A}/\mathbb{F}_{p^u}$ and $\mathcal{B}/\mathbb{F}_{q^2}$, and Definition 1. □

*Example 1 (continued).* We continue with $p = 1373$, $u = 2$, and $q = p^2 + p + 1 = 1886503$ as above. Let $\mathbb{F}_{q^2} = \mathbb{F}_q(\xi)$ with $\xi^2 + 1 = 0$. On input of $\mathbb{F}_{q^2}$ and $t = 2q$, Bröker's algorithm [13] outputs the supersingular elliptic curve $\mathcal{B}/\mathbb{F}_{q^2} \colon y^2 = x^3 - (4\xi + 3)x$ with trace $t$ such that $\mathcal{B}(\mathbb{F}_{q^2}) \cong \mathbb{Z}_{p(p+1)} \times \mathbb{Z}_{p(p+1)}$.

In the supersingular case, a situation arises that is similar to the scenario we discussed at the end of §5.1 for the ordinary case. In theory, there is nothing preventing us from finding supersingular curves $\mathcal{E}/\mathbb{F}_{q^v}$ whose $p$-torsion is minimally defined over $\mathbb{F}_{q^v}$ with $v > 2$. However, the following proposition shows that they are $\mathbb{F}_{q^v}$-isogenous to the $\mathcal{B}/\mathbb{F}_{q^2}$ in Proposition 5. In other words, in terms of increasing $v$ to decrease the size of $q$, there is nothing to be gained by looking for supersingular curves with $v > 2$, as it leaves the door open for an attacker that could use the isogeny to bring the corresponding DLP instances into $\mathbb{F}_{q^2}$.

**Proposition 6.** *Let $q = p^{2u} \pm p^u + 1$ be a prime where $p > 3$ is also prime, let $v$ be an integer, and let $\mathcal{E}/\mathbb{F}_{q^v}$ be a supersingular elliptic curve such that $\mathcal{E}[p] \subseteq \mathcal{E}(\mathbb{F}_{q^v})$. Then $\mathcal{E}$ is $\mathbb{F}_{q^v}$-isogenous to $\mathcal{B}$ from Proposition 5.*

*Proof.* Theorem 1((iv)) states that $t = 0$ for odd $v$, meaning $\#\mathcal{E}(\mathbb{F}_{q^v}) = q^v + 1 \equiv 2 \bmod p$, which precludes $\mathcal{E}[p] \subseteq \mathcal{E}(\mathbb{F}_{q^v})$, hence $v$ must be even. The same argument rules out $t = 0$ for even $v$ from Theorem 1((iii)). Our choice of $q$ is such that $q \equiv 1 \bmod 3$, while rules out $t = \pm\sqrt{q^v}$ for even $v$ from Theorem 1((ii)). Thus, the only options for even $v$ are $t = -2\sqrt{q^v}$ and $t = 2\sqrt{q^v}$. The former is again ruled out by $\mathcal{E}[p] \subseteq \mathcal{E}(\mathbb{F}_{q^v})$, since $\#\mathcal{E}(\mathbb{F}_{q^v}) \equiv 4 \bmod p$ in that case. Thus, it must be that $t = 2q^{v/2}$, which (with $\mathcal{B}/\mathbb{F}_{q^2}$ as in Proposition 5) is the same trace as $\mathcal{B}(\mathbb{F}_{q^v})$ [9, Corollary VI.2]. □

### 5.3 $\mathcal{B}$ is ordinary and defined over $\mathbb{F}_{q^3}$

In this section, we present a construction for an ordinary elliptic curve $\mathcal{B}/\mathbb{F}_{q^3}$ that can be used to form a cycle with $\mathcal{A}/\mathbb{F}_{p^2}$ constructed in Proposition 1 (i.e., we fix $u = 2$).

Due to the Hasse bound, the trace $t$ lies between $-2p^3$ and $2p^3$. So, to find such a $\mathcal{B}/\mathbb{F}_{q^3}$ we set its trace to be $t = t_0 + t_1 p + t_2 p^2 + t_3 p^3$, for some unknowns $t_0, t_1, t_2 \in \mathbb{Z}$ and $t_3 \in \{-2, -1, 0, 1, 2\}$. Our goal is to find $t_i \in \mathbb{Z}$ such that: (a) $p^2 \mid (q^3 + 1 - t)$; and (b) the squarefree part of $4q^3 - t^2$ is small. The former condition ensures that $p^2$ divides $\#\mathcal{B}(\mathbb{F}_{q^3})$ so that a cycle can be formed with $\mathcal{A}$, and the latter ensures that the discriminant $D$ of $\mathcal{B}$ is small enough that $\mathcal{B}$ can be constructed using the CM method. This leads us to the following proposition.

**Proposition 7.** *Let $p \equiv 2 \bmod 3$ be an odd prime such that $q = p^2 + p + 1$ is also prime. The elliptic curve $\mathcal{B}/\mathbb{F}_{q^3}$ with trace $t = 2 + 3p \pm 3p^2 \pm 2p^3$ forms a cycle with $\mathcal{A}/\mathbb{F}_{p^2}$ constructed in Proposition 1. Let $4q^3 - t^2 = DV^2$ with squarefree discriminant $D$. Then:*

1. *If $t = 2 + 3p + 3p^2 + 2p^3$, then $D$ is equal to the squarefree part of $3p^2 + 2p + 3$.*
2. *If $t = 2 + 3p - 3p^2 - 2p^3$, then $D = 3$ and $\mathcal{B}$ is a cubic twist of the elliptic curve from Proposition 3.*

*Proof.* Letting $(t_0, t_1) = (2, 3)$ we get $DV^2 = 4q^3 - t^2 = -p^2 \cdot f(p)$, where

$$f(p) = (t_3^2 - 4)p^4 + (2t_2 t_3 - 12)p^3 + (t_2^2 + 6t_3 - 24)p^2 + (6t_2 + 4t_3 - 28)p + 4$$

ensuring $p^2 \mid (q^3 + 1 - t)$. If $(t_2, t_3) = (3, 2)$, we obtain

$$DV^2 = p^2(3p^2 + 2p + 3). \qquad (2)$$

If $(t_2, t_3) = (-3, -2)$, then $DV^2 = 27p^2(p+1)^2$ and so $D = 3$. This corresponds to one of the cubic twists in Proposition 4, that is, $\mathbb{F}_{q^3}$-isomorphic to the elliptic curve $\mathcal{B}/\mathbb{F}_q$ from Proposition 3. □

In the above proposition, we note that if the squarefree part of $(3p^2 + 2p + 3)$ is small[8], then $\mathcal{B}/\mathbb{F}_{q^3}$ with trace $t = 2 + 3p + 3p^2 + 2p^3$ can be constructed using the CM method.

*Example 1 (continued).* We continue with $p = 1373$ and $q = p^2 + p + 1 = 1886503$, this time taking $\mathbb{F}_{q^3} = \mathbb{F}_q(\xi)$ with $\xi^3 = 3$. Viewing (2), we see that the squarefree discriminant $D$ is the squarefree part of $3p^2 + 2p + 3$, which in this case is $D = 1414534$. The Hilbert class polynomial $H_{-4D}(x) \in \mathbb{F}_{q^2}[x]$ is $H_{-4D}(x) = x^{720} + 839185x^{719} + \cdots + 437552$; all 720 of its roots are unique elements of $\mathbb{F}_q$ and again give rise to non-isomorphic options for $\mathcal{B}$. One such instance has $j$-invariant $j = 1773$, a model for which is $\mathcal{B}\colon y^2 = x^3 + 1130838x + 1511330$; the trace over $\mathbb{F}_{q^3}$ is $t = 2p^3 + 3p^2 + 3p + 2$ and the group structure is $\mathcal{B}(\mathbb{F}_{q^3}) \cong \mathbb{Z}_p \times \mathbb{Z}_{p(p^2+p+1)(p^2+2p+3)}$. Note that $\mathcal{B}$ is minimally defined over $\mathbb{F}_q$, but we do not find points of order $p$ until we consider the group $\mathcal{B}(\mathbb{F}_{q^3})$, where we find $\mathcal{B}[p] \subset \mathcal{B}(\mathbb{F}_{q^3})$.

### 5.4 $\mathcal{B}$ is ordinary and defined over $\mathbb{F}_{q^v}$, $v$ even

We now consider ordinary $\mathcal{B}$ defined over even extension fields, i.e., $\mathcal{B}/\mathbb{F}_{p^v}$ for $v$ even, which will form a cycle with $\mathcal{A}/\mathbb{F}_{p^2}$ constructed in Proposition 1.

First, for simplicity, we fix $v = 2$ to get an analogous construction as in §5.2 for an ordinary elliptic curve. We do so by following the method introduced in the previous section. Namely, we let the trace of $\mathcal{B}$ be $t = t_0 + t_1 p + t_2 p^2$, for some unknowns $t_0, t_1 \in \mathbb{Z}$ and $t_2 \in \{-2, -1, 0, 1, 2\}$ (again by considering the Hasse bound). We want to choose the $t_i$ so that: (a) $p^2 \mid (q^2 + 1 - t)$; and (b) $4q^2 - t^2$ has small squarefree part. This is achieved by setting $t_0 = t_1 = 2$, and $t_2 = -2$. Indeed, we obtain

$$\#\mathcal{B}(\mathbb{F}_{q^2}) = p^2(p^2 + 2p + 5) \qquad \text{and} \qquad DV^2 = 16p^2(p + 1). \qquad (3)$$

[8] In practice, searching for large $p$ such that the squarefree part of $3p^2 + 2p + 3$ is small can be done by using Pell equations; this same issue arises when constructing MNT curves.

