

Supersingularity and Superspeciality Verification of Abelian Surfaces

Maria Corte-Real Santos¹, Gioella Lorenzon², and Krijn Reijnders²

¹ École Normale Supérieure de Lyon, CNRS

² COSIC, KU Leuven

Abstract. Supersingular abelian surfaces are essential in isogeny-based cryptography. Despite this, we have no efficient algorithm to verify if a given abelian surface is supersingular. In this work, we initiate this research topic by giving an efficient Monte Carlo algorithm to verify if an abelian surface over $\mathbb{F}_p$ is supersingular in $O(\log p)$ with negligible failure probability, and an efficient conclusive algorithm if the order is smooth. We derive this algorithm by a careful analysis on the structure of supersingular Jacobians over $\mathbb{F}_p$. Furthermore, we derive efficient algorithms to verify if an abelian variety of any dimension is minimal or maximal, and to verify if a Jacobian of any dimension is superspecial.

Keywords: post-quantum cryptography, isogenies, Jacobians, supersingularity

1 Introduction

Since the spectacular break of SIDH/SIKE [10, 25, 33], higher-dimensional techniques have revolutionized isogeny-based cryptography. Modern protocols, such as the signature schemes SQIsign [1] and PRISM [3], the NIKE MIKE [35], or the KEM POKE [5] heavily rely on higher-dimensional isogenies for both performance and small sizes. Abelian varieties of dimension $g > 1$ have therefore become fundamental objects in isogeny-based cryptography. More precisely, such protocols rely on *supersingular* principally polarized abelian varieties, and often even the more restricted *superspecial* principally polarized abelian varieties. With recent developments, such as the module action framework [4, 35] or the Shimura class group action on abelian surfaces [11], validating supersingularity becomes crucial to security. This can be seen as the higher-dimensional equivalent of public key validation in CSIDH [12], where omitting key validation would introduce a significant attack vector for an adversary.

Supersingular elliptic curves. Supersingularity verification of elliptic curves has been studied extensively in both mathematical and cryptographic literature. Sutherland [42] initiated this study by describing a Monte Carlo test for elliptic curves over $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$: take a random point $P \in E(\mathbb{F}_q)$ and check if $[p]P = \pm P$. The probability of a false positive is $O(q^{-\frac{1}{2}})$ and therefore suitable for almost all cryptographic purposes, where q is large.

Nevertheless, such a test does not *conclusively prove* that a curve is supersingular. To do so, Sutherland describes an algorithm based on the depth of isogeny volcanoes. In CSIDH [12], the supersingularity test is instead performed by verifying that the order of a random point is larger than $4\sqrt{p}$, which, by the bound on width of the Hasse-Weil interval, proves that the order of the curve is $p + 1$, and therefore the curve is supersingular. dCSIDH [8] optimizes this approach for primes p where $2^f \mid p + 1$ with $f > \frac{1}{2} \log p$, e.g., most primes used in current-day isogeny-based cryptography. Doliskani [18] describes an algorithm based on polynomial identity testing to establish supersingularity, which uses the fact that the p -th division polynomial $\psi_p(x)$ is precisely ± 1 for supersingular curves, as these have p -rank 0. Banegas, Gilchrist, and Smith [2] give an in-depth performance comparison between these algorithms, and reinterpret Doliskani's test using Montgomery arithmetic, for which Robert [34] gives a reinterpretation as a self-pairing using cubical arithmetic. Lastly, in [31], pairings are used to optimize the verification of the order of the curve, moving much of the computational cost from curve arithmetic to field arithmetic.

Supersingular and superspecial abelian surfaces. Moving up in dimension, there is no single analogue of supersingularity. Instead, there are several inequivalent generalizations organized by the Ekedahl–Oort stratification. As a leading example in dimension 2, supersingularity for elliptic curves may be generalized as either supersingularity of an abelian surface, or the more specific notion of superspeciality. The latter property is often the right generalization for cryptographic purposes. Although literature exists which studies this classification of abelian varieties in this stratification, we are not aware of literature addressing the specific question of *efficiently* verifying the supersingularity and superspeciality of abelian surfaces over a finite field. To the best of our knowledge, the best known methods to verify such results depend on point-counting algorithms or L -polynomial computations, which are prohibitively slow for the large primes used in isogeny-based cryptography. In this work, we present an efficient algorithm for supersingularity testing of abelian surfaces over $\mathbb{F}_p$. We furthermore study the question of minimality and maximality of abelian varieties, which allows us to efficiently verify superspeciality of Jacobians over $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$.

Key Example. We demonstrate the core idea of our simple and efficient probabilistic verification with the following key example, in which we verify minimality or maximality of an abelian variety. This property implies superspeciality, and therefore supersingularity [22, Thm. 5.3].

Algorithm 1 *Let A be an abelian surface over $\mathbb{F}_{p^2}$. Let $P \xleftarrow{\$} A(\mathbb{F}_{p^2})$.*

- If $[p + 1]P = \mathbf{0}_A$, return **true**.
- Otherwise, return **false**.

The algorithm for minimal abelian surfaces replaces $p + 1$ by $p - 1$. The probability of a false positive is $O(p^{-1})$, and is thus negligibly small for large primes.

This follows from what we call the *width-bound argument*, used by Sutherland for elliptic curves [42]. In [Theorem 4.1](#), we generalize this argument to abelian varieties. However, this algorithm only works for minimal and maximal varieties, whereas general supersingularity testing is much more complicated. Already for the cases of abelian surfaces over $\mathbb{F}_p$, we require a deeper understanding of the group structures of supersingular abelian surfaces and their twists. Furthermore, the above algorithm can never *conclusively prove* that an abelian surface is supersingular or even superspecial, which requires additional understanding of the isotropic subgroups of abelian surfaces.

Contributions. We provide the first practical polynomial time supersingularity and superspeciality verification algorithms for abelian surfaces over $\mathbb{F}_p$. We develop both probabilistic and conclusive algorithms.

1. In [Section 3](#), we analyze the structure of supersingular and superspecial Jacobians over $\mathbb{F}_p$, resulting in three key results:
 - (a) [Theorem 3.12](#), which describes the possible orders of supersingular Jacobians over $\mathbb{F}_{p^2}$;
 - (b) [Table 3](#), giving the group structures of supersingular Jacobians over $\mathbb{F}_p$;
 - (c) [Theorem 3.26](#), which classifies superspecial Jacobians using the automorphism group of the associated genus-2 curve.
 These results underlie both the probabilistic and conclusive testing.
2. In [Section 4](#), we derive algorithms for *probabilistic verification* of extremality, supersingularity and superspeciality of abelian surfaces.
 - (a) In [Algorithm 2](#) and [Theorem 4.1](#), we generalize [Algorithm 1](#) to verify minimality and maximality of an abelian variety of any dimension.
 - (b) Using [Theorem 3.26](#) we construct [Algorithm 3](#), an efficient algorithm for testing superspeciality of Jacobians over $\mathbb{F}_p$. Its correctness and runtime are proved in [Theorem 4.2](#). We show a similar result for superspecial Jacobians over $\mathbb{F}_{p^2}$ in [Appendix B](#).
 - (c) In [Algorithm 4](#) we give a $O(\log p)$ Monte Carlo supersingularity test for abelian surfaces over $\mathbb{F}_p$, with all arithmetic performed over $\mathbb{F}_p$. Its correctness and runtime are based on [Theorem 4.7](#).
3. In [Section 5](#), we derive algorithms for *conclusive verification* of supersingularity for abelian surfaces over $\mathbb{F}_p$, summarized in [Corollaries 5.5](#) and [5.10](#). We furthermore analyze the factorization and discrete logarithm requirements for these algorithms, and specialize to a case of specific cryptographic interest, i.e. when $2^f \mid p+1$, with f close to $\log p$.

We give an overview of all verification algorithms in this work in [Table 1](#) (probabilistic tests) and [Table 2](#) (conclusive tests), listing the setting in which each algorithm applies, its complexity, and either its failure probability or its structural requirements. We implemented these algorithms in **Magma**, and benchmark their performance in [Section 6](#). The code is available at the following repository,

<https://github.com/KULeuven-COSIC/supersingularity-and-superspeciality>.

Table 1: Overview of probabilistic (Monte Carlo) verification algorithms in this work. Complexities count field operations in the stated field, and $q = p$ or p^2 .

Algorithm	Verifies	Variety	Complexity	False pos.
Algorithm 1	maximality	$A/\mathbb{F}_{p^2}$	$O(\log p)$	$O(p^{-1})$
Algorithm 2	maximality	$A/\mathbb{F}_q$, any g	$O(\log p)$	$O(p^{-1})$
Algorithm 3	superspeciality	$\mathcal{J}/\mathbb{F}_q$, any g	$O(g \log p)$	$O((g-1)p^{-1})$
Algorithm 4	supersingularity	$A/\mathbb{F}_p$	$O(\log p)$	$O(p^{-1/2})$

Table 2: Overview of conclusive verification algorithms in this work. In the first three rows, $n = p^2 - bp + 1$ for $b \in \{-1, 0, 1\}$ and $n = p \mp 1$ for $b = \pm 2$, and $\omega(n)$ is the number of distinct prime factors of n . We assume the factorization of n is known. Complexities count field operations in the stated field.

Algorithm	Verifies	Setting	Complexity	Requirements
Corollary 5.5	supersing.	$b = 2$ over $\mathbb{F}_p$	$O(\log \omega(n) \log p)$	factorization of n
Corollary 5.5	supersing.	$b = -2$ over $\mathbb{F}_p$	$O(\log \omega(n) \log p)$	DLog in μ_{p+1}
Corollary 5.10	supersing.	$b \in \{-1, 0, 1\}$ over $\mathbb{F}_p$	$O(\log \omega(n) \log p)$	works over $\mathbb{F}_{p^k}$
Lemma 5.15	supersing.	$b = \pm 2$ over $\mathbb{F}_p$	$O(\log p)$	$p = c \cdot 2^f \pm 1$
Algorithm 5	maximality	$b = -2$ over $\mathbb{F}_{p^2}$	$O(\log p)$	DLog in μ_{p+1}
Lemma 5.16	maximality	$b = -2$ over $\mathbb{F}_{p^2}$	$O(\log p)$	$p = c \cdot 2^f - 1$

Some of this work is phrased using Jacobians, representing principally polarized abelian surfaces that are neither products nor Weil restrictions. However, in practice we need fairly little machinery to apply our algorithms: the probabilistic algorithms rely only on uniform random sampling and scalar multiplication, whereas the conclusive algorithms additionally require pairing computations and discrete logarithms. Our conventions and the role of the principal polarization are detailed in [Section 2](#).

Related Work. The task of verifying supersingularity or superspeciality in dimension 2 fits into the much more general task of classifying curves and principally polarized abelian varieties according to their p -rank. This is called the Ekedahl–Oort stratification [\[28\]](#), and has been widely studied (see, e.g., [\[17, 27\]](#)).