Condition (a) ensures that $\mathcal{B}/\mathbb{F}_{p^2}$ will form a cycle with $\mathcal{A}/\mathbb{F}_{p^2}$ from Proposition 1. If the squarefree part of $p+1$ (which corresponds to the discriminant of $\mathcal{B}$) is small, then condition (b) is satisfied and we can explicitly construct the equation defining $\mathcal{B}$ using the CM method.

*Example 1 (continued).* We continue with $p = 1373$, $q = p^2+p+1 = 1886503$, and $\mathbb{F}_{q^2} = \mathbb{F}_q(\xi)$ with $\xi^2 + 1 = 0$ as above. Viewing (3), we see that the squarefree discriminant $D$ is the squarefree part of $p+1$, which in this case is $D = p+1 = 1374$. The Hilbert class polynomial $H_{-4D}(x) \in \mathbb{F}_{q^2}[x]$ is $H_{-4D}(x) = x^{28} + 111311x^{27} + \cdots + 786521$; all 28 of its roots are unique elements of $\mathbb{F}_q$ and give rise to non-isomorphic options for $\mathcal{B}$. One such instance has $j$-invariant $j = 219133$, a model for which is $\mathcal{B}/\mathbb{F}_{q^2} : y^2 = x^3 + (808231\xi + 52195)x + (1293228\xi + 1434207)$; the trace is $t(\mathcal{B}) = -2p^2 + 2p + 2$ and the group structure is $\mathcal{B}(\mathbb{F}_{q^2}) \cong \mathbb{Z}_{2p} \times \mathbb{Z}_{p(p^2+2p+5)/2}$. Note that we can always find an elliptic curve $\mathcal{E}/\mathbb{F}_q$ with the prescribed $j \in \mathbb{F}_q$, but that $\mathcal{E}(\mathbb{F}_{q^2})$ may not have the correct group order from (3); in such cases, we can take $\mathcal{B}$ as the quadratic twist of $\mathcal{E}(\mathbb{F}_{q^2})$, and in general $\mathcal{B}$ will not be minimally defined over $\mathbb{F}_q$, as we see in the above instance.

Following the case of $v = 2$, we obtain a construction for general field extensions of even degree $v$. We start with a general parameterisation of the trace $t$ as $t = \sum_{i=0}^{v} t_i p^i$ and attempt to find small integer coefficients $t_i$ such that the group order is divisible by $p^2$ and $4q^v - t^2 = DV^2$ as polynomials in $p$, where $D$ is at most quadratic in $p$.

Our first observation is that picking $t_0 = 2$ and $t_1 = v$ ensures that $p^2 \mid (q^v + 1 - t)$. This follows directly from $q = p^2 + p + 1$ by explicitly computing $q^v + 1 - t = (2 - t_0) + (v - t_1)p + p^2(\dots)$ as a polynomial in $p$. The following lemma shows how to pick $t$ as a polynomial in $p$ such that $D$ is the squarefree part of $p+1$ in the norm equation.

**Lemma 1.** *Let $p$ and $v$ be positive integers such that $v = 2w$ is even, and let $q = p^2 + p + 1$. If $t = 2q^{w-1}(-p^2 + p + 1)$, then*

$$p^2 \mid (q^v + 1 - t) \quad \textit{and} \quad 4q^v - t^2 = 16p^2q^{v-2}(p+1) = (4pq^{w-1})^2(p+1). \tag{4}$$

*Proof.* Note that $q^m = (1 + p + p^2)^m \equiv 1 + mp \bmod p^2$ for all $m \geq 0$. It follows that

$$\begin{aligned} q^v + 1 - t &\equiv 1 + vp + 1 - 2q^{w-1}(p+1) \\ &\equiv 2 + 2wp - 2(1 + (w-1)p)(p+1) \\ &\equiv 2 + 2wp - 2(p+1) - 2(w-1)p \equiv 0 \bmod p^2. \end{aligned}$$

Furthermore, it holds that

$$\begin{aligned} t - 2q^w &= 2q^{w-1}(-p^2 + p + 1) - 2q^w = 2q^{w-1}(-p^2 + p + 1 - q) = -4q^{w-1}p^2 \text{ and} \\ t + 2q^w &= 2q^{w-1}(-p^2 + p + 1) + 2q^w = 2q^{w-1}(-p^2 + p + 1 + q) = 4q^{w-1}(p+1), \end{aligned}$$

which means that $4q^v - t^2 = -(t - 2q^w)(t + 2q^w) = 16q^{2w-2}p^2(p+1)$. □

From this lemma, we immediately obtain the following proposition.

**Proposition 8.** *Let $p \equiv 2 \bmod 3$ be an odd prime such that $q = p^2 + p + 1$ is also prime. For $v \in 2\mathbb{Z}$, the elliptic curve $\mathcal{B}/\mathbb{F}_{q^v}$ with trace $t = 2q^{v/2-1}(-p^2 + p + 1)$, forms a cycle with $\mathcal{A}/\mathbb{F}_{p^2}$ constructed in Proposition 1. The discriminant $D$ of $\mathcal{B}$ is equal to the squarefree part of $p+1$.*

To explicitly construct $\mathcal{B}$ as in Proposition 8, one can run through integers of the form $p = D(V')^2 - 1$ for feasible CM discriminants $D$ and integers $V'$ of the appropriate size such that $p \equiv 2 \bmod 3$ until $p$ is prime. Then $4q^v - t^2 = DV^2$, where $V = 4pq^{v/2-1} \cdot V'$ according to Lemma 1 and $\mathcal{B}$ can be constructed with the CM method via computing the Hilbert class polynomial $H_D(x)$ as described in Section 2.

*Remark 1.* Note that Lemma 1 is still true if one replaces $p$ by $p^{u/2}$ for any even $u$. This also gives an analog of Proposition 8 showing that cycles between $\mathcal{A}/\mathbb{F}_{p^u}$ and $\mathcal{B}/\mathbb{F}_{q^v}$ exist for any $u \in 2 + 4\mathbb{Z}$ and $v \in 2\mathbb{Z}$. However, the CM discriminant of $\mathcal{B}$ will be the squarefree part of $p^{u/2} + 1$. Even for the smallest possible $u$ larger than 2, which is $u = 6$, we have not yet found a way to guarantee for $p$ of cryptographic size that the squarefree part of $p^3 + 1$ is small enough for the CM method to be feasible. Therefore, we were not able to explicitly construct the corresponding $\mathcal{B}$ for values other than $u = 2$.

## 6 $\mathcal{A}$ is a supersingular abelian surface

We now return to constructing $\mathcal{A}$'s that can be paired with the curves $\mathcal{B}$ constructed in the previous section. In this section, we fix the dimension of $\mathcal{A}$ to be 2, i.e., $\mathcal{A}$ is an abelian surface. In §6.1 and §6.2 we present $\mathcal{A}$ with cryptographic exponent $c_{\mathcal{A}} = 3$ and 6 by considering $\mathcal{A}/\mathbb{F}_{p^u}$ with group order $p^{2u} \pm p^u + 1$, respectively.

### 6.1 $\mathcal{A}$ has cryptographic exponent 3

**Proposition 9.** *Let $p \equiv 2 \bmod 3$ be an odd prime and $u$ be an odd integer such that $q = p^{2u}+p^u+1$ is also prime. There exists a simple abelian surface $\mathcal{A}/\mathbb{F}_{p^u}$ such that:*

1. *$\mathcal{A}$ is supersingular;*
2. *the characteristic polynomial of the $p^u$-power Frobenius endomorphism on $\mathcal{A}$ is*
$$P(x) = x^4 + p^u x^2 + p^{2u};$$
3. *$\#\mathcal{A}(\mathbb{F}_{p^u}) = q$;*
4. *$\mathcal{A}$ has cryptographic exponent $c_{\mathcal{A}} = 3$ with respect to $q$;*
5. *$\mathcal{A}$ is (principally polarized as) the Jacobian of some twist of the curve $\mathcal{C}'/\mathbb{F}_{p^u}\colon\ y^2 = x^6 + 1$; and*
6. *$\mathcal{A}(\mathbb{F}_{p^u})$ forms a* cycle *$\mathcal{A} \rightleftharpoons \mathcal{B}$, with the ordinary elliptic curve $\mathcal{B}/\mathbb{F}_q$ from Proposition 3, or with the supersingular elliptic curve $\mathcal{B}/\mathbb{F}_{q^2}$ from Proposition 5.*

*Proof.* Claims 1 and 2 are due to Maisner and Nart—see [43, Corollary 2.11] and [43, Theorem 2.9], respectively. Claim 3 follows from $\#\mathcal{A} = P(1)$, and Claim 4 follows from $P(1)$ being $\Phi_3(p)$, i.e., the third cyclotomic polynomial evaluated at $p$. Claim 5 is due to Howe, Nart and Ritzenthaler [36, pp. 282–283]. Finally, Claim 6 follows from Claim 3 and Propositions 3 and 5, together with Definition 1. □

*Example 1 (continued).* We continue with $p = 1373$ and take $u = 1$ so $q = p^2 + p + 1 = 1886503$. The curve $\mathcal{C}/\mathbb{F}_p\colon y^2 = x^6 + 733x^5 + 900x^4 + 1052x^3 + 393x^2 + 901x + 1332$ is a twist of $\mathcal{C}'/\mathbb{F}_p\colon y^2 = x^6 + 1$. The characteristic polynomial of the $p$-power Frobenius endomorphism on $\mathcal{A} = \mathcal{J}_{\mathcal{C}}$ is $P(x) = x^4 + 1373x^2 + 1373^2$ and $\#\mathcal{A}(\mathbb{F}_p) = 1886503$. The order-$q$ Weil pairing on $\mathcal{A}$ maps to a subgroup of $\mathbb{F}_{p^3}^{\times}$.

### 6.2 $\mathcal{A}$ has cryptographic exponent 6

**Proposition 10.** *Let $p \equiv 5 \bmod 12$ be an odd prime and $u$ be an even integer such that $q = p^{2u} - p^u + 1$ is also prime. There exists a simple abelian surface $\mathcal{A}/\mathbb{F}_{p^u}$ such that:*

1. *$\mathcal{A}$ is supersingular;*
2. *the characteristic polynomial of the $p^u$-power Frobenius endomorphism on $\mathcal{A}$ is*
$$P(x) = x^4 - p^u x^2 + p^{2u};$$
3. *$\#\mathcal{A}(\mathbb{F}_{p^u}) = q$;*
4. *$\mathcal{A}$ has cryptographic exponent $c_{\mathcal{A}} = 6$ with respect to $q$;*
5. *$\mathcal{A}$ is $\mathbb{F}_{p^u}$-isogenous to the Jacobian of a twist of $\mathcal{E} \times \mathcal{E}$, where $\mathcal{E}/\mathbb{F}_p\colon y^2 = x^3 + 1$; and,*
6. *$\mathcal{A}(\mathbb{F}_{p^u})$ forms a* cycle *$\mathcal{A} \rightleftharpoons \mathcal{B}$, with the ordinary elliptic curve $\mathcal{B}/\mathbb{F}_q$ from Proposition 3, or with the supersingular elliptic curve $\mathcal{B}/\mathbb{F}_{q^2}$ from Proposition 5.*

*Proof.* Claims 1 and 2 are again due to Maisner and Nart—see [43, Corollary 2.11] and [43, Theorem 2.9], respectively. Claim 3 follows from $\#\mathcal{A} = P(1)$, and Claim 4 follows from $P(1)$ being $\Phi_6(p)$, i.e., the sixth cyclotomic polynomial evaluated at $p$. Claim 5 is due to Howe, Nart and Ritzenthaler—see the proof of [36, Proposition 13.4]. Finally, Claim 6 follows from Claim 3 and Propositions 3 and 5, together with Definition 1. □

## 7 $\mathcal{A}$ is a trace-zero subvariety

Our final construction exploits the theorem of Rubin and Silverberg [49], given in Theorem 3. We take the supersingular elliptic curve $\mathcal{E}/\mathbb{F}_{p^u}$ considered in Proposition 1, and consider $\mathcal{E}$ over $\mathbb{F}_{p^{ur}}$ for $r$ a power of 2. Using Weil restriction, we can construct an abelian variety $\mathcal{A}/\mathbb{F}_{p^u}$ of dimension $g = r/2$ with cryptographic exponent $c_{\mathcal{A}} = 3 \cdot 2^{g-1}$. By increasing the dimension of $\mathcal{A}$, we obtain an arbitrarily large cryptographic exponent $c_{\mathcal{A}}$. This will, however, come at the cost of more expensive arithmetic for higher dimensional varieties. The upside is that we can identify $\mathcal{A}/\mathbb{F}_{p^u}$ with a subgroup of $\mathcal{E}(\mathbb{F}_{p^{ur}})$: the trace-zero subvariety[9]. Thus, all arithmetic can instead be performed in this subgroup, rather than on a $g$-dimensional abelian variety. This result is given in Theorem 4. In §7.2 we provide several examples for cryptographic sized $p$ constructed using Theorem 4 and draw some comparisons with the MNT cycle.

### 7.1 Applying the theorem of Rubin and Silverberg

In the statement of the theorem below we start with $\mathcal{E}/\mathbb{F}_{p^u}$ as the curve from Proposition 1. However, we no longer need to insist that $q = \#\mathcal{E}(\mathbb{F}_{p^u})$ is prime; this was done so that the curve in Proposition 1 could form a cycle with subsequent constructions of $\mathcal{B}/\mathbb{F}_{q^v}$. Instead, we will be insisting that $q = P(1)$ is prime, where $P(x)$ is given in item 2 of the theorem that follows.

**Theorem 4.** *Let $\mathcal{E}/\mathbb{F}_{p^u}$ be the elliptic curve in Proposition 1 and let $r = 2g$ where $g = 2^\ell$ with $\ell \geq 0$. Then there is a supersingular abelian variety $\mathcal{A}/\mathbb{F}_{p^u}$ such that*

1. $\dim(\mathcal{A}) = g$;
2. *the characteristic polynomial of the Frobenius endomorphism of $\mathcal{A}$ is*
$$P(x) = x^{ug} - p^{ug/2}x^{ug/2} + p^{ug};$$
3. *the cryptographic exponent is $c_{\mathcal{A}} = 3 \cdot 2^{g-1}$;*
4. *there is a natural identification of $\mathcal{A}(\mathbb{F}_{p^u})$ with the subgroup of $\mathcal{E}(\mathbb{F}_{p^{ur}})$*
$$\mathcal{T}_r^0 = \{Q \in \mathcal{E}(\mathbb{F}_{p^{ur}}) \colon \mathrm{Tr}_{\mathbb{F}_{p^{ur}}/\mathbb{F}_{p^{ug}}}(Q) = \mathcal{O}\}.$$

*Furthemore, if $q = P(1)$ is prime, then in the sense of Definition 1, $\mathcal{A}(\mathbb{F}_{p^u})$ forms a* cycle *$\mathcal{A} \rightleftharpoons \mathcal{B}$, with the ordinary elliptic curve $\mathcal{B}/\mathbb{F}_q$ from Proposition 3, or with the supersingular elliptic curve $\mathcal{B}/\mathbb{F}_{q^2}$ from Proposition 5 (where $u$ is replaced with $u \cdot g$ in the statement of both propositions).*

*Proof.* The curve $\mathcal{E}/\mathbb{F}_{p^u}$ from Proposition 1 has $c_{\mathcal{E}} = 3/2$, so $\gcd(r, 2pc_{\mathcal{E}}) = \gcd(r, 3p) = 1$ as required to apply Theorem 3 since $r = 2^{\ell+1}$. Then, Claims 1, 3 and 4 follow from Theorem 3 (i), (iii), and (iv) respectively. For Claim 2, $\pi$ is a $p^u$-Weil number for $\mathcal{E}$ and satisfies the characteristic polynomial $P_{\mathcal{E}}(x) = x^u + p^{u/2}x^{u/2} + p^u$ and $\zeta$ is a primitive $r$-th root of unity, where $r = 2g$ and $g = 2^\ell$, meaning $\zeta$ satisfies $x^g + 1 = 0$. Theorem 3(ii) says $\zeta\pi$ is a $p^u$-number for $\mathcal{A}$, the minimal polynomial for which is $P(x) = x^{ug} - p^{ug/2}x^{ug/2} + p^{ug}$. Finally, $\mathcal{A} \rightleftharpoons \mathcal{B}$ follows immediately from $q = P(1)$ and Theorem 2(iv). □

*Example 1 (continued).* Recall (from the example corresponding to Proposition 1) that $p = 1373$, $u = 2$, $\mathbb{F}_{p^2} = \mathbb{F}_p(\lambda)$ with $\lambda^2 = 2$, and $\mathcal{E}/\mathbb{F}_{p^2} \colon y^2 = x^3 + (\lambda + 12)$. We will illustrate Theorem 4 for $\ell = 2$, which gives $g = 4$ and $r = 8$, so $\mathcal{A}/\mathbb{F}_{p^2}$ is identified with $\mathcal{T}_8^0 = \{Q \in \mathcal{E}(\mathbb{F}_{p^{16}}) \colon \mathrm{Tr}_{\mathbb{F}_{p^{16}}/\mathbb{F}_{p^8}}(Q) = \mathcal{O}\}$. Now, $\#\mathcal{E}(\mathbb{F}_{p^{16}}) = (p^8 + p^4 + 1)(p^8 - p^4 + 1)$, and $\#\mathcal{T}_8^0 = P(1) = p^8 - p^4 + 1$, so $\mathcal{A}/\mathbb{F}_{p^2}$ is an abelian variety of dimension $g = 4$ identified with the order-$(p^8 - p^4 + 1)$ subgroup of $\mathcal{E}(\mathbb{F}_{p^{16}})$. Here $q = P(1) = 1262886433524143595063624l$ is prime, so taking $\beta = 11$ as the primitive element of $\mathbb{F}_q$, from Proposition 3 we get the ordinary curve $\mathcal{B}/\mathbb{F}_q \colon y^2 = x^3 + \beta^5$, which has group structure $\mathcal{B}(\mathbb{F}_q) \cong \mathbb{Z}_{p^4} \times \mathbb{Z}_{p^4}$ and we have the cycle

$$\mathcal{A}/\mathbb{F}_{p^2} \rightleftharpoons \mathcal{B}/\mathbb{F}_q.$$

[9] Trace-zero varieties were first suggested for use in cryptography by Frey [20].