In dimension 2, one may directly detect supersingularity by computing the L -polynomial of the abelian surface or, equivalently, the characteristic polynomial of Frobenius. Methods to do so often rely on generalizations of Schoof-like algorithms to determine the number of points on a curve or variety. Most directly applicable is the Schoof–Pila algorithm [\[29\]](#), and subsequent improvements [\[20, 24\]](#). Of particular interest to this work is the article by Shi [\[39\]](#) on lifting L -polynomials of genus-2 curves. For superspeciality, the most well-

known approach relies on computation of the Cartier-Manin or Hasse-Witt matrix, which also allows one to verify supersingularity. In [Section 6](#), we compare these approaches to the algorithms given in this work.

Acknowledgements. This work is supported by the European Research Council under grant No. 101116169 (AGATHA CRYPTY), under the European Union’s Horizon 2020 research and innovation programme (grant agreement ISOCRYPT – No. 101020788), by the Research Council KU Leuven grant C14/24/099 and by CyberSecurity Research Flanders with reference number VOEWICS02. The second-listed author is additionally supported by the Fonds voor Wetenschappelijk Onderzoek (FWO) under grant number 1139225N.

2 Preliminaries

We assume basic familiarity with elliptic curves and their arithmetic, see [\[40\]](#) for more background. Throughout, $\mathbb{F}_q$ denotes a finite field of characteristic p , and $\overline{\mathbb{F}}_p$ its algebraic closure.

2.1 Supersingular Elliptic Curves

Supersingularity of elliptic curves over $\mathbb{F}_q$ can be defined by several equivalent properties. Among these, is that their endomorphism ring is isomorphic to a maximal order in a quaternion algebra, whereas ordinary curves have endomorphism rings isomorphic to quadratic orders. For this work, essential properties of supersingular elliptic curves are that their p -rank is 0, meaning that $E[p](\overline{\mathbb{F}}_p) = \mathbf{0}$, and that the trace of the characteristic polynomial of Frobenius is a multiple of p . A shared feature of all these characteristics is that they enforce strict group structures on $E(\mathbb{F}_q)$, in contrast with ordinary curves, whose group structures are much more flexible.

Supersingular curves are fundamental in isogeny-based cryptography, as their rich endomorphism ring structures allow for flexibility and efficiency in the design of cryptographic algorithms. Furthermore, the precise control on the group structure allows for efficient isogeny computations using Velu’s formulas [\[43\]](#).

2.2 Abelian Varieties

A *polarization* of an abelian variety A is an isogeny λ between A and its dual $\hat{A}$ induced by an ample line bundle. Such a polarization is *principal* whenever λ is an isomorphism. In this work we mostly focus on abelian surfaces, which are abelian varieties of dimension 2. A principally polarized abelian surface over $\mathbb{F}_q$ is either the Jacobian of a hyperelliptic curve of genus 2, the product of two elliptic curves over $\mathbb{F}_q$, or the Weil restriction of an elliptic curve over $\mathbb{F}_{q^2}$. All three come equipped with a canonical principal polarization.

For brevity, we will often use the term abelian surface instead of *principally polarized abelian surfaces*. We remark, however, that the polarization is used

in only two ways: through the classification above, and results derived from it (e.g., [Corollary 3.22](#) and [Theorem 3.26](#)); and through the Weil-pairing isotropy conditions of (1), used in the pairing-based conclusive tests in [Section 5](#).

Furthermore, in this work, we mainly focus on Jacobians of hyperelliptic curves, as supersingularity testing for Weil restrictions and products is easy: over a quadratic extension, a Weil restriction is isomorphic to a product, and a product is supersingular, and in particular superspecial, if and only if both factors are supersingular.

Structure. The n -torsion of an abelian variety over a finite field are those points $P \in A(\mathbb{F}_q)$ such that $[n]P = \mathbf{0}$. Let $A[n]$ denote the subgroup of n -torsion points over the algebraic closure $\overline{\mathbb{F}}_p$. If $\dim A = g$ and n is coprime to p , then

$$A[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}.$$

The $\mathbb{F}_q$ -rational n -torsion $A[n](\mathbb{F}_q)$ is significantly more restricted, due to isotropy conditions enforced by the Weil pairing, which is where the principal polarization is used as it identifies A with $\hat{A}$ and thereby turns the Weil pairing into a non-degenerate alternating pairing on $A[n]$. We follow [13, Prop. 5.78]: for a principally polarized abelian variety $A/\mathbb{F}_q$ of dimension g and an integer n coprime to p , let $d = \gcd(n, q-1)$. Then we have

$$A[n](\mathbb{F}_q) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^g \times (\mathbb{Z}/d\mathbb{Z})^g. \quad (1)$$

In contrast, the p -torsion $A[p]$ of an abelian variety is a more nuanced object, and in general has rank at most g instead of $2g$, referred to as the p -rank of A .

We refer to the smallest field extension $\mathbb{F}_{q^k}$ such that $A[n] \subseteq A(\mathbb{F}_{q^k})$ as the *full n -torsion degree* of A . This is closely related to the *embedding degree* k' of n , defined by the smallest k' such that $n \mid q^{k'} - 1$, i.e., $\mu_n \subseteq \mathbb{F}_{q^{k'}}^\times$. By the non-degeneracy of the Weil pairing $e_n : A[n] \times A[n] \rightarrow \mu_n$, we have $k' \leq k$.

From the above, we can derive the general group structure of $A(\mathbb{F}_q)$ as

$$A(\mathbb{F}_q) \cong \mathbb{Z}/n_0\mathbb{Z} \times \dots \times \mathbb{Z}/n_{r-1}\mathbb{Z}$$

where $r \leq 2g$ is the *rank* of A and $n_{i+1} \mid n_i$ for all i . We refer to n_0 as the *exponent* of $A(\mathbb{F}_q)$, as we have $[n_0]P = \mathbf{0}$ for all $P \in A(\mathbb{F}_q)$, whereas the order is $|A(\mathbb{F}_q)| = \prod n_i$.

Supersingularity. In higher dimensions, supersingularity can be generalized in several ways. A distinguishing property for elliptic curves is the p -rank, which is 1 for ordinary curves, and 0 for supersingular curves. Similarly, in dimension 2, ordinary abelian surfaces have p -rank 2 and supersingular abelian surfaces have p -rank 0. Equivalently, supersingular abelian surfaces are isogenous, as unpolarized varieties, to a product of supersingular elliptic curves. Abelian surfaces are *superspecial* whenever they are *isomorphic* to a product of supersingular elliptic curves as unpolarized varieties. Hence, superspecial varieties are always supersingular, but not the other way around. For Jacobians of hyperelliptic curves, we say that the associated curve is supersingular, or superspecial, if the Jacobian is supersingular or superspecial, respectively.

2.3 Characteristic Polynomial of Frobenius

Let $A/\mathbb{F}_q$ be an abelian variety of dimension g , then we denote by φ_A the characteristic polynomial of the q -Frobenius endomorphism $\pi : A \rightarrow A$, also called the *Weil polynomial*. This polynomial captures essential information for abelian varieties:

1. We have $\varphi_A(x) = \prod_{i=1}^{2g} (x - \alpha_i)$, where the α_i are the q -Weil numbers with $|\alpha_i| = \sqrt{q}$,
2. We have $\varphi_A(1) = |A(\mathbb{F}_q)|$,
3. Two varieties A and B are isogenous if and only if $\varphi_A = \varphi_B$,
4. If $\varphi_q(x) = \prod_{i=1}^{2g} (x - \alpha_i)$ is the Weil polynomial of a variety with respect to the q -Frobenius, then $\varphi_{q^k}(x) = \prod_{i=1}^{2g} (x - \alpha_i^k)$ is the Weil polynomial with respect to the q^k -Frobenius.

For abelian surfaces over $\mathbb{F}_p$, the characteristic polynomial is of the form

$$\varphi_A(x) = x^4 + ax^3 - bx^2 + apx + p^2, \quad a, b \in \mathbb{Z}. \quad (2)$$

Since $-a$ is the trace of π , by an abuse of language we will refer to a as the *trace* of A over $\mathbb{F}_p$. Most pertinent to this work is the fact that abelian surfaces are supersingular if and only if they have trace $a = 0$ and $p \mid b$. For a given abelian surface A , there are only two variables, so in general we can explicitly derive $\varphi_A(x)$ if we know the evaluation of φ_A at two values.

Bounds. Not any characteristic polynomial $\varphi_A(x)$ is possible over $\mathbb{F}_q$. In general, we get the following bounds [26], which we refer to as *Weil bounds*

$$|a| \leq 4\sqrt{q}, \quad (3)$$

$$b \leq 2q - 2\sqrt{q}|a|, \quad (4)$$

$$b \geq -2q - \frac{1}{4}a^2. \quad (5)$$

The Hasse-Weil Interval. One may see from the shape of φ_A that an abelian variety A of dimension g over $\mathbb{F}_q$ must have at least $(\sqrt{q} - 1)^{2g}$ points, and at most $(\sqrt{q} + 1)^{2g}$ points. This is the Hasse-Weil interval:

$$(\sqrt{q} - 1)^{2g} \leq |A(\mathbb{F}_q)| \leq (\sqrt{q} + 1)^{2g}. \quad (6)$$

In general, we find that the number of points is always $O(q^g)$ and the width of this interval is $O(4gq^{g-1/2})$. For abelian surfaces over $\mathbb{F}_p$, this gives roughly p^2 points, and a width of $8\sqrt{p}(p+1)$ for the interval. In this work, we will often use the following result, which we refer to as the *width-bound argument*.

Lemma 2.1. *Let A be an abelian variety over $\mathbb{F}_q$ of dimension g and $H \subseteq A(\mathbb{F}_q)$ with $|H|$ larger than the width of the Hasse-Weil interval. Then $|A(\mathbb{F}_q)| = n$, where n is the unique multiple of $|H|$ in the Hasse-Weil interval.*

Proof. The generalized width of the Hasse–Weil interval is

$$(\sqrt{q} + 1)^{2g} - (\sqrt{q} - 1)^{2g} \leq 4^g \cdot q^{g-1/2}$$

and the lower bound of the Hasse–Weil interval is $(\sqrt{q} - 1)^{2g}$. Thus, for any subgroup $H \subseteq A(\mathbb{F}_q)$ such that $|H|$ is larger than the width of the Hasse–Weil interval, there is only one unique multiple n of $|H|$ in the Hasse–Weil interval. But this must then be the size of $A(\mathbb{F}_q)$, as $|A(\mathbb{F}_q)|$ is in the Hasse–Weil interval, and a multiple of $|H|$. $\square$

Extremal Abelian Varieties. An abelian variety that reaches the lower bound is called *minimal*, one that reaches the upper bound is called *maximal*. We say that an abelian variety is *extremal* if it is either minimal or maximal. Such extremal varieties are special, as the following result shows.