Here $c_{\mathcal{A}} = 24$, so the order-$q$ Weil pairing on $\mathcal{A}$ maps to $\mathbb{F}_{p^{48}}^{\times}$, and $c_{\mathcal{B}} = 1$, so the order-$p$ Weil pairing on $\mathcal{B}$ maps to $\mathbb{F}_q^{\times}$. Alternatively, we can take the supersingular $\mathcal{B}$ from Proposition 5. Let $\mathbb{F}_{q^2} = \mathbb{F}_q(\xi)$ with $\xi^2 + 11 = 0$. On input of the trace $t = 2q$, Bröker's algorithm [13] outputs the supersingular curve $\mathcal{B}/\mathbb{F}_{q^2} \colon y^2 = x^3 + ax + b$ with

$$\begin{aligned} a &= 7556923987885274573241445 \cdot \xi + 6346076494481973586254723, \\ b &= 7284530327753877594920076 \cdot \xi + 3813091413099528533306290, \end{aligned}$$

which has group structure $\mathcal{B}(\mathbb{F}_{q^2}) \cong \mathbb{Z}_{p^4(p^4-1)} \times \mathbb{Z}_{p^4(p^4-1)}$, and gives rise to the cycle

$$\mathcal{A}/\mathbb{F}_{p^2} \rightleftharpoons \mathcal{B}/\mathbb{F}_{q^2}.$$

The order-$p$ Weil pairing on $\mathcal{B}$ maps to $\mathbb{F}_{q^2}^{\times}$.

### 7.2 Cryptographic examples

We now illustrate Theorem 4 by presenting some examples of cryptographic size. In line with the discussions in Section 1, we draw comparisons to the MNT cycle merely to illustrate the potential of using higher dimensional varieties and the relaxations in Definition 1 in terms of achieving smaller sizes of $p$. In particular, we do not claim that any cycle given in this paper will outperform an MNT cycle at the same security level for a given SNARK construction.

We give two examples at the 80- and 112-bit security levels and three examples at the 128-bit security level. These are summarised and presented alongside the three cycles of MNT curves in Table 1 below. The smaller MNT cycles are from the original paper on cycles by Ben-Sasson, Chiesa, Tromer and Virza [6] and the 128-bit example is due to Guillevic [33]. We note that drawing comparisons at these lower security levels is not as favourable to our construction as higher security levels would be: the sizes of $p$ and $q$ in the MNT cycle necessarily grow linearly with the size of the extension fields required to resist (subexponential) attacks in $\mathbb{F}_{p^4}^{\times}$. One drawback of our construction is that $c_{\mathcal{B}} = 1$ forces $q$ to grow linearly with the sizes of the extension fields as well, but as we discussed in Sections 1 and 3, this is a consequence of the restrictions we imposed in this paper (in particular, §3.1,4). On the other hand, our construction affords us to choose $p$ as small as possible at a given security level, i.e., based on the complexity of the generic Pollard-$\rho$ attack, as can be seen in Cycles 1, 2, 3, 5 and 7.

At each of the three security levels, we found the example cycles summarised in Table 1 subject to the following two constraints: (1) we ensured that the smallest of the two extension fields $\mathbb{F}_{p^{u \cdot c_{\mathcal{A}}}}$ and $\mathbb{F}_{q^{v \cdot c_{\mathcal{B}}}}$ in our construction was no smaller than the smallest extension field in the corresponding MNT construction; and, (2) we wanted the bitlength of $p$ (our smallest prime) to be at least twice the security parameter in order to meet the requisite ECDLP security. In all cases, once the bitlength $l$ of $p$ was determined, we searched backwards from $2^l - 1$ until we found the first prime $p \equiv 2 \bmod 3$ such that $q = p^u \pm p^{u/2} + 1$ was also prime. An alternative set of primes that give identical constructions but maximise the 2-adicity of $p - 1$ and $q - 1$ are given in §8.4.

The bold numbers in Table 1 indicate when the size of $p$ in our construction is less than the sizes of the primes in the corresponding MNT construction. Cycle 7 shows the optimal scenario where the bitlength of our $p$ is twice the security level and $\mathcal{A}$'s field of definition is $\mathbb{F}_{p^2}$, which itself is signifcantly smaller than the sizes of $p$ and $q$ in the MNT construction. Of course, in this case $\mathcal{A}$ has dimension $g = 4$, meaning that arithmetic is much more complex than on its dimension-1 counterparts. However, in the next section we cite a number of optimisations that significantly accelerate arithmetic on $\mathcal{A}$.

For each cycle, we provide `Magma` and `Sage` code that verifies all parameters. This can be found at

`https://github.com/craigcostello/pairing-friendly-cycles`.

**Table 1.** A summary of some examples of our construction together alongside three instantiations of the MNT cycle found in the literature. Further explanation in text.

| target | MNT cycle | | | | | this work | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| security | ref. | $p$ | $q$ | $p^k$ | $q^{k'}$ | ref. | $\dim(\mathcal{A})$ | $p$ | $p^u$ | $q$ | $(p^u)^{c_\mathcal{A}}$ | $q^v$ |
| 80 | [6] | 298 | 298 | 1192 | 1788 | Cycle 1 | 1 | **160** | 640 | 640 | 1920 | 1280 |
| | | | | | | Cycle 2 | 2 | **160** | 320 | 640 | 1920 | 1280 |
| 112 | [6] | 753 | 753 | 3012 | 4517 | Cycle 3 | 1 | **224** | 1792 | 1792 | 5376 | 3584 |
| | | | | | | Cycle 4 | 2 | **377** | 754 | 1508 | 4512 | 3012 |
| 128 | [33] | 992 | 992 | 3966 | 5948 | Cycle 5 | 1 | **256** | 2048 | 2048 | 6144 | 4096 |
| | | | | | | Cycle 6 | 2 | **512** | 1024 | 2048 | 6144 | 4096 |
| | | | | | | Cycle 7 | 4 | **256** | **512** | 2048 | 12288 | 4096 |

**Cycle 1** Let $p = 2^{160} - 44159$, $\mathbb{F}_{p^2} = \mathbb{F}_p(\lambda)$ with $\lambda^2 = 3$ and $\mathbb{F}_{p^4} = \mathbb{F}_{p^2}(\mu)$ with $\mu^2 = \lambda$. Following Proposition 1, the curve $\mathcal{A}/\mathbb{F}_{p^4}\colon y^2 = x^3 + \alpha$ with $\alpha = \lambda + \mu$ is such that $\#\mathcal{A}(\mathbb{F}_{p^4}) = q$, where $q = p^4 - p^2 + 1$ is 640 bits. Let $\mathbb{F}_{q^2} = \mathbb{F}_q(\xi)$ with $\xi^2 + 5 = 0$. Following Proposition 5, Bröker's algorithm outputs a supersingular curve $\mathcal{B}/\mathbb{F}_{q^2}\colon y^2 = x^3 + ax + b$ with $a, b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and $j(\mathcal{B}) \in \mathbb{F}_q$ whose group structure is $\mathcal{B}(\mathbb{F}_{q^2}) = \mathbb{Z}_{p^2(p^2-1)} \times \mathbb{Z}_{p^2(p^2-1)}$. The parameters $a, b$ and $j$ are in the file `cycle1.m`. Here $c_\mathcal{A} = 3$ and $c_\mathcal{B} = 1$: the $q$-Weil pairing on $\mathcal{A}/\mathbb{F}_{p^4}$ maps into the 1920-bit field $\mathbb{F}_{p^{12}}^\times$, and the $p$-Weil pairing on $\mathcal{B}/\mathbb{F}_{q^2}$ maps into the 1280-bit field $\mathbb{F}_{q^2}^\times$.

**Cycle 2** Let $p, \mathbb{F}_{p^2}, q, \mathbb{F}_{q^2}$ and $\mathcal{B}/\mathbb{F}_{q^2}$ be as in Cycle 1. Following Proposition 1, $\mathcal{E}/\mathbb{F}_{p^2}\colon y^2 = x^3 + \alpha$ with $\alpha = \lambda + 3$ is such that $\#\mathcal{E}(\mathbb{F}_{p^2}) = p^2 + p + 1$. Setting $g = \dim(\mathcal{A}) = 2$ gives $r = 4$, so from Theorem 4 we identify $\mathcal{A}/\mathbb{F}_{p^2}$ with

$$\mathcal{T}_4^0 = \{Q \in \mathcal{E}(\mathbb{F}_{p^8})\colon \mathrm{Tr}_{\mathbb{F}_{p^8}/\mathbb{F}_{p^4}}(Q) = \mathcal{O}\},$$

i.e., $\mathcal{T}_4^0$ corresponds to the points of order $q$ in $\mathcal{E}(\mathbb{F}_{p^8})$, whose cardinality is $\#\mathcal{E}(\mathbb{F}_{p^8}) = q\cdot(p^4 + p^2 + 1)$. As in Cycle 1, the $q$-Weil pairing on $\mathcal{A}/\mathbb{F}_{p^2}$ maps into the 1920-bit field $\mathbb{F}_{p^{12}}^\times$, and the $p$-Weil pairing on $\mathcal{B}/\mathbb{F}_{q^2}$ maps into the 1280-bit field $\mathbb{F}_{q^2}^\times$.

**Cycle 3** Let $p = 2^{224} - 44159$, $\mathbb{F}_{p^2} = \mathbb{F}_p(\lambda)$ with $\lambda^2 = 2$, $\mathbb{F}_{p^4} = \mathbb{F}_{p^2}(\mu)$ with $\mu^2 = \lambda$, and $\mathbb{F}_{p^8} = \mathbb{F}_{p^4}(\nu)$ with $\nu^2 = \mu$. Following Proposition 2, the curve $\mathcal{A}/\mathbb{F}_{p^8}\colon y^2 = x^3 + \alpha$ with $\alpha = \lambda + \mu + \nu$ is such that $\#\mathcal{A}(\mathbb{F}_{p^8}) = q$, where $q = p^8 - p^4 + 1$ is 1792 bits. Let $\mathbb{F}_{q^2} = \mathbb{F}_q(\xi)$ with $\xi^2 + 13 = 0$. Following Proposition 5, Bröker's algorithm outputs a supersingular curve $\mathcal{B}/\mathbb{F}_{q^2}\colon y^2 = x^3 + ax + b$ with $a, b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and $j(\mathcal{B}) \in \mathbb{F}_q$ whose group structure is $\mathcal{B}(\mathbb{F}_{q^2}) = \mathbb{Z}_{p^4(p^4-1)} \times \mathbb{Z}_{p^4(p^4-1)}$. The parameters $a, b$ and $j$ are in the file `cycle3.m`. Here $c_\mathcal{A} = 3$ and $c_\mathcal{B} = 1$: the $q$-Weil pairing on $\mathcal{A}/\mathbb{F}_{p^8}$ maps into the 5376-bit field $\mathbb{F}_{p^{12}}^\times$, and the $p$-Weil pairing on $\mathcal{B}/\mathbb{F}_{q^2}$ maps into the 3584-bit field $\mathbb{F}_{q^2}^\times$.

**Cycle 4** Let $p = 2^{377} - 12351$, $\mathbb{F}_{p^2} = \mathbb{F}_p(\lambda)$ with $\lambda^2 = 3$. Following Proposition 1, $\mathcal{E}/\mathbb{F}_{p^2}\colon y^2 = x^3 + \alpha$ with $\alpha = \lambda + 6$ is such that $\#\mathcal{E}(\mathbb{F}_{p^2}) = p^2 + p + 1$. Setting $g = \dim(\mathcal{A}) = 2$ gives $r = 4$, so from Theorem 4 we identify $\mathcal{A}/\mathbb{F}_{p^2}$ with

$$\mathcal{T}_4^0 = \{Q \in \mathcal{E}(\mathbb{F}_{p^8})\colon \mathrm{Tr}_{\mathbb{F}_{p^8}/\mathbb{F}_{p^4}}(Q) = \mathcal{O}\},$$

i.e., $\mathcal{T}_4^0$ corresponds to the points of order $q = p^4 - p^2 + 1$ in $\mathcal{E}(\mathbb{F}_{p^8})$, whose order is $\#\mathcal{E}(\mathbb{F}_{p^8}) = q \cdot (p^4 + p^2 + 1)$. Let $\mathbb{F}_{q^2} = \mathbb{F}_q(\xi)$ with $\xi^2 + 11 = 0$. Following Proposition 5, Bröker's algorithm outputs a supersingular curve $\mathcal{B}/\mathbb{F}_{q^2}\colon y^2 = x^3 + ax + b$ with $a, b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and $j(\mathcal{B}) \in \mathbb{F}_q$ whose group structure is $\mathcal{B}(\mathbb{F}_{q^2}) = \mathbb{Z}_{p^2(p^2-1)} \times \mathbb{Z}_{p^2(p^2-1)}$. The parameters $a, b$ and $j$ are in the file `cycle4.m`. Here $c_\mathcal{A} = 6$ and $c_\mathcal{B} = 1$: the $q$-Weil pairing on $\mathcal{A}/\mathbb{F}_{p^2}$ maps into the 4512-bit field $\mathbb{F}_{p^{12}}^\times$, and the $p$-Weil pairing on $\mathcal{B}/\mathbb{F}_{q^2}$ maps into the 3012-bit field $\mathbb{F}_{q^2}^\times$.

**Cycle 5** Let $p = 2^{256} - 6539$, $\mathbb{F}_{p^2} = \mathbb{F}_p(\lambda)$ with $\lambda^2 = 2$, $\mathbb{F}_{p^4} = \mathbb{F}_{p^2}(\mu)$ with $\mu^2 = i$, and $\mathbb{F}_{p^8} = \mathbb{F}_{p^4}(\nu)$ with $\nu^2 = \mu$. Following Proposition 1, the curve $\mathcal{A}/\mathbb{F}_{p^8}: y^2 = x^3 + \alpha$ with $\alpha = \lambda + \nu$ is such that $\#\mathcal{A}(\mathbb{F}_{p^8}) = q$, where $q = p^8 - p^4 + 1$. Let $\mathbb{F}_{q^2} = \mathbb{F}_q(\xi)$ with $\xi^2 + 11 = 0$. Following Proposition 5, Bröker's algorithm outputs a supersingular curve $\mathcal{B}/\mathbb{F}_{q^2}: y^2 = x^3 + ax + b$ with $a, b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and $j(\mathcal{B}) \in \mathbb{F}_q$ whose group structure is $\mathcal{B}(\mathbb{F}_{q^2}) = \mathbb{Z}_{p^4(p^4-1)} \times \mathbb{Z}_{p^4(p^4-1)}$. The parameters $a, b$ and $j$ are in the file `cycle5.m`. Here $c_{\mathcal{A}} = 3$ and $c_{\mathcal{B}} = 1$: the $q$-Weil pairing on $\mathcal{A}/\mathbb{F}_{p^8}$ maps into the 6144-bit field $\mathbb{F}_{p^{24}}^{\times}$, and the $p$-Weil pairing on $\mathcal{B}/\mathbb{F}_{q^2}$ maps into the 4096-bit field $\mathbb{F}_{q^2}^{\times}$.

**Cycle 6** Let $p = 2^{512} - 258887$, $\mathbb{F}_{p^2} = \mathbb{F}_p(\lambda)$ with $\lambda^2 = 3$. Following Proposition 1, $\mathcal{E}/\mathbb{F}_{p^2}: y^2 = x^3 + \alpha$ with $\alpha = \lambda + 3$ is such that $\#\mathcal{E}(\mathbb{F}_{p^2}) = p^2 + p + 1$. Setting $g = \dim(\mathcal{A}) = 2$ gives $r = 4$, so from Theorem 4 we identify $\mathcal{A}/\mathbb{F}_{p^2}$ with

$$\mathcal{T}_4^0 = \{Q \in \mathcal{E}(\mathbb{F}_{p^8}) \colon \mathrm{Tr}_{\mathbb{F}_{p^8}/\mathbb{F}_{p^4}}(Q) = \mathcal{O}\},$$

i.e., $\mathcal{T}_4^0$ corresponds to the points of order $q = p^4 - p^2 + 1$ in $\mathcal{E}(\mathbb{F}_{p^8})$, whose order is $\#\mathcal{E}(\mathbb{F}_{p^8}) = q \cdot (p^4 + p^2 + 1)$. Let $\mathbb{F}_{q^2} = \mathbb{F}_q(\xi)$ with $\xi^2 + 7 = 0$. Following Proposition 5, Bröker's algorithm outputs a supersingular curve $\mathcal{B}/\mathbb{F}_{q^2}: y^2 = x^3 + ax + b$ with $a, b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and $j(\mathcal{B}) \in \mathbb{F}_q$ whose group structure is $\mathcal{B}(\mathbb{F}_{q^2}) = \mathbb{Z}_{p^2(p^2-1)} \times \mathbb{Z}_{p^2(p^2-1)}$. The parameters $a, b$ and $j$ are in the file `cycle6.m`. Here $c_{\mathcal{A}} = 6$ and $c_{\mathcal{B}} = 1$: the $q$-Weil pairing on $\mathcal{A}/\mathbb{F}_{p^4}$ maps into the 6144-bit field $\mathbb{F}_{p^{24}}^{\times}$, and the $p$-Weil pairing on $\mathcal{B}/\mathbb{F}_{q^2}$ maps into the 4096-bit field $\mathbb{F}_{q^2}^{\times}$.