Lemma 2.2. *If A is an extremal abelian variety over $\mathbb{F}_{p^2}$, then A is superspecial.*

Proof. By [22, Theorem 5.3], a maximal abelian variety A over $\mathbb{F}_{p^2}$ is isomorphic to a product of maximal, hence supersingular, elliptic curves over $\mathbb{F}_{p^2}$. Thus, A is superspecial. The analogous argument holds for minimal abelian varieties. $\square$

Twists. An abelian variety that is isomorphic to an abelian surface A over an extension field but not the base field is called a *twist* of A . Twists are closely related to automorphisms of the variety [40, Ch. X, Thm 2.2]. For Jacobians, any twist is induced by a twist of the associated hyperelliptic curve. Generally, when clear from context, we may refer to *the* twist A^t when we refer to the quadratic twist induced by $[-1] \in \text{Aut}(A)$.

3 Supersingular Abelian Surfaces

The possible orders and group structures of abelian surfaces over $\mathbb{F}_p$, and the existence of an abelian surface with a given group structure, are established in several places throughout the literature. In this section, we list and derive the essential results on which we base our later supersingularity tests.

Specializing to dimension $g = 2$, our approach is broadly as follows: we verify supersingularity of an abelian surface by determining the characteristic polynomial $\varphi_A(x)$. Although the order and/or group structure of $A(\mathbb{F}_p)$ does not by itself fix the characteristic polynomial, when combined with the order and/or group structure of either $A(\mathbb{F}_{p^2})$ or $A^t(\mathbb{F}_p)$, the characteristic polynomial $\varphi_A(x)$ is fixed. We therefore derive the necessary results on the possible shapes of $\varphi_A(x)$, the associated orders, and the group structures of A and its twist.³

³ The notation A^t in this section refers to the quadratic twist over the respective field, hence may denote different abelian surfaces depending on the base field. Furthermore, ρ refers to the associated twisting isomorphism.

3.1 Group Structures of Abelian Surfaces

We explore the possible group structures of abelian surfaces over $\mathbb{F}_q$ of characteristic p .⁴ Surprisingly, they are quite limited, with strong restrictions imposed by both the Weil polynomial and the Weil bounds.

The Weil Polynomial. Rybakov [37] showed that the Weil polynomial imposes precise limitations on the possible group structures of principally polarized abelian varieties over $\mathbb{F}_q$. We reformulate this result for abelian surfaces.

Lemma 3.1 (Cor. 3.1, [37]). *Let A be an abelian surface over $\mathbb{F}_q$ with characteristic polynomial of Frobenius $\varphi_A(x) = x^4 + ax^3 - bx^2 + qax + q^2$ with group structure*

$$A(\mathbb{F}_q) \cong \mathbb{Z}_{n_0} \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \mathbb{Z}_{n_3},$$

where $n_{i+1} \mid n_i$. Write $\varphi_A(1-x)$ as $\lambda_0 + \lambda_1x + \lambda_2x^2 + \lambda_3x^3 + x^4$. Then,

$$n_3 \mid \lambda_3, \quad n_2n_3 \mid \lambda_2, \quad n_1n_2n_3 \mid \lambda_1, \quad n_0n_1n_2n_3 \mid \lambda_0.$$

Rewriting $\varphi_A(1-x)$ allows us to express the coefficients λ_i in terms of a and b .

Corollary 3.2. *Over $\mathbb{F}_q$, given $\varphi_A(x) = x^4 + ax^3 - bx^2 + qax + q^2$, then*

$$\begin{aligned} \lambda_0 &= q^2 + 1 + a(q+1) - b, \\ \lambda_1 &= -a(q+1) - 2(a-b+2), \\ \lambda_2 &= 3a - b + 6, \\ \lambda_3 &= -(a+4). \end{aligned}$$

3.2 Group Structures of Supersingular Abelian Surfaces

We refine our characterization of group structures to the case of supersingular abelian surfaces over $\mathbb{F}_p$. Whereas supersingular elliptic curves over $\mathbb{F}_p$ have only one possible characteristic polynomial and order, and two possible group structures, supersingular abelian surfaces now have five different characteristic polynomials and nine different group structures. Note that in this section we write b for minus the coefficient of x^2 divided by p in the characteristic polynomial of Frobenius of a supersingular abelian surface.

Lemma 3.3. *Let A be an abelian surface over $\mathbb{F}_p$. Then A is supersingular if and only if its characteristic polynomial of Frobenius is of the form*

$$\varphi_A(x) = x^4 - bpx^2 + p^2, \quad b \in \{-2, -1, 0, 1, 2\}.$$

Consequently, the possible orders of supersingular abelian surfaces over $\mathbb{F}_p$ are

$$|A(\mathbb{F}_p)| = \begin{cases} (p+1)^2 & \text{if } b = -2 \\ p^2 + p + 1 & \text{if } b = -1 \\ p^2 + 1 & \text{if } b = 0 \\ p^2 - p + 1 & \text{if } b = 1 \\ (p-1)^2 & \text{if } b = 2 \end{cases}$$

⁴ From here onwards, we assume $p > 5$; there are esoteric abelian surfaces for $p \leq 5$.

Proof. The result on $\varphi_A(x)$ follows from [21]. The possible orders are then derived from $|A(\mathbb{F}_p)| = \varphi_A(1)$. $\square$

These five types of abelian surfaces will be crucial to many of the results in this work, and we therefore introduce the following notation.

Definition 3.4. *Let A be a supersingular abelian surface over $\mathbb{F}_p$. When $\varphi_A(x) = x^4 - bpx^2 + p^2$, we say that A is of type b . Furthermore, when $n = |A(\mathbb{F}_p)|$, i.e., $n = p^2 - bp + 1$ for $b \in \{-2, -1, 0, 1, 2\}$, then n is a supersingular order.*

Ignoring the 2-torsion, the group structures of these abelian surfaces are simple: those with parameter $b = \pm 2$ are rank 2, whereas for $b \in \{-1, 0, 1\}$ the groups are cyclic. Including the 2-torsion, we get the following more precise result.

Theorem 3.5 ([44]). *Let $A/\mathbb{F}_p$ be a supersingular abelian surface with $p > 5$.*

1. *If $b \in \{-1, 0, 1\}$, then the group structure is cyclic and:*
 - (a) *if $b = -1$, then $A(\mathbb{F}_p) \cong \mathbb{Z}/(p^2 + p + 1)\mathbb{Z}$,*
 - (b) *if $b = 0$, then $A(\mathbb{F}_p) \cong \mathbb{Z}/(p^2 + 1)\mathbb{Z}$,*
 - (c) *if $b = 1$, then $A(\mathbb{F}_p) \cong \mathbb{Z}/(p^2 - p + 1)\mathbb{Z}$,*
2. *if $b = \pm 2$, then the group structure is of rank at least 2 and:*
 - (a) *if $b = -2$ and $p \equiv 1 \pmod{4}$, then $A(\mathbb{F}_p) \cong (\mathbb{Z}/(p+1)\mathbb{Z})^2$,*
 - (b) *if $b = -2$ and $p \equiv 3 \pmod{4}$, then $A(\mathbb{F}_p)$ is isomorphic to*

$$(\mathbb{Z}/(p+1)\mathbb{Z})^2 \quad \text{or} \quad \mathbb{Z}/(p+1)\mathbb{Z} \times \mathbb{Z}/(\frac{p+1}{2})\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad \text{or} \quad (\mathbb{Z}/(\frac{p+1}{2})\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})^2,$$

- (c) *if $b = 2$ and $p \equiv 1 \pmod{4}$, then $A(\mathbb{F}_p)$ is isomorphic to*

$$(\mathbb{Z}/(p-1)\mathbb{Z})^2 \quad \text{or} \quad \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/(\frac{p-1}{2})\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad \text{or} \quad (\mathbb{Z}/(\frac{p-1}{2})\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})^2,$$

- (d) *if $b = 2$ and $p \equiv 3 \pmod{4}$, then $A(\mathbb{F}_p) \cong (\mathbb{Z}/(p-1)\mathbb{Z})^2$.*

Remark 3.6. By [21], for every prime $p > 5$ there exists a supersingular Jacobian $\mathcal{J}$ with such a group structure, except for the case $b = 1$ for primes $p \equiv 1 \pmod{6}$. Note that the reverse of Theorem 3.5 is *not* true: such group structures exist for non-supersingular Jacobians $\mathcal{J}/\mathbb{F}_p$ too.⁵

Using Theorem 3.5, we can derive the group structure up to the rank of the 2-torsion given only the order of a supersingular Jacobian. We derive the rank of the 2-torsion $\mathcal{J}[2](\mathbb{F}_p)$ using the factorization of the polynomial defining the associated hyperelliptic curve.⁶ We say that a non-zero polynomial $f \in \mathbb{F}_p[x]$ has factorization type $\{d_1, \dots, d_N\}$ over $\mathbb{F}_p$ if it factors as $f = c \prod_{i=1}^N f_i$ where the factors f_i are distinct, monic, irreducible over $\mathbb{F}_p$, and of degree d_i , and $c \in \mathbb{F}_p$ is the leading coefficient.

⁵ For example, for $p = 7$, the Jacobian $\mathcal{J}$ of the hyperelliptic curve defined by $y^2 = 4x^6 + 3x^5 + x^4 + 5x^3 + 6x^2 + 5$ satisfies $\mathcal{J}(\mathbb{F}_p) \cong \mathbb{Z}/(p^2 + 1)\mathbb{Z}$.

⁶ This rank is important in later sections, as it decides isotropy behaviour of eigenspaces, see e.g., Section 5.1 and Remark 5.4.

Lemma 3.7 ([14]). *Let $\mathcal{J}$ be the Jacobian over $\mathbb{F}_p$ of a genus-2 hyperelliptic curve C defined by $y^2 = f(x)$, with $\deg f \in \{5, 6\}$. Given the factorization $f(x) = c \prod_{i=1}^N f_i(x)$, with f_i distinct monic irreducible polynomials over $\mathbb{F}_p$ and leading coefficient c , let d_i denote the degree of f_i , so that $\{d_1, d_2, \dots, d_N\}$ is the factorization type of f over $\mathbb{F}_p$. Then $\mathcal{J}[2](\mathbb{F}_p)$ is isomorphic to*

- $\langle 1 \rangle$, if f is irreducible, or $\deg(f) = 6$ and f factors as $\{5, 1\}, \{3, 3\}$;
- $(\mathbb{Z}/2\mathbb{Z})$, if $\deg(f) = 6$ and f factors as $\{4, 1, 1\}, \{3, 2, 1\}, \{4, 2\}$, or $\deg(f) = 5$ and f factors as $\{4, 1\}, \{3, 2\}$;
- $(\mathbb{Z}/2\mathbb{Z})^2$, if $\deg(f) = 6$ and f factors as $\{3, 1, 1, 1\}, \{2, 2, 1, 1\}, \{2, 2, 2\}$, or $\deg(f) = 5$ and f factors as $\{3, 1, 1\}, \{2, 2, 1\}$;
- $(\mathbb{Z}/2\mathbb{Z})^3$, if $\deg(f) = 6$ and f factors as $\{2, 1, 1, 1, 1\}$, or $\deg(f) = 5$ and f factors as $\{2, 1, 1, 1\}$;
- $(\mathbb{Z}/2\mathbb{Z})^4$, if f splits into linear factors.