**Cycle 7** Let $p, \mathbb{F}_{p^2}, q, \mathbb{F}_{q^2}$ and $\mathcal{B}/\mathbb{F}_{q^2}$ be as in Cycle 5. Following Proposition 1, $\mathcal{E}/\mathbb{F}_{p^2}: y^2 = x^3 + \alpha$ with $\alpha = \lambda + 4$ is such that $\#\mathcal{E}(\mathbb{F}_{p^2}) = p^2 + p + 1$. Setting $g = \dim(\mathcal{A}) = 4$ gives $r = 8$, so from Theorem 4 we identify $\mathcal{A}/\mathbb{F}_{p^2}$ with

$$\mathcal{T}_8^0 = \{Q \in \mathcal{E}(\mathbb{F}_{p^{16}}) \colon \mathrm{Tr}_{\mathbb{F}_{p^{16}}/\mathbb{F}_{p^8}}(Q) = \mathcal{O}\},$$

, $\mathcal{T}_4^0$ corresponds to the points of order $q$ in $\mathcal{E}(\mathbb{F}_{p^{16}})$, whose order is $\#\mathcal{E}(\mathbb{F}_{p^{16}}) = q \cdot (p^8 + p^4 + 1)$. Here $c_{\mathcal{A}} = 24$ and $c_{\mathcal{B}} = 1$: the $q$-Weil pairing on $\mathcal{A}/\mathbb{F}_{p^2}$ maps into the 12288-bit field $\mathbb{F}_{p^{48}}^{\times}$, and the $p$-Weil pairing on $\mathcal{B}/\mathbb{F}_{q^2}$ maps into the 4096-bit field $\mathbb{F}_{q^2}^{\times}$.

## 8 Hashing, group exponentiations, and pairing computations

Instantiating an efficient pairing-based cryptosystem typically requires much more than optimising the pairing $e \colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ itself. In most applications it is also desirable to be able to efficiently hash into (or randomly sample elements from) either or both of the groups $\mathbb{G}_1$ and $\mathbb{G}_2$, as well as being able to perform fast group exponentiations in some or all of $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$. In the case of modern SNARK constructions, there is also the core operation of efficiently computing enormous multiscalar multiplications in $\mathbb{G}_1$ and $\mathbb{G}_2$; these routines typically take many (e.g. thousands or millions of) curve points $P_i$ and scalars $n_i$, and output the point $\sum_i [n_i]P_i$. Furthermore, in the case of pairing-friendly cycles, we now have six groups to consider: the three pairing groups $\mathbb{G}_1^{\mathcal{A}}$, $\mathbb{G}_2^{\mathcal{A}}$ and $\mathbb{G}_T^{\mathcal{A}}$ corresponding to $\mathcal{A}$, as well as the three groups $\mathbb{G}_1^{\mathcal{B}}$, $\mathbb{G}_2^{\mathcal{B}}$ and $\mathbb{G}_T^{\mathcal{B}}$ corresponding to $\mathcal{B}$.

In this section we discuss efficiently hashing to, exponentiating in, and computing pairings between these six groups in the framework of our construction. In particular, we focus on these computations in the context of Theorem 4, since these constructions are of the most practical interest. Thus, throughout this section $\mathcal{A}/\mathbb{F}_{p^u}$ is a dimension-$g$ abelian variety, which we identify with a subgroup of $\mathcal{E}(\mathbb{F}_{p^{2ug}})$ where $\mathcal{E}$ is an elliptic curve defined over $\mathbb{F}_{p^u}$ (as defined in Theorem 4), and $\mathcal{B}$ is the supersingular elliptic curve from Proposition 5 defined over $\mathbb{F}_{q^2}$.

We note that this section is not intended to present any novel optimisations and, as such, we will not dig into the finer details of all of these computations. Instead, we aim to point implementers to the related literature in order to highlight the unique options that correspond to our construction. In comparison to the MNT cycle, where the available optimisations are rather limited, our construction can exploit a variety of tricks from the existing literature on optimised pairing-based protocols. We do not intend to claim that any of our observations are the most efficient algorithms for these operations, but merely wish to show the myriad of optimisations that can be applied in our setting. Implementers wishing to experiment with our constructions may be pleased to read the following remark.

*Remark 2 (Elliptic curve arithmetic only).* Although Theorem 4 can be used to produce an abelian variety $\mathcal{A}$ of dimension $g = 2^{\ell}$ for any $\ell \geq 0$, we re-emphasise that all of the arithmetic is implementable as elliptic curve arithmetic. Even in the case of the two propositions involving abelian surfaces in Section 6, we note that both of these constructions can be recast as invocations of Theorem 4, and that elliptic curve arithmetic can be used in place of genus 2 arithmetic there as well.

### 8.1 Efficient group exponentiations

We first point out that producing a cycle $A \rightleftharpoons \mathcal{B}$ by combining an $\mathcal{A}$ from Theorem 4 with a $\mathcal{B}$ from Proposition 5 typically produces $\mathbb{G}_1^{\mathcal{A}}$, $\mathbb{G}_2^{\mathcal{A}}$, $\mathbb{G}_1^{\mathcal{B}}$ and $\mathbb{G}_2^{\mathcal{B}}$ as prime order subgroups of a larger group whose cardinality is divisible by 4. Thus, the twisted Edwards [7] and/or Montgomery [46] models can be used in order to exploit efficient curve arithmetic in all of these groups.

**Exponentiations in $\mathbb{G}_1^{\mathcal{A}}$.** Let $\pi$ be the $p^u$-power Frobenius map on elliptic curve $\mathcal{E}/\mathbb{F}_{p^u}$. Then $\pi^i$ for $1 \leq i \leq r-1$ can be used to accelerate (multi)scalar multiplications in $\mathbb{G}_1^{\mathcal{A}} \subset \mathcal{E}(\mathbb{F}_{p^{ur}})$ using the techniques by Galbraith and Scott [25], and Scott et al. [52, §3]. It may also be helpful to additionally incorporate the endomorphism $\phi\colon \mathcal{E} \to \mathcal{E}$, $(x, y) \mapsto (\xi x, y)$ where $\xi$ is a non-trivial cube root of unity in $\mathbb{F}_{p^2}$ [23, §4].

**Exponentiations in $\mathbb{G}_2^{\mathcal{A}}$.** The same speedups will work in $\mathbb{G}_2^{\mathcal{A}} \subset \mathcal{E}(\mathbb{F}_{p^{urc_{\mathcal{A}}}})$, but larger $c_{\mathcal{A}}$ allows even more powers of $\pi$ to be exploited. Furthermore, since $\mathcal{E}/\mathbb{F}_{p^u}$ has $j$-invariant $j = 0$ and $c_{\mathcal{A}} = 3 \cdot 2^{g-1}$, when $g > 1$ the sextic twist from [54, Proposition X.5.4] will be available to transport operations in $\mathbb{G}_2$ into a subfield whose degree is a factor 6 smaller.

**Exponentiations in $\mathbb{G}_1^{\mathcal{B}}$ and $\mathbb{G}_2^{\mathcal{B}}$.** In the context of our constructions, Bröker's algorithm outputs a supersingular curve $\mathcal{B}$ that is minimally defined over $\mathbb{F}_{q^2}$. However, it is typically produced by starting with a curve $\mathcal{B}'/\mathbb{F}_q$ that is lifted to $\mathcal{B}'(\mathbb{F}_{q^2})$, and then taking $\mathcal{B}$ as the quadratic twist of $\mathcal{B}'$ over $\mathbb{F}_{q^2}$—see [13, §3]. This means both $\mathbb{G}_1^{\mathcal{B}}$ and $\mathbb{G}_2^{\mathcal{B}}$ can both exploit the Galbraith-Lin-Scott (GLS) endomorphism in [23, Theorem 2].

**Exponentiations in $\mathbb{G}_T^{\mathcal{A}}$ and $\mathbb{G}_T^{\mathcal{B}}$.** Elements in $\mathbb{G}_T^{\mathcal{A}}$ and $\mathbb{G}_T^{\mathcal{B}}$ lie in the "cyclotomic groups" of the extension fields $\mathbb{F}_{p^{u \cdot c_{\mathcal{A}}}}$ and $\mathbb{F}_{q^{v \cdot c_{\mathcal{B}}}}$, so can use the respective Frobenius operations to speed up group exponentiations—see the works by Stam and Lenstra [56] and Galbraith and Scott [25].

### 8.2 Hashing

The first step in hashing to both the $\mathcal{A}$ and $\mathcal{B}$ groups involves taking a random point on the respective varieties. In their seminal paper [11], Boneh and Franklin described an efficient `MapToPoint` algorithm that can produce uniform points on the curve $\mathcal{E}/\mathbb{F}_p\colon y^2 = x^3 + 1$ with $p \equiv 2 \bmod 3$ by taking $y_0$ as a random element of $\mathbb{F}_p$ (via a presumably uniform hash function $H\colon \{0,1\}^* \to \mathbb{F}_p$), then computing the point $Q = (x_0, y_0) = ((y_0^2 - 1)^{1/3}, y_0)$, before outputting the image $Q' = [h]Q$ of a cofactor multiplication. This hashing is made easy by virtue of the fact that the cube root function $f\colon \mathbb{F}_p \to \mathbb{F}_p, x \mapsto x^{1/3}$ is a bijection.