Recall that we generally need two evaluations of $\varphi_A(x)$ to reconstruct $\varphi_A(x)$, which we use to verify the supersingularity of abelian surface. While a first evaluation is given by the order $|A(\mathbb{F}_p)| = \varphi_A(1)$, we can get a second evaluation of $\varphi_A(x)$ by deriving the order of the twist, where we use that supersingular abelian varieties have trace $a = 0$.

Lemma 3.8. *An abelian surface $A/\mathbb{F}_p$ has trace $a = 0$ iff $|A(\mathbb{F}_p)| = |A^t(\mathbb{F}_p)|$.*

Proof. We get $\varphi_{A^t}(x) = \varphi_A(-x)$ by [41, Lem. 3]. For

$$\varphi_A(x) = x^4 + ax^3 - bx^2 + apx + p^2$$

the equality of $\varphi_A(1) = |A(\mathbb{F}_p)|$ and $\varphi_{A^t}(1) = |A^t(\mathbb{F}_p)|$ implies $a + ap = -a - ap$, thus $a = 0$. Conversely, if $a = 0$, we get $\varphi_A(x) = \varphi_A(-x) = \varphi_{A^t}(x)$. $\square$

Remark 3.9. As $A[2](\mathbb{F}_p) = A^t[2](\mathbb{F}_p)$, we may combine the above result with Theorem 3.5 to derive the stronger result that for supersingular A , as $a = 0$, we get $A(\mathbb{F}_p) \cong A^t(\mathbb{F}_p)$.

3.3 Uniqueness of Supersingular Orders

From Lemma 3.3, we know that if $A/\mathbb{F}_p$ is supersingular, then its order n is of the form $n = p^2 - bp + 1$ for $b \in \{-2, -1, 0, 1, 2\}$. The converse is (almost) true, except we have to look over $\mathbb{F}_{p^2}$: if $A/\mathbb{F}_p$ is an abelian surface with $|A(\mathbb{F}_{p^2})| = n^2$ for a supersingular order n , then A is supersingular. The goal of this section will be proving this result, which is a key ingredient in our supersingularity testing.

At a high level, our argument is as follows. We first observe that even though for a supersingular order n the equality $|A(\mathbb{F}_p)| = n$ can be satisfied by both supersingular and non-supersingular abelian surfaces, for the cases $b \in \{\pm 1, \pm 2\}$ the equality $|A(\mathbb{F}_{p^2})| = n^2$ is only satisfied by supersingular abelian surfaces. The case $b = 0$ is more nuanced: there exist non-supersingular abelian surfaces A with $|A(\mathbb{F}_{p^2})| = (p^2 + 1)^2$, but such abelian surfaces are never defined over

$\mathbb{F}_p$. More precisely, we show that any abelian surface $A/\mathbb{F}_p$ with $|A(\mathbb{F}_{p^2})| = n^2$ is supersingular.

In this section, we often require the Weil polynomial of an abelian surface A over both $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$. When the abelian surface A is clear from context, we write the Weil polynomial over $\mathbb{F}_p$ as

$$\varphi_p(x) = x^4 + a_p x^3 - b_p x^2 + a_p p x + p^2$$

and the Weil polynomial over $\mathbb{F}_{p^2}$, using $q = p^2$, as

$$\varphi_q(x) = x^4 + a_q x^3 - b_q x^2 + a_q p^2 x + p^4.$$

Note that a_p, b_p and a_q, b_q denote the (unnormalised) coefficients of φ_p and φ_q as displayed, so that A is of type $b = b_p/p$ in the sense of [Definition 3.4](#). In the proofs of [Lemma 3.10](#) and [Lemma 3.11](#), it is convenient to work with the x^2 -coefficients $c_p := -b_p$ and $c_q := -b_q$.

The case $\mathbf{b} = \pm 2$. [Lemma 2.2](#) resolves the case $b = \pm 2$: any abelian surface A with $|A(\mathbb{F}_{p^2})| = (p \pm 1)^4$ is either minimal or maximal, and is thus supersingular (and even superspecial).

The case $\mathbf{b} = \pm 1$. We derive the result from the central requirement that $\varphi_A(1) = n^2$ over $\mathbb{F}_{p^2}$, with $n = p^2 \pm p + 1$, together with the Weil bounds.

Lemma 3.10. *Let $n = p^2 \pm p + 1$ and let A be an abelian surface such that $|A(\mathbb{F}_{p^2})| = n^2$. Then the Weil polynomial of A over $\mathbb{F}_{p^2}$ is*

$$(x^2 \pm px + p^2)^2 = x^4 \pm 2px^3 + 3p^2x^2 \pm 2p^3x + p^4,$$

and in particular A is supersingular. Moreover, if A is defined over $\mathbb{F}_p$, then A is of type $b = \mp 1$.

Proof. We derive the result for $n = p^2 + p + 1$, which requires us to show that $a_q = 2p$ and $c_q = 3p^2$. The analogous result can be derived for $n = p^2 - p + 1$ simply by a change of sign in the right places. With $q = p^2$, the Weil bounds in [Eqs. \(3\) to \(5\)](#) become

$$|a_q| \leq 4p, \quad c_q \leq 2p^2 + \frac{1}{4}a_q^2, \quad \text{and} \quad c_q \geq -2p^2 + 2p \cdot |a_q|.$$

As $|A(\mathbb{F}_{p^2})| = n^2 = \varphi_A(1)$, we get

$$a_q(p^2 + 1) + c_q = 2p^3 + 3p^2 + 2p. \tag{7}$$

We now derive the two bounds $a_q \geq 2p$ and $a_q \leq 2p$ to conclude that $a_q = 2p$, which directly implies $c_q = 3p^2$. First, by $c_q \leq 2p^2 + \frac{1}{4}a_q^2$, and substituting c_q into [Eq. \(7\)](#), we get

$$\frac{1}{4}a_q^2 + a_q(p^2 + 1) - (2p^3 + p^2 + 2p) \geq 0,$$

where equality with 0 is reached at $a_q = 2p$ and $a_q = -4p^2 - 2p - 4$. The bound $|a_q| \leq 4p$ excludes the second branch, so we get $2p \leq a_q \leq 4p$. Then, by $c_q \geq -2p^2 + 2p|a_q|$ and substituting c_q , noticing $|a_q| = a_q$ as $a_q \geq 2p$, we get

$$2pa_q - 2p^2 \leq 2p^3 + 3p^2 + 2p - a_q(p^2 + 1),$$

which can be rewritten to

$$a_q \leq 2p + \frac{p^2}{(p+1)^2}.$$

This last fraction is always smaller than 1, so as a_q is an integer we have that $a_q \leq 2p$. We conclude that $a_q = 2p$ and $c_q = 3p^2$, i.e., $b_q = -3p^2$, as required.

Now suppose that A is the base change of an abelian surface over $\mathbb{F}_p$, with Weil polynomial φ_p . We have that

$$a_q = 2c_p - a_p^2, \quad c_q = c_p^2 - 2a_p^2p + 2p^2. \quad (8)$$

Substituting into $a_q = 2p$ and $c_q = 3p^2$, we get $a_p^2(a_p^2 - 4p) = 0$. As $p > 5$, $4p$ is not a square, so $a_p = 0$ and $c_p = p$ and A is of type $b = -1$. $\square$

The case $\mathbf{b} = \mathbf{0}$. This case is most interesting, as for $n = p^2 + 1$ there exist non-supersingular abelian surfaces such that $|A(\mathbb{F}_{p^2})| = n^2$, in contrast with the other cases. However, we show that such abelian surfaces are never defined over $\mathbb{F}_p$, except for the supersingular ones.

Lemma 3.11. *Let $n = p^2 + 1$ and let A be an abelian surface over $\mathbb{F}_p$ with $|A(\mathbb{F}_{p^2})| = n^2$. Then A is supersingular, and in particular, the Weil polynomial of A over $\mathbb{F}_p$ is $x^4 + p^2$.*

Proof. We denote the Weil polynomial for A over $\mathbb{F}_p$ by $\varphi_p(x)$ and over $\mathbb{F}_{p^2}$ by $\varphi_q(x)$. The goal is to use [Lemma 3.3](#) and show that $a_p = 0$ and $p \mid c_p$.

As $|A(\mathbb{F}_{p^2})| = n^2$ we get from $\varphi_q(1) = n^2$ that

$$a_q(p^2 + 1) + c_q = 2p^2. \quad (9)$$

By $\varphi_p(x) = \prod (x - \alpha_i)$ and $\varphi_q(x) = \prod (x - \alpha_i^2)$, we have that $\varphi_p(x)\varphi_p(-x) = \varphi_q(x^2)$. Expanding this out and comparing coefficients, we find that $a_q = 2c_p - a_p^2$ and $c_q = c_p^2 - 2a_p^2p + 2p^2$. This allows us to rewrite [Eq. \(9\)](#) as

$$a_p^2 = \frac{c_p^2 + 2c_p(p^2 + 1)}{(p+1)^2}, \quad (10)$$

and so from $a_q = 2c_p - a_p^2$, by expressing everything in terms of c_p , we get

$$a_q = \frac{c_p(4p - c_p)}{(p+1)^2}. \quad (11)$$

First we bound c_p . From the Weil bound in [Eq. \(4\)](#) we have $c_p \leq 2p + \frac{1}{4}a_p^2$. Together with [Eq. \(10\)](#), we obtain

$$c_p^2 - 2c_p(p^2 + 4p + 1) + 8p(p + 1)^2 \geq 0.$$

Solving the quadratic in c_p , we get that $c_p \leq 4p$ or $c_p \geq 2(p^2 + 2p + 1)$. The latter is not possible due to the Weil bounds, so we find that $c_p \leq 4p$.

Furthermore, the right-hand side of [Eq. \(10\)](#) should be positive, which implies that $c_p^2 + 2c_p(p^2 + 1) \geq 0$. Writing as $c_p(c_p + 2p^2 + 2) \geq 0$, and noting that $c_p + 2p^2 + 2 \geq 0$ by [Eq. \(5\)](#), we have that $c_p \geq 0$. Thus, we know $0 \leq c_p \leq 4p$. Using these values for c_p in [Eq. \(11\)](#), and noting that a_q is an integer, we have $a_q \in \{0, 1, 2, 3\}$. We now show that only $a_q = 0$ is possible.

- $a_q = 1$: From $(p + 1)^2 = c_p(4p - c_p)$, we get $2 \mid c_p$. But then $1 = a_q = 2c_p - a_p^2$ cannot have a solution, as this requires a_p odd and $a_p^2 \equiv 3 \pmod{4}$, which is impossible.
- $a_q = 2$: From $2(p + 1)^2 = c_p(4p - c_p)$, we get $4 \mid c_p$. But then $2 = a_q = 2c_p - a_p^2$ cannot have a solution mod 8.
- $a_q = 3$: To get an integer solution to the quadratic in c_p from [Eq. \(11\)](#), the discriminant needs to be a square. This discriminant is equal to $(p - 3)^2 - 12$ and hence only a square for $p = 7$. Thus, for $p > 7$, this case is never possible. For $p = 7$, the solutions $c_p = 12, 16$ force a non-integer solution for a_p in $3 = a_q = 2c_p - a_p^2$.

We conclude that $a_q = 0$ and hence $c_q = 2p^2$ by [Eq. \(9\)](#). This is enough to show supersingularity of A , but we can even deduce from [Eq. \(11\)](#) that $c_p = 0$, so that $a_p = 0$ (from $a_q = 2c_p - a_p^2$), as the case $c_p = 4p$ forces $a_p^2 = 8p$, which can only happen for $p = 2$. $\square$

We summarize the results of this section in the following theorem.

Theorem 3.12. *Let $n = p^2 - bp + 1$ with $b \in \{-2, -1, 0, 1, 2\}$.*

- *Assuming $b \neq 0$, if A is an abelian surface over $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$ such that $|A(\mathbb{F}_{p^2})| = n^2$, then A is supersingular.*
- *If $b = 0$ and A is an abelian surface over $\mathbb{F}_p$ such that $|A(\mathbb{F}_{p^2})| = n^2$, then A is supersingular.*

3.4 Structure theory of m -torsion

Our conclusive supersingularity testing in [Section 5](#) uses the m -Weil pairing to identify the structure of the rational m -torsion, where m is the exponent of $A(\mathbb{F}_p)$. The goal of this section is to show that knowing the structure of $A[m]$ is sufficient to determine the supersingularity of A . To this end, we develop theory on the m -torsion of supersingular Jacobians, and derive the necessary results on the Weil pairing to enable this testing.

To determine the full m -torsion degree of $A[m]$, we use the following lemma.

Lemma 3.13. *Let $\varphi(x) = x^4 - bpx^2 + p^2$ and let m be any divisor of $p^2 - bp + 1$. Then*

$$\varphi(x) \equiv (x^2 - 1) \cdot (x^2 - p^2) \pmod{m}.$$

Remark 3.14. The minimal polynomial of the Frobenius endomorphism π is squarefree (as π is central in $\text{End}^0(A)$, which is semisimple) and divides φ . In particular, for A of type $b = \pm 2$ we have $\pi^2 = [\pm p]$ on A . Hence, π^2 acts trivially on $A[p \mp 1]$, so $A[p \mp 1] \subseteq A(\mathbb{F}_{p^2})$.

As $\varphi(x)$ splits completely modulo m , if the roots are distinct modulo ℓ for all primes $\ell \mid m$, then the action of Frobenius on $A[m]$ is diagonalizable, and its order will be the lowest common multiple of the orders of the four eigenvalues $\pm 1, \pm p \in (\mathbb{Z}/m\mathbb{Z})^\times$. Hence, we can derive the full m -torsion degree from the embedding degree of m , and decompose $A[m]$ accordingly. Generically, we get $X^2 + X + 1 \mid X^3 - 1$, $X^2 + 1 \mid X^4 - 1$ and $X^2 - X + 1 \mid X^6 - 1$, which gives embedding degrees 3, 4, and 6 for m -th root of unities where m is the exponent for b -type $-1, 0$, and 1 respectively. With a slight abuse of notation, for $\lambda \in \{\pm 1, \pm p\}$ we write $A[\pi - \lambda] = \ker(\pi - \lambda) \cap A[m]$ for the corresponding eigenspace. These are defined over the following fields.

Lemma 3.15. *Let A over $\mathbb{F}_p$ be a supersingular abelian surface of type b and exponent m . If $\lambda^k \equiv 1 \pmod{m}$, then $A[\pi - \lambda] \subseteq A(\mathbb{F}_{p^k})$, and if $\lambda^k \equiv -1 \pmod{m}$, then $A[\pi - \lambda] \subseteq A^t(\mathbb{F}_{p^k})^\rho$. Furthermore:*

1. *The eigenspaces of $\lambda = \pm 1$ are $A[\pi - 1] = A(\mathbb{F}_p)$ and $A[\pi + 1] = A^t(\mathbb{F}_p)^\rho$.*
2. *The eigenspaces of $\pm p$ are, per type b :*
 - (a) $b = 2$: $A[\pi - p] = A[\pi - 1] = A(\mathbb{F}_p)$ and $A[\pi + p] = A[\pi + 1] = A^t(\mathbb{F}_p)^\rho$.
 - (b) $b = -2$: $A[\pi - p] = A[\pi + 1] = A^t(\mathbb{F}_p)^\rho$ and $A[\pi + p] = A[\pi - 1] = A(\mathbb{F}_p)$.
 - (c) $b = 0$: $A[\pi - p] = A^t(\mathbb{F}_{p^2})^\rho$ and $A[\pi + p] = A^t(\mathbb{F}_{p^2})^{\rho'}$.
 - (d) $b = -1$: $A[\pi - p] = A(\mathbb{F}_{p^3})$ and $A[\pi + p] = A^t(\mathbb{F}_{p^3})^{\rho'}$.
 - (e) $b = 1$: $A[\pi - p] = A^t(\mathbb{F}_{p^3})^\rho$ and $A[\pi + p] = A(\mathbb{F}_{p^3})$.

Proof. For $P \in A[\pi - \lambda]$ we have $\pi^k P = [\lambda^k]P$. If $\lambda^k \equiv 1 \pmod{m}$ this equals P , so P is fixed by the p^k -power Frobenius and hence $P \in A(\mathbb{F}_{p^k})$. If $\lambda^k \equiv -1 \pmod{m}$, we have $\pi^k P = -P$, so $P \in A^t(\mathbb{F}_{p^k})$.

The congruences follow from $m \mid p^2 - bp + 1$. For $b = \pm 2$ we have $m \in \{p \mp 1, \frac{p \mp 1}{2}\}$ by Theorem 3.5, so $p \equiv \pm 1 \pmod{m}$. For $b = 0$ we have $m = p^2 + 1$, so $p^2 \equiv -1 \pmod{m}$. Finally, for $b = \pm 1$ we have $m = p^2 \mp p + 1$ dividing $p^3 \pm 1$, hence $p^3 \equiv \mp 1 \pmod{m}$. The statements for $A[\pi + p]$ follow from $(-p)^k = (-1)^k p^k$. $\square$

The subgroup generated by these four eigenspaces is almost all of $A[m]$; the index is a power of 2 or of 3, and is determined by the type b and the group structure of $A(\mathbb{F}_p)$.

Lemma 3.16. *Let A be a supersingular abelian surface defined over $\mathbb{F}_p$, of type b and exponent m . Let*

$$H = A[\pi - 1] + A[\pi + 1] + A[\pi - p] + A[\pi + p] \subseteq A[m]$$

be the subgroup generated by the four eigenspaces of Lemma 3.15. Then the index of H in $A[m] \cong (\mathbb{Z}/m\mathbb{Z})^4$ is as follows:

– *If $b = \pm 2$, then $H = A(\mathbb{F}_p) + A^t(\mathbb{F}_p)^\rho$ and*

$$[A[m] : H] = \frac{m^4 \cdot |A[2](\mathbb{F}_p)|}{|A(\mathbb{F}_p)|^2} = \begin{cases} 4 & \text{if } A(\mathbb{F}_p) \cong (\mathbb{Z}/m\mathbb{Z})^2, \\ 8 & \text{if } A(\mathbb{F}_p) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/\frac{m}{2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \\ 1 & \text{if } A(\mathbb{F}_p) \cong (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})^2, \end{cases}$$

where the first two cases have $m = p \mp 1$ and the third has $m = \frac{p \mp 1}{2}$.

- *If $b = 0$, then $[A[m] : H] = 8$.*
- *If $b = -1$, then $[A[m] : H] = 9$ if $p \equiv 1 \pmod{3}$, and $[A[m] : H] = 1$ otherwise.*
- *If $b = 1$, then $[A[m] : H] = 9$ if $p \equiv 2 \pmod{3}$, and $[A[m] : H] = 1$ otherwise.*

Proof. Since $A[m] = \bigoplus_{\ell^e | m} A[\ell^e]$ and every eigenspace decomposes accordingly, the index of H is the product of the local indices $[A[\ell^e] : H \cap A[\ell^e]]$ over the prime powers $\ell^e | m$. For a given prime factor ℓ , suppose that $1, -1, p, -p$ are pairwise distinct modulo ℓ . By Lemma 3.13 we have $\varphi(x) \equiv \prod_\lambda (x - \lambda) \pmod{\ell^e}$, and these factors are pairwise coprime in $(\mathbb{Z}/\ell^e\mathbb{Z})[x]$ because the differences $\lambda - \lambda'$ are units. Thus, $A[\ell^e] = \bigoplus_\lambda \ker(\pi - \lambda)$, where each summand is free of rank 1 over $\mathbb{Z}/\ell^e\mathbb{Z}$. This implies that the local index at ℓ is 1. The only cases where this fails, i.e., $1, -1, p, -p$ are *not* pairwise distinct modulo ℓ , are: $b = 0$ and $\ell = 2$; $b = \pm 1$ and $\ell = 3$; or $b = \pm 2$, where the eigenvalues ± 1 and $\pm p$ agree (in some order) modulo every $\ell | m$.

Consider first the case $b = \pm 2$. By Lemma 3.15 we have $p \equiv \pm 1 \pmod{m}$, so $A[\pi - p]$ and $A[\pi + p]$ coincide, in some order, with $A[\pi - 1] = A(\mathbb{F}_p)$ and $A[\pi + 1] = A^t(\mathbb{F}_p)^\rho$; thus $H = A(\mathbb{F}_p) + A^t(\mathbb{F}_p)^\rho$. As $A(\mathbb{F}_p) \cap A^t(\mathbb{F}_p)^\rho = A[2](\mathbb{F}_p)$, we have

$$|H| = \frac{|A(\mathbb{F}_p)| \cdot |A^t(\mathbb{F}_p)|}{|A[2](\mathbb{F}_p)|} = \frac{|A(\mathbb{F}_p)|^2}{|A[2](\mathbb{F}_p)|}.$$

Substituting the three group structures of Theorem 3.5 yields the three indices.

Consider the case $b = 0$, where $m = p^2 + 1$ and $A(\mathbb{F}_p)$ is cyclic by Theorem 3.5. As $p^2 \equiv 1 \pmod{8}$ we get $m \equiv 2 \pmod{8}$, so $2 | m$ and the 2-Sylow subgroup of $A(\mathbb{F}_p)$ is $\mathbb{Z}/2\mathbb{Z}$. All four eigenvalues are congruent modulo 2 to 1, so each eigenspace has its 2-part contained in $\ker(\pi - 1) \cap A[2] = A[2](\mathbb{F}_p) \cong \mathbb{Z}/2\mathbb{Z}$. So, $H \cap A[2] \cong \mathbb{Z}/2\mathbb{Z}$ with local index at 2 being $2^4/2 = 8$; other local indices are 1.