In our case we also have $p \equiv 2 \bmod 3$, but our supersingular curves are defined over $\mathbb{F}_{p^2}$, where the cube root function is unfortunately no longer a bijection. Thus, we are also faced with the same hashing difficulties that typical ordinary curves have, which is the uniform sampling of random points on $\mathcal{E}$. The literature on this specific issue is vast in and of itself, so below we simply focus on the subsequent hashing step of performing the cofactor multiplication efficiently.

**Hashing to $\mathbb{G}_1^{\mathcal{A}}$ and $\mathbb{G}_2^{\mathcal{A}}$.** Recall from Section 7 that $\mathbb{G}_1^{\mathcal{A}}$ is the set of points of order $q = (p^{ug} - p^{ug/2} + 1)$ in $\mathcal{E}(\mathbb{F}_{p^{ur}})$, which can be obtained by a scalar multiplication of a random point in $\mathcal{E}(\mathbb{F}_{p^{ur}})$ by the cofactor $h = (p^{ug} + p^{ug/2} + 1)$. These special types of cofactors can exploit additional tricks related to Frobenius endomorphisms—see [52]. In the context of SNARK constructions, it may also be convenient to exploit a distortion map between $\mathbb{G}_1^{\mathcal{A}}$ and $\mathbb{G}_2^{\mathcal{A}}$. For example, the curve $\mathcal{E}/\mathbb{F}_{p^2} : y^2 = x^3 + \alpha$ with $\alpha \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ in Proposition 2 has a convenient distortion map—see [38, Table 1]. Alternatively, hashing to $\mathbb{G}_2^{\mathcal{A}}$ can be performed via a larger cofactor multiplication, which can exploit the same tricks (as well as the sextic twist we touched on in §8.1).

**Hashing to $\mathbb{G}_1^{\mathcal{B}}$ and $\mathbb{G}_2^{\mathcal{B}}$.** The techniques in [52] are unlikely to be as useful for cofactor multiplications on $\mathcal{B}$, but the GLS endomorphism can be used to accelerate cofactor multiplications in exactly the same way as it was described in §8.1. Again, there are distortion maps available between $\mathbb{G}_1^{\mathcal{B}}$ and $\mathbb{G}_2^{\mathcal{B}}$ [62, Theorem 5] that may be useful in a given SNARK construction. If not, then the fact that all of the $p$-torsion on $\mathcal{B}$ is minimally defined over $\mathbb{F}_{q^2}$ might make it difficult to hash into the same specific order-$p$ subgroups via a cofactor multiplication.

### 8.3 Pairing computation

As we discussed in §3.2, the earliest instantiations of bilinear pairings used supersingular curves. Thus, there is a vast amount of literature dedicated to optimising such pairings. In the case of our constructions, there are subtle differences that may prevent a trivial adoption of these optimisations, but nevertheless the main ideas can still be applied to accelerate the pairings on both $\mathcal{A}$ and $\mathcal{B}$.

**Efficient pairings on $\mathcal{A}$.** Let $\mathcal{E}$ and $\mathcal{A}$ be as in Theorem 4. (In the case where $\mathcal{E}$ is instead the curve in Proposition 2, see the fast pairing techniques in [59].) Together with $\gamma\colon (x, y) \mapsto (\xi x, -y)$, which has order 6 in $\mathrm{Aut}(\mathcal{E})$, and a distortion map $\psi$, the variety $\mathcal{A}$ satisfies the conditions in [2, Theorem 1], meaning that the $\eta_T$ pairing can be applied. Moreover, when $g > 1$, the sextic twist mentioned in §8.1 will help accelerate the pairing. Finally, the $p^u$-power Frobenius map can be used to accelerate the final exponentiation using the techniques in [25,53].

**Efficient pairings on $\mathcal{B}$.** The $\eta_T$ pairing can be invoked on $\mathcal{B}$ by combining the GLS endomorphism with a distortion map under the conditions in [2, Theorem 1], but the automorphism group of $\mathcal{B}$ will be smaller which means the loop shortening factor will not be as large as for $\mathcal{A}$.

### 8.4 Other optimisations

**Compression.** Depending on the SNARK construction and on the target application, it may be desirable to exploit the compression and decompression techniques that Rubin and Silverberg gave for the trace zero varieties we exploited in this paper—see [50, §10-11].

**2-adicity.** For efficiency reasons, it is desirable for pairing-based SNARKs to work with (sub)groups of prime order $r$ such that $r - 1$ is divisible by a large power of 2—see [6, §3.2]. In the context of cycles, this means we would like both $p$ and $q$ to be such that $2^e \mid p - 1$ and $2^{e'} \mid q - 1$. In the case of the MNT cycle for which $p$ and $q$ come as the solutions of Pell equations, it is difficult to obtain large 2-adicity for primes of a prescribed bitlength—see [33] and the examples in [6, §3.2].

In the case of our constructions where suitable primes are plentiful, one can search for primes of a given bitlength with very large 2-adicity. Recall that the examples in §7.2 searched for the largest primes $p$ of a prescribed bitlength $\ell$ such that $q = p^u - p^{u/2} + 1$ is also prime; this was done to illustrate how quickly a suitable prime $p = 2^\ell - m$ is found by showing how small $m$ is. Alternatively, we could substitute in the following primes that were found in a modified search that maximises the 2-adicity subject to the prescribed bit length. Note that in our constructions the 2-adicity of

$q-1$ is always guaranteed to be larger than that of $p-1$, since $q-1 = p^u - p^{u/2} = p^{u/2}(p^{u/2}-1)$, meaning that $2(p-1) \mid q-1$. Let $v_2(x)$ be the largest power of 2 dividing $x$. The 160-bit prime in Cycles 1 and 2 could be replaced with the 160-bit prime $p = 2^{144} \cdot 39991 + 1$, which gives $v_2(p-1) = 144$ and $v_2(q-1) = 145$. The 224-bit prime in Cycle 3 could be replaced with the 224-bit prime $p = 2^{208} \cdot 36841 + 1$, which gives $v_2(p-1) = 208$ and $v_2(q-1) = 210$. The 377-bit prime in Cycle 4 could be replaced with the 377-bit prime $p = 2^{361} \cdot 34631 + 1$, which gives $v_2(p-1) = 361$ and $v_2(q-1) = 362$. The 256-bit prime in Cycle 5 could be replaced with the 256-bit prime $p = 2^{241} \cdot 27101 + 1$, which gives $v_2(p-1) = 241$ and $v_2(q-1) = 243$. And, the 512-bit prime in Cycles 6 and 7 could be replaced with the 512-bit prime $p = 2^{494} \cdot 174475 + 1$, which gives $v_2(p-1) = 494$ and $v_2(q-1) = 495$.

Pairing-based SNARKs that benefit from 2-adicity typically only need powers of 2 that are far smaller than those we can obtain above. Once that threshold has been met, extra 2-adicity does not give additional benefits and is therefore overkill. Thus, in practice one would be able to combine the requisite 2-adicity with other desirable properties of the target primes, e.g. primes that offer fast field arithmetic.

**Acknowledgements.** We thank Gaurish Korpal for his extensive feedback, and thank the anonymous reviewers for their insightful comments on an earlier version of this paper.

## References

1. D. F. Aranha, Y. El Housni, and A. Guillevic. A survey of elliptic curves for proof systems. *Designs, Codes and Cryptography*, pages 1–46, 2022.
2. P. S. L. M. Barreto, S. D. Galbraith, C. O'hEigeartaigh, and M. Scott. Efficient pairing computation on supersingular abelian varieties. *Des. Codes Cryptogr.*, 42(3):239–271, 2007.
3. P. S. L. M. Barreto, B. Lynn, and M. Scott. Constructing elliptic curves with prescribed embedding degrees. In *SCN 2002*, volume 2576 of *LNCS*, pages 257–267. Springer, 2002.
4. P. S. L. M. Barreto and M. Naehrig. Pairing-friendly elliptic curves of prime order. In *SAC 2005*, volume 3897 of *LNCS*, pages 319–331. Springer, 2005.
5. M. Bellés-Muñoz, J. Jiménez Urroz, and J. Silva. Revisiting cycles of pairing-friendly elliptic curves. In *CRYPTO 2023*, volume 14082 of *LNCS*, pages 3–37. Springer, 2023.
6. E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza. Scalable zero knowledge via cycles of elliptic curves. In *CRYPTO 2014*, volume 8617 of *LNCS*, pages 276–294. Springer, 2014.
7. D. J. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters. Twisted Edwards curves. In *AFRICACRYPT 2008*, volume 5023 of *LNCS*, pages 389–405. Springer, 2008.
8. N. Bitansky, R. Canetti, A. Chiesa, and E. Tromer. Recursive composition and bootstrapping for SNARKS and proof-carrying data. In *STOC'13*, pages 111–120. ACM, 2013.
9. I. F. Blake, G. Seroussi, and N. P. Smart. *Elliptic curves in cryptography*, volume 265. Cambridge university press, 1999.
10. I. F. Blake, G. Seroussi, and N. P. Smart. *Advances in elliptic curve cryptography*, volume 317. Cambridge University Press, 2005.
11. D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. In *CRYPTO 2001*, pages 213–229. Springer, 2001.
12. S. Bowe, J. Grigg, and D. Hopwood. Recursive proof composition without a trusted setup, 2019. `https://eprint.iacr.org/2019/1021`.
13. R. Bröker. Constructing supersingular elliptic curves. *J. Comb. Number Theory*, 1(3):269–273, 2009.
14. R. Bröker and P. Stevenhagen. Efficient cm-constructions of elliptic curves over finite fields. *Mathematics of Computation*, 76(260):2161–2179, 2007.
15. J. H. Cheon. Security analysis of the strong Diffie-Hellman problem. In *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 1–11. Springer, 2006.
16. A. Chiesa, L. Chua, and M. Weidner. On cycles of pairing-friendly elliptic curves. *SIAM Journal on Applied Algebra and Geometry*, 3(2):175–192, 2019.
17. C. Costello, C. Fournet, J. Howell, M. Kohlweiss, B. Kreuter, M. Naehrig, B. Parno, and S. Zahur. Geppetto: Versatile verifiable computation. In *IEEE SP*, pages 253–270. IEEE Comp. Soc., 2015.
18. D. Freeman. Constructing pairing-friendly elliptic curves with embedding degree 10. In *ANTS-VII*, volume 4076 of *LNCS*, pages 452–465. Springer, 2006.