In the case $b = \pm 1$, we have that $m = p^2 \mp p + 1$ is odd, and $3 | m$ if and only if $p \equiv \mp 1 \pmod{3}$. If $3 \nmid m$, the index is 1. If $3 | m$, then $\varphi(x) \equiv (x - 1)^2(x + 1)^2 \pmod{3}$. Since $A(\mathbb{F}_p)$ is cyclic, we get $\ker(\pi - 1) \cap A[3] = A[3](\mathbb{F}_p) \cong \mathbb{Z}/3\mathbb{Z}$, and likewise $\ker(\pi + 1) \cap A[3] \cong A^t[3](\mathbb{F}_p) \cong \mathbb{Z}/3\mathbb{Z}$. Therefore, $H \cap A[3]$ has order 9 and local index at 3 is $3^4/3^2 = 9$. $\square$

Such a basis of eigenpoints as a subgroup of $A[m]$ is almost symplectic as the following result on their pairing values shows.

Lemma 3.17. *Let A over $\mathbb{F}_p$ be a supersingular abelian surface of exponent m , and let $P \in A[\pi - 1], Q \in A[\pi + 1], R \in A[\pi - p], S \in A[\pi + p]$ be eigenpoints in $A[m]$. Then $e_m(P, S)$ and $e_m(Q, R)$ are of order at most $\gcd(m, 2)$, and $e_m(P, Q)$ and $e_m(R, S)$ are of order at most $\gcd(m, p + 1)$.*

Proof. Generically, for two eigenpoints D and D' of eigenvalue λ, λ' respectively, we may set $\zeta = e_m(D, D')$, and derive constraints on ζ using

$$e_m(\pi(D), \pi(D')) = \zeta^p \text{ and } e_m(\pi(D), \pi(D')) = e_m(\lambda D, \lambda' D') = \zeta^{\lambda \cdot \lambda'}.$$

For example, this gives as constraints on $\zeta_{P,Q} = e_m(P, Q)$ that $\zeta_{P,Q}^p = \zeta_{P,Q}^{-1}$ and hence $\zeta_{P,Q}^{p+1} = 1$, which implies $\zeta_{P,Q} \in \mu_{p+1}$. Similarly, we get

$$\zeta_{P,R}^0 = 1, \quad \zeta_{P,S}^{2p} = 1, \quad \zeta_{Q,R}^{2p} = 1, \quad \zeta_{Q,S}^0 = 1, \quad \text{and} \quad \zeta_{R,S}^{p^2+p} = 1.$$

Since m and p are coprime, this implies $\zeta_{P,S} \in \mu_2$ and $\zeta_{Q,R} \in \mu_2$. For $\zeta_{R,S}$, we can remove a factor p to obtain $\zeta_{R,S}^{p+1} = 1$. Thus, $e_m(P, S), e_m(Q, R) \in \mu_{\gcd(m, 2)}$, and $e_m(P, Q), e_m(R, S) \in \mu_{\gcd(m, p+1)}$. $\square$

For $b = \pm 2$, Lemma 3.17 leaves an ambiguity at 2, as it only determines the pairings between the eigenspaces of ± 1 (for $b = 2$), or within them (for $b = -2$), up to μ_2 . We resolve it using the trace map $\pi + 1$, which interacts with the Weil pairing as follows. Note that we will work with $n = p \mp 1$ rather than with the exponent m of $A(\mathbb{F}_p)$, so that statements can be made uniformly over the three group structures (since $|A(\mathbb{F}_p)| = n^2$ in all cases).

Lemma 3.18. *Let $A/\mathbb{F}_p$ be a supersingular abelian surface of type $b = \pm 2$, and let $n = p \mp 1$. Then $A(\mathbb{F}_p) \subseteq A[n] \subseteq A(\mathbb{F}_{p^2})$, and*

$$(\pi + 1)A[n] = A(\mathbb{F}_p), \quad (\pi - 1)A[n] = A^t(\mathbb{F}_p)^\rho.$$

Moreover, for all $R \in A[n], Q \in A(\mathbb{F}_p)$ and $S \in A^t(\mathbb{F}_p)^\rho$,

$$e_n((\pi + 1)R, Q) = e_n(R, Q)^{p+1}, \quad e_n((\pi - 1)R, S) = e_n(R, S)^{-(p+1)}.$$

Proof. The exponent of $A(\mathbb{F}_p)$ divides n , so $A(\mathbb{F}_p) \subseteq A[n]$; the same holds for A^t , which is again of type $b = \pm 2$. By Remark 3.14, $A[n] \subseteq A(\mathbb{F}_{p^2})$ and $(\pi - 1)(\pi + 1) = \pi^2 - 1 = 0$ on $A[n]$. On $A[n]$, the kernel of $\pi - 1$ is $A(\mathbb{F}_p)$. The kernel of $\pi + 1$ is $A^t(\mathbb{F}_p)^\rho$ that is of order n^2 , so $(\pi + 1)A[n]$ has order $n^4/n^2 = n^2$. It is contained in $\ker(\pi - 1) = A(\mathbb{F}_p)$, thus $(\pi + 1)A[n] = A(\mathbb{F}_p)$. Similarly, $(\pi - 1)A[n] = A^t(\mathbb{F}_p)^\rho$.

Moreover, $e_n(\pi R, \pi T) = e_n(R, T)^p$ for all $R, T \in A[n]$. If $Q \in A(\mathbb{F}_p)$, then $e_n(\pi R, Q) = e_n(\pi R, \pi Q) = e_n(R, Q)^p$, and multiplying by $e_n(R, Q)$ gives the first identity. For $S \in A^t(\mathbb{F}_p)^\rho$, we have $\pi S = -S$ giving the second identity. $\square$

Table 3: Properties of supersingular abelian surfaces $A/\mathbb{F}_p$ by b -type, for $p > 5$. Here m denotes the exponent of $A(\mathbb{F}_p)$, the embedding degree is the smallest k with $m \mid p^k - 1$, and the full m -torsion field is the smallest extension of $\mathbb{F}_p$ over which $A[m]$ is defined.

b	Group structure $A(\mathbb{F}_p)$	$ A(\mathbb{F}_p) $	Emb. deg. of m	Full m -torsion
-2	$(\mathbb{Z}/(p+1)\mathbb{Z})^2$ or $\mathbb{Z}/(p+1)\mathbb{Z} \times \mathbb{Z}/\frac{p+1}{2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $(\mathbb{Z}/\frac{p+1}{2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})^2$	$(p+1)^2$	2	$\mathbb{F}_{p^2}$
-1	$\mathbb{Z}/(p^2 + p + 1)\mathbb{Z}$	$p^2 + p + 1$	3	$\mathbb{F}_{p^6}$
0	$\mathbb{Z}/(p^2 + 1)\mathbb{Z}$	$p^2 + 1$	4	$\mathbb{F}_{p^4}$
1	$\mathbb{Z}/(p^2 - p + 1)\mathbb{Z}$	$p^2 - p + 1$	6	$\mathbb{F}_{p^6}$
2	$(\mathbb{Z}/(p-1)\mathbb{Z})^2$ or $\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/\frac{p-1}{2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $(\mathbb{Z}/\frac{p-1}{2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})^2$	$(p-1)^2$	1	$\mathbb{F}_{p^2}$

An overview of these structural results is given in [Table 3](#).

Remark 3.19. For $b = 1$, a Jacobian with the corresponding group structure does not exist when $p \equiv 1 \pmod{6}$, as shown by Howe, Nart, and Ritzenthaler [21]. Furthermore, when $p \equiv 1 \pmod{4}$, all three rows for $b = -2$ are equivalent, as $\frac{p+1}{2}$ is odd, and when $p \equiv 3 \pmod{4}$, all three rows for $b = 2$ are equivalent, as $\frac{p-1}{2}$ is odd.

3.5 Superspecial Jacobians

Thus far, we have only considered the supersingular case; it is also important to understand the superspecial case, particularly for cryptographic applications. In this section, we focus in particular on Jacobians, as we will appeal to results about the associated genus-2 hyperelliptic curve, and products of supersingular elliptic curves are by definition superspecial. To show that a Jacobian is superspecial, we require two results from the literature that allow us to reduce to determining a simpler property: minimality or maximality. Essentially, superspecial Jacobians are always related to the supersingular varieties that reach the minimal or maximal number of points. The first result we need is [Lemma 2.2](#), which relates maximality to superspeciality for abelian varieties. The next result connects this to curves.

Lemma 3.20 (Thm. 2.6, [23]). *Let C be a curve over $\mathbb{F}_{p^2}$. Then C is superspecial if and only if C has a twist over $\mathbb{F}_{p^2}$ that is minimal or maximal.*

Remark 3.21. There is a significant difference in behaviour between Jacobians over $\mathbb{F}_p$ of order $(p+1)^2$, and Jacobians over $\mathbb{F}_{p^2}$ of order $(p+1)^4$. Namely, the first category contains both ordinary and supersingular Jacobians, and only the supersingular Jacobians of order $(p+1)^2$ become maximal, i.e., of order $(p+1)^4$ over $\mathbb{F}_{p^2}$. The second category only contains supersingular, and by [Lemma 2.2](#) superspecial, Jacobians.

From this, we get a simple criterion for superspeciality of principally polarized Jacobians: a Jacobian $\mathcal{J}$ is superspecial if and only if the associated curve C is superspecial. [Lemma 3.20](#) shows that this implies a maximal or minimal twist. We derive our main criterion for superspeciality as a direct corollary to [Lemma 3.20](#).

Corollary 3.22. *Let A be a principally polarized abelian surface over $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$. Then A is superspecial if and only if A has a twist over $\mathbb{F}_{p^2}$ that is minimal or maximal.*

We refer to non-minimal or non-maximal superspecial Jacobians as *twisted superspecial Jacobians* to emphasize the dichotomy between minimal and maximal superspecial Jacobians and those Jacobians that require a twist to become minimal or maximal. For the quadratic twist $\mathcal{J}^t$, we know that $\varphi_{\mathcal{J}^t}(x) = \varphi_{\mathcal{J}}(-x)$, and this equals $\varphi_{\mathcal{J}}(x)$ for superspecial Jacobians over $\mathbb{F}_p$, as in the proof of [Lemma 3.8](#). Hence, twisted superspecial Jacobians must arise from non-trivial twists over a larger extension field. Using two known results, we identify curves with additional twists and the effect on characteristic polynomials.

Lemma 3.23 (Ch. X, Thm 2.2(c), [40]). *Let C be a curve over a field k and let G_k denote the Galois group $\text{Gal}(\bar{k}/k)$. Then there is a bijection*

$$\text{Twists}(C/k) \rightarrow H^1(G_k, \text{Aut}(C)).$$

We can therefore associate to any twist C' of C some automorphism $\sigma \in \text{Aut}(C)$, and we will denote C' by C^σ in such a case. Luckily, for a hyperelliptic curve C of genus 2, there are not too many options for $\text{Aut}(C)$: We always have $[-1] \in \text{Aut}(C)$, so we instead analyse the reduced automorphism group $\text{RA}(C) := \text{Aut}(C)/\langle -1 \rangle$. Bolza [6] shows that there are only 7 options for $\text{RA}(C)$. For every option of $\text{RA}(C)$, Cardona [9] computed the corresponding cohomology group. Recall that we are mostly interested in the change of the characteristic polynomial $\varphi_{C^\sigma}(x)$ in terms of $\varphi_C(x)$, which is exactly what Howe, Nart, and Ritzenthaler [21] have described for minimal and maximal curves over $\mathbb{F}_{p^2}$.