19. D. Freeman. A generalized Brezing-Weng algorithm for constructing pairing-friendly ordinary abelian varieties. In *Pairing 2008*, volume 5209 of *LNCS*, pages 146–163. Springer, 2008.
20. G. Frey. Applications of arithmetical geometry to cryptographic constructions. In *Finite Fields and Applications*, pages 128–161. Springer, 2001.
21. G. Frey, M. Müller, and H. G. Rück. The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems. *IEEE Tr. Inf. Theory*, 45(5):1717–1719, 1999.
22. S. D. Galbraith. Supersingular curves in cryptography. In *ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 495–513. Springer, 2001.
23. S. D. Galbraith, X. Lin, and M. Scott. Endomorphisms for faster elliptic curve cryptography on a large class of curves. In *EUROCRYPT 2009*, volume 5479 of *LNCS*, pages 518–535. Springer, 2009.
24. S. D. Galbraith, J. Pujolàs, C. Ritzenthaler, and B. Smith. Distortion maps for supersingular genus two curves. *Journal of Mathematical Cryptology*, 3(1):1–18, 2009.
25. S. D. Galbraith and M. Scott. Exponentiation in pairing-friendly groups using homomorphisms. In *Pairing 2008*, volume 5209 of *LNCS*, pages 211–224. Springer, 2008.
26. P. Gaudry, E. Thomé, N. Thériault, and C. Diem. A double large prime variation for small genus hyperelliptic index calculus. *Mathematics of computation*, 76(257):475–492, 2007.
27. J. Groth. Simulation-sound NIZK proofs for a practical language and constant size group signatures. In *ASIACRYPT 2006*, volume 4284 of *LNCS*, pages 444–459. Springer, 2006.
28. J. Groth. Short pairing-based non-interactive zero-knowledge arguments. In *ASIACRYPT 2010*, volume 6477 of *LNCS*, pages 321–340. Springer, 2010.
29. J. Groth. On the size of pairing-based non-interactive arguments. In *EUROCRYPT 2016*, volume 9666 of *LNCS*, pages 305–326. Springer, 2016.
30. J. Groth, R. Ostrovsky, and Amit Sahai. Non-interactive zaps and new techniques for NIZK. In *CRYPTO 2006*, volume 4117 of *LNCS*, pages 97–111. Springer, 2006.
31. J. Groth and A. Sahai. Efficient non-interactive proof systems for bilinear groups. In *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 415–432. Springer, 2008.
32. IEEE P1363 Working Group. Standard specifications for public-key cryptography – IEEE Std 1363-2000, 2000.
33. A. Guillevic. Pairing-friendly curves. `https://members.loria.fr/AGuillevic/pairing-friendly-curves/`, 2021.
34. T. Honda. Isogeny classes of abelian varieties over finite fields. *Journal of the Mathematical Society of Japan*, 20(1-2):83–95, 1968.
35. Y. El Housni and A. Guillevic. Families of SNARK-friendly 2-chains of elliptic curves. In *EUROCRYPT 2022*, volume 13276 of *LNCS*, pages 367–396. Springer, 2022.
36. E. W. Howe, E. Nart, and C. Ritzenthaler. Jacobians in isogeny classes of abelian surfaces over finite fields. In *Annales de l'Institut Fourier*, volume 59, pages 239–289, 2009.
37. A. Joux. A one round protocol for tripartite Diffie–Hellman. In *ANTS IV*, pages 385–393. Springer, 2000.
38. A. Joux and K. Nguyen. Separating Decision Diffie-Hellman from Computational Diffie-Hellman in Cryptographic Groups. *J. Cryptol.*, 16(4):239–247, 2003.
39. K. Karabina and E. Teske. On prime-order elliptic curves with embedding degrees k = 3, 4, and 6. In *ANTS-VIII*, volume 5011 of *LNCS*, pages 102–117. Springer, 2008.
40. N. Koblitz. Hyperelliptic cryptosystems. *Journal of cryptology*, 1:139–150, 1989.
41. N. Koblitz and A. Menezes. Pairing-based cryptography at high security levels. In *IMACC*, volume 3796 of *LNCS*, pages 13–36. Springer, 2005.
42. J. Lee. Dory: Efficient, transparent arguments for generalised inner products and polynomial commitments. In *TCC*, volume 13043 of *LNCS*, pages 1–34. Springer, 2021.
43. D. Maisner, E. Nart, and E. W. Howe. Abelian surfaces over finite fields as jacobians. *Experimental mathematics*, 11(3):321–337, 2002.
44. A. Menezes, S. A. Vanstone, and T. Okamoto. Reducing elliptic curve logarithms to logarithms in a finite field. In *STOC*, pages 80–89. ACM, 1991.
45. A. Miyaji, M. Nakabayashi, and S. Takano. Characterization of elliptic curve traces under FR-reduction. In *ICISC 2000*, volume 2015 of *LNCS*, pages 90–108. Springer, 2000.
46. P. L. Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Mathematics of computation*, 48(177):243–264, 1987.
47. F. Morain. Classes d'isomorphismes des courbes elliptiques supersingulières en caractéristique $\geq 3$. *Utilitas Mathematica*, 52, 1997.
48. J. M. Pollard. Monte Carlo methods for index computation (mod $p$). *Mathematics of computation*, 32(143):918–924, 1978.

49. K. Rubin and A. Silverberg. Supersingular abelian varieties in cryptology. In *CRYPTO 2002*, volume 2442 of *LNCS*, pages 336–353. Springer, 2002.
50. K. Rubin and A. Silverberg. Using abelian varieties to improve pairing-based cryptography. *J. Cryptol.*, 22(3):330–364, 2009.
51. R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystems based on pairing. *SCIS*, 2000.
52. M. Scott, N. Benger, M. Charlemagne, L. J. Dominguez Perez, and E. J. Kachisa. Fast hashing to $G_2$ on pairing-friendly curves. In *Pairing 2009*, volume 5671 of *LNCS*, pages 102–113. Springer, 2009.
53. M. Scott, N. Benger, M. Charlemagne, L. J. Dominguez Perez, and E. J. Kachisa. On the final exponentiation for calculating pairings on ordinary elliptic curves. In *Pairing 2009*, volume 5671 of *LNCS*, pages 78–88. Springer, 2009.
54. J. H. Silverman. *The arithmetic of elliptic curves*, volume 106. Springer, 2009.
55. J. H. Silverman and K. E. Stange. Amicable pairs and aliquot cycles for elliptic curves. *Exp. Math.*, 20(3):329–357, 2011.
56. M. Stam and A. K. Lenstra. Efficient subgroup exponentiation in quadratic and sixth degree extensions. In *CHES*, volume 2523, pages 318–332. Springer, 2002.
57. A. V. Sutherland. Computing hilbert class polynomials with the Chinese remainder theorem. *Math. Comput.*, 80(273):501–538, 2011.
58. J. Tate. Classes d'isogénie des variétés abéliennes sur un corps fini (d'après t. honda). In *Séminaire Bourbaki vol. 1968/69 Exposés 347-363*, pages 95–110. Springer, 2006.
59. T. Teruya, K. Saito, N. Kanayama, Y. Kawahara, T. Kobayashi, and E. Okamoto. Constructing symmetric pairings over supersingular elliptic curves with embedding degree three. In *Pairing 2013*, volume 8365 of *LNCS*, pages 97–112. Springer, 2013.
60. J. Thaler. Proofs, arguments, and zero-knowledge. `https://people.cs.georgetown.edu/jthaler/ProofsArgsAndZK.pdf`, 2023.
61. P. Valiant. Incrementally verifiable computation or proofs of knowledge imply time/space efficiency. In *TCC*, volume 4948 of *LNCS*, pages 1–18. Springer, 2008.
62. E. R. Verheul. Evidence that XTR is more secure than supersingular elliptic curve cryptosystems. *J. Cryptol.*, 17(4):277–296, 2004.
63. W. C. Waterhouse. Abelian varieties over finite fields. In *Annales scientifiques de l'École normale supérieure*, volume 2, pages 521–560, 1969.
64. H. J. Zhu. Group structures of elementary supersingular abelian varieties over finite fields. *Journal of Number Theory*, 81(2):292–309, 2000.