Lemma 3.24 (Prop. 13.1, [21]). *Let C be a minimal or maximal supersingular curve over $\mathbb{F}_{p^2}$, so that π acts as $[\pm p]$. Let C^σ be a twist of C induced by $\sigma \in \text{Aut}(C)$, and let f_σ denote the characteristic polynomial of σ . Then*

$$\varphi_{C^\sigma}(x) = p^4 \cdot f_\sigma(x/\pm p).$$

Using [21, Table 4], we know all possible minimal polynomials of automorphisms of genus-2 curves. and may compute which possible automorphisms twist a curve of type $b = \pm 2$ into a curve of type $b \in \{-1, 0, 1\}$. We describe the non-trivial automorphisms τ and ρ on genus-2 hyperelliptic curves in [Appendix A](#).

Proposition 3.25. *Let C be a hyperelliptic curve of genus 2 over $\mathbb{F}_p$ of type $b = \pm 2$ so that $C/\mathbb{F}_{p^2}$ is extremal. Then*

- if $\tau \in \text{RA}(C)$, the twist C^τ over $\mathbb{F}_{p^2}$ has $f_\tau = (x^2 + 1)^2$, so is the base change of a type $b = 0$ surface over $\mathbb{F}_p$,
- if $\rho \in \text{RA}(C)$, the twist C^ρ over $\mathbb{F}_{p^2}$ has $f_\rho = (x^2 + x + 1)^2$, so it is the base change of a type $b = \pm 1$ surface over $\mathbb{F}_p$.

From this we find that twisted superspecial curves and Jacobians are very sparse, as in general Jacobians with non-trivial automorphisms beyond $[-1]$ are sparse in the 3-dimensional space of generic Jacobians:

- $\tau \in \text{RA}(C)$ implies $\text{RA}(C) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, $\text{RA}(C) \cong S_4$, or $\text{RA}(C) \cong D_{2 \times 6}$ which implies $\mathcal{J}$ is $(2, 2)$ -isogenous to a square E^2 for some curve E [19]. This describes a 1-dimensional space of Jacobians.
- $\rho \in \text{RA}(C)$ implies $\text{RA}(C) \cong S_3$, $\text{RA}(C) \cong S_4$, or $\text{RA}(C) \cong D_{2 \times 6}$, which implies $\mathcal{J}$ is $(2, 2)$ -isogenous to a product $E \times E'$ for some curves E and E' that are 3-isogenous [19]. This describes a 1-dimensional space of Jacobians.

Thus, we can very quickly identify the twisted superspecial Jacobians by their automorphism groups, which can be computed efficiently directly from the curve equation or most sets of invariants, such as Igusa or Clebsch invariants [6, 38]. Summarizing, we get the following.

Theorem 3.26. *Let $\mathcal{J}$ be the Jacobian over $\mathbb{F}_p$ of a hyperelliptic curve C of genus 2. Then $\mathcal{J}$ is superspecial if and only if*

- $\mathcal{J}$ is of type $b = \pm 2$,
- $\mathcal{J}$ is of type $b = \pm 1$ and $\text{RA}(C)$ is equal to S_3 , S_4 , or $D_{2 \times 6}$,
- $\mathcal{J}$ is of type $b = 0$ and $\text{RA}(C)$ is equal to $\mathbb{Z}_2 \times \mathbb{Z}_2$, S_4 , or $D_{2 \times 6}$.

For completeness, we perform the same computation and characterization of twisted superspecial Jacobians over $\mathbb{F}_{p^2}$ in [Appendix B](#).

4 Probabilistic Supersingularity Testing

In this section, we derive three main results. First, in [Section 4.1](#), we derive a simple test for minimality or maximality of abelian varieties of any dimension g . Second, we use this result to derive a simple algorithm for superspeciality testing of Jacobians over $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$ in [Section 4.2](#). Third, in [Section 4.4](#), we specialize to Jacobians over $\mathbb{F}_p$ and derive a Monte Carlo algorithm for supersingularity testing of Jacobians $\mathcal{J}$ over $\mathbb{F}_p$ ([Algorithm 4](#)). This last algorithm requires two specific results about Jacobians over $\mathbb{F}_p$:

1. [Theorem 3.12](#): A supersingular Jacobian over $\mathbb{F}_p$ has order $n = p^2 - bp + 1$ for $b \in \{-2, -1, 0, 1, 2\}$. Any abelian surface over $\mathbb{F}_p$ such that $|A(\mathbb{F}_{p^2})| = n^2$ is supersingular.
2. [Theorem 4.7](#): For an abelian surface over $\mathbb{F}_p$, we can verify $|A(\mathbb{F}_{p^2})| = n^2$ by verifying $[n]P = \mathbf{0}$ for random points P . This has only a negligible chance of false positives using a generalization of Sutherland's argument using the width of the Hasse–Weil interval.

We proved the first result in [Section 3.3](#), which allows us to derive the second result in [Section 4.3](#). Together, these give [Algorithm 4](#).

4.1 Minimality and Maximality Testing for Varieties

In this section, we give an algorithm to verify minimality and maximality of abelian varieties of any dimension g over $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$, by generalising the algorithm for our key example ([Algorithm 1](#)) using [Lemma 2.1](#). Similar arguments are used in later sections when we derive supersingularity tests for Jacobians over $\mathbb{F}_p$, and superspeciality tests over $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$.

Algorithm 2 *Let A be an abelian variety of dimension g over $\mathbb{F}_q$ with $q = p$ or p^2 . Let $P \xleftarrow{\$} A(\mathbb{F}_{p^2})$.*

- If $[p]P = \pm P$, return **true**.
- Otherwise, return **false**

[Algorithm 2](#) checks whether A is minimal or maximal, and thus whether it is superspecial by [Lemma 2.2](#). The failure probability is again negligible, as the following result shows.

Theorem 4.1. *[Algorithm 2](#) runs in $O(\log p)$ time and returns **true** for any minimal or maximal abelian variety over $\mathbb{F}_q$. For any non-extremal variety of dimension g , [Algorithm 2](#) returns **true** with probability at most $O(p^{-1})$.*

Proof. This follows directly from [Lemma 2.1](#). We detail the maximal case; the minimal case follows similarly. For the subgroup $H = A[p+1](\mathbb{F}_{p^2})$, we get that $|H|$ divides $(p+1)^{2g}$, and thus if $|H|$ is larger than $4gp^{2g-1}$, then $|A(\mathbb{F}_{p^2})| = (p+1)^{2g}$ and A is maximal, and therefore superspecial. So, for any non-maximal A , the subgroup H is smaller than $O(4gp^{2g-1})$. The probability of sampling a point $P \in A(\mathbb{F}_{p^2})$ such that $[p+1]P = \mathbf{0}$ is equal to the probability of sampling a point in H . In the non-maximal case we therefore have that the probability is

$$\frac{|H|}{|A(\mathbb{F}_{p^2})|} \leq \frac{4gp^{2g-1}}{(p-1)^{2g}} = O(p^{-1}).$$

□

4.2 Superspeciality Testing for Jacobians

By combining [Theorem 4.1](#) with [Corollary 3.22](#), we get the following simple test for superspeciality for Jacobians of any dimension g over both $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$, as long as g is small compared to p .

Algorithm 3 *Let $\mathcal{J}$ be a Jacobian of dimension g of a curve C over $\mathbb{F}_q$ with $q = p$ or p^2 . Let $\text{Aut}(C)$ be the geometric automorphism group of C (i.e., automorphisms defined over $\overline{\mathbb{F}_p}$). For each $\sigma \in \text{Aut}(C)$:*

- *Let $\mathcal{J}^\sigma$ be the Jacobian of the twist C^σ of C by σ over $\mathbb{F}_{p^2}$.*
- *Sample $P \xleftarrow{\$} \mathcal{J}^\sigma(\mathbb{F}_{p^2})$.*
- *If $[p]P = \pm P$, return **true**.*

*If no $\mathcal{J}^\sigma$ passes the $[p]P = \pm P$ test, return **false**.*

[Algorithm 3](#) checks that $\mathcal{J}$ or any of its twists is maximal or minimal, which shows superspeciality by [\[22, Thm. 5.3\]](#). Using [Theorem 4.1](#), we show that the failure probability is again negligible.

Theorem 4.2. *Let $p > g + 1$. Then [Algorithm 3](#) runs in $O(g \log p)$ time and returns **true** for any superspecial Jacobian. For any non-superspecial Jacobian of dimension g , [Algorithm 3](#) returns **true** with probability at most $O((g - 1) \cdot p^{-1})$.*

Proof. By [Theorem 4.1](#), the probability of passing the $[p]P = -P$ test for any non-maximal Jacobian is bounded by $O(p^{-1})$. By Hurwitz’s automorphisms theorem, we get $|\text{Aut}(C)| \leq 84(g - 1)$, as long as $p > g + 1$ [\[36\]](#)⁷ and we can bound the number of twists we have to visit by the size of $\text{Aut}(C)$ by [Lemma 3.23](#). Each test costs $O(\log p)$ group operations, giving a total cost of $O(g \log p)$. Furthermore, if the $[p]P = -P$ test succeeds on any twist $\mathcal{J}^\sigma$, then $\mathcal{J}$ is superspecial and a union bound over the twists gives the stated probability $O((g - 1) \cdot p^{-1})$. The analogous argument holds replacing maximal with minimal and $[p]P = -P$ with $[p]P = P$. $\square$

4.3 Probabilistic Order Determination over $\mathbb{F}_p$

We now generalize Sutherland’s probabilistic argument to cases beyond minimal or maximal abelian surfaces. If a uniformly random point $P \in A(\mathbb{F}_q)$ on an abelian variety A of dimension g over $\mathbb{F}_q$ satisfies $[n]P = \mathbf{0}_A$ for some $n \in \mathbb{N}$, what can we say about the order of $A(\mathbb{F}_q)$? We answer this question for abelian surfaces over $\mathbb{F}_p$ in [Theorem 4.7](#): for the supersingular orders $n = p^2 - bp + 1$, if $[n]P = \mathbf{0}_A$ for a random $P \in A(\mathbb{F}_p)$ and $[n]Q = \mathbf{0}_A$ for a random $Q \in A^t(\mathbb{F}_p)$, then it is extremely likely that A is supersingular (at least for large p). A special case is $b = -2$, which only needs a single test $[n]P = \mathbf{0}_A$ for a random $P \in A(\mathbb{F}_p)$ to verify supersingularity. We derive these results case by case, mainly using [Theorem 3.12](#). We rely heavily on [Corollary 3.2](#).⁸

⁷ Roquette [\[36\]](#) shows this result for all curves except one, but the exceptional curve is itself a superspecial curve.

⁸ As in [Section 3.3](#), the arguments here use only random sampling and scalar multiplication, so no polarization is assumed in this subsection.

The extremal cases $\mathbf{b} = \pm 2$. Interestingly, these differ for $b = -2$ and $b = 2$. The former needs only 1 point, whereas the latter needs 2. In both cases, we multiply by $p \pm 1$ instead of the supersingular order $(p \pm 1)^2$.

Lemma 4.3. *Let A be an abelian surface over $\mathbb{F}_p$. Let P be a random point on $A(\mathbb{F}_p)$. The probability that $[p+1]P = \mathbf{0}$ is*

- 1, if A is supersingular of type $b = -2$,
- $O(p^{-1/2})$, otherwise.

Proof. Let $m = p+1$. The probability to sample a point P with $[m]P = \mathbf{0}$ equals

$$\mathcal{P} := \frac{|A(\mathbb{F}_p)[m]|}{|A(\mathbb{F}_p)|}.$$

Let $h_0, \dots, h_3 \in \mathbb{N}$ be such that $A(\mathbb{F}_p)[m] \cong \mathbb{Z}_{h_0} \times \mathbb{Z}_{h_1} \times \mathbb{Z}_{h_2} \times \mathbb{Z}_{h_3}$ and $h_{i+1} \mid h_i$. From Eq. (1), $h_3 \mid h_2 \mid 2$, and we have $h_1 \mid h_0 \mid p+1$ and $h_1 \mid \lambda_0, h_1 \mid \lambda_1$. Since $\lambda_0 = (p+1)(p-1+a_p) + 2 - b_p$ and $\lambda_1 = -a_p(p+1) - 2a_p - 2(2-b_p)$, this implies $h_1 \mid 2a_p$.

Let $W = 8\sqrt{p}(p+1)$ denote the width of the Hasse–Weil interval over $\mathbb{F}_p$. If $h_0h_1 \leq W$, then $|A(\mathbb{F}_p)[m]| = h_0h_1h_2h_3 \leq 4W$, and therefore

$$\mathcal{P} \leq \frac{4W}{(\sqrt{p}-1)^4} = \frac{32\sqrt{p}(p+1)}{(\sqrt{p}-1)^4} = O(p^{-1/2}).$$

Suppose instead that $h_0h_1 > W$. If $a_p \neq 0$, then $h_1 \leq 2|a_p| \leq 8\sqrt{p}$ by Eq. (3), so that $h_0h_1 \leq 8\sqrt{p}(p+1) = W$, a contradiction. Hence, $a_p = 0$. Now $A(\mathbb{F}_p)$ contains a subgroup isomorphic to $\mathbb{Z}_{h_0} \times \mathbb{Z}_{h_1}$, whose order exceeds W and divides $(p+1)^2$. By Lemma 2.1, $|A(\mathbb{F}_p)| = (p+1)^2$ and so $b_p = -2p$. Therefore, A is supersingular of type $b = -2$ and $\mathcal{P} = 1$. $\square$

Lemma 4.4. *Let A be an abelian surface over $\mathbb{F}_p$. The probability that $[p-1]P = \mathbf{0}$ for a random $P \in A(\mathbb{F}_p)$ and $[p-1]Q = \mathbf{0}$ for a random $Q \in A^t(\mathbb{F}_p)$, is*

- 1, if A is supersingular of type $b = 2$,
- $O(p^{-1/2})$, otherwise.

Proof. Let $G = A[p-1](\mathbb{F}_p)$ and $H = A^t[p-1](\mathbb{F}_p)$ with twisting isomorphism $\rho : A^t \rightarrow A$. Then $S = \langle G, H^\rho \rangle$ is a subgroup of $A(\mathbb{F}_{p^2})$ whose order divides $\#A[p-1] = (p-1)^4$. By the width-bound argument, if $|S| \geq 8(p^3+p)$, then $|A(\mathbb{F}_{p^2})| = (p-1)^4$, which implies A is minimal, and hence superspecial by Lemma 2.2. In particular, it is of type $b = 2$ as this is the only $\mathbb{F}_p$ -type to lift to a minimal abelian surface over $\mathbb{F}_{p^2}$. Thus, in the non-supersingular case we have $|S| \leq 8(p^3+p)$. Since G and H share only the 2-torsion, of size at most 16, and $|S| = |G| \cdot |H|/|G \cap H|$, then $|G| \cdot |H| \leq 16 \cdot |S| \leq 2^7 \cdot p^3 + 2^7 \cdot p$, so at least one of $|G|$ or $|H|$ is smaller than $2^{7/2} \cdot p^{3/2} + \epsilon$. $\square$

Remark 4.5. We stress that the situation for $n = p - 1$ is significantly different from the situation for $n = p + 1$. Indeed, there exist ordinary abelian surfaces $A/\mathbb{F}_p$ such that $[p - 1]A(\mathbb{F}_p) = \mathbf{0}$. An example is given by the Jacobian $\mathcal{J}_C$ over $\mathbb{F}_p$, where $p = 73$, for the hyperelliptic curve

$$C : y^2 = x^6 + 68x^5 + 41x^4 + 31x^3 + 17x^2 + 11x + 51,$$

whose rational group $\mathcal{J}_C(\mathbb{F}_p)$ is isomorphic to

$$\mathcal{J}_C(\mathbb{F}_p) \cong \mathbb{Z}/12 \times \mathbb{Z}/12 \times \mathbb{Z}/6 \times \mathbb{Z}/6.$$

Crucially, the proof of [Lemma 4.3](#) uses the shape of the Weil bounds ([Eq. \(3\)](#)) to make the probability for non-zero a values negligible; similar arguments cannot be repeated for $p - 1$.

The cyclic cases $\mathbf{b} = \mathbf{0}, \pm 1$. All three cases are very similar. We show this for $n = p^2 + p + 1$, the other cases follow mutatis mutandis.

Lemma 4.6. *Let A be an abelian surface over $\mathbb{F}_p$ and let $n = p^2 - bp + 1$ with $b \in \{-1, 0, 1\}$. The probability that $[n]P = \mathbf{0}$ for a random $P \in A(\mathbb{F}_p)$ and $[n]Q = \mathbf{0}$ for a random $Q \in A^t(\mathbb{F}_p)$, is*

- 1, if A is supersingular of type $b = 0, \pm 1$,
- $O(p^{-1/2})$, otherwise.

Proof. Let $H = A[n](\mathbb{F}_p)$ and $G = A^t[n](\mathbb{F}_p)$. These groups do not share points beyond the 2-torsion. We again look at $S = \langle H, G^\rho \rangle$, where ρ is the twisting isomorphism. Let $\gcd(n, p^2 - 1) = d \in \{1, 2, 3\}$. By [Eq. \(1\)](#), beyond the 2-torsion or 3-torsion, the rank of $A[n](\mathbb{F}_{p^2})$ is at most 2, so $|S|$ divides $d^2 n^2$. Suppose first that $d = 1$ so that $|S|$ divides n^2 . By the width-bound argument, $|S| \geq 8(p^3 + p)$ implies $|A(\mathbb{F}_{p^2})| = n^2$, hence A is supersingular by [Theorem 3.12](#). If $d = 2$ or 3, then we replace S by its prime-to- d part, which has order dividing n^2 , and the same argument applies (with the probability bound only losing a constant factor of at most 81). We conclude that either $|S| \geq 8(p^3 + p)$ hence A is supersingular, or $|S| \leq 8(p^3 + p)$ and so the $[n]P = \mathbf{0}$ test succeeds on both A and A^t with probability $O(p^{-1/2})$, similarly as in the proof of [Lemma 4.4](#). $\square$

General Theorem. We summarize the results in this section in the following theorem, which follows directly from [Lemmas 4.3, 4.4](#) and [4.6](#).

Theorem 4.7. *Let $n = p^2 - bp + 1$ for $b \in \{\pm 1, 0\}$, and $n = p \pm 1$ for $b = \mp 2$. Let A be an abelian surface over $\mathbb{F}_p$, P be a random point of $A(\mathbb{F}_p)$ and Q be a random point of $A^t(\mathbb{F}_p)$. Then,*

- if $b = -2$, the probability that $[n]P = \mathbf{0}$ is 1 if A is supersingular, and $O(p^{-1/2})$ otherwise.
- if $b \in \{-1, 0, 1, 2\}$, the probability that $[n]P = \mathbf{0}$ and $[n]Q = \mathbf{0}$ is 1 if A is supersingular, and $O(p^{-1/2})$ otherwise.

Algorithm 4 lsSupersingular**Input:** An abelian surface A defined over $\mathbb{F}_p$.**Output:** A boolean indicating whether A is supersingular. If true, we also return $|A(\mathbb{F}_p)|$.

```

1:  $P \xleftarrow{\$} A(\mathbb{F}_p) \setminus (A[2] \cup A[3])$ 
2:  $Q \xleftarrow{\$} A^t(\mathbb{F}_p) \setminus (A^t[2] \cup A^t[3])$ 
3:  $R \leftarrow [p]P$ 
4: if  $R = -P$  then
5:   return true,  $(p+1)^2$ 
6: if  $R = P$  then
7:    $S \leftarrow [p]Q$ 
8:   if  $S = Q$  then
9:     return true,  $(p-1)^2$ 
10:  $T = [p]R$ 
11: if  $T = -P$  then
12:    $n \leftarrow p^2 + 1$ 
13: else if  $T + P = \pm R$  then
14:    $n \leftarrow p^2 \mp p + 1$ 
15: else
16:   return false
17: if  $[n]Q = 0$  then
18:   return true,  $n$ 
19: return false

```

4.4 Supersingularity Testing for Abelian Surfaces over $\mathbb{F}_p$

Based on [Theorem 4.7](#), we derive a simple algorithm to verify supersingularity for abelian surfaces over $\mathbb{F}_p$ in lsSupersingular.

Theorem 4.8. *Algorithm 4 runs in $O(\log p)$ time and returns **true** for any supersingular abelian surface. For any non-supersingular abelian surface, Algorithm 4 returns **true** with probability $O(p^{-1/2})$.*

Proof. As multiplication-by- p and random sampling can be performed in $O(\log p)$ time, [Algorithm 4](#) terminates in $O(\log p)$. Correctness and probability bounds follow directly from [Theorem 4.7](#), as long as we exclude 2- or 3-torsion. Although cryptographically such torsion occurs with negligible probability, their exclusion ensures that [Algorithm 4](#) never misclassifies a supersingular surface.⁹ $\square$

The probability that lsSupersingular returns **true** when A is ordinary is negligible when p is large. For example, primes p in isogeny-based cryptography are often of size 2λ bits, making the failure probability of lsSupersingular roughly $2^{-\lambda}$ where λ is the security parameter, typically $\lambda \in \{128, 192, 256\}$.

Remark 4.9. It is crucial that the points sampled in [Algorithm 4](#) are uniformly random, otherwise an adversary may always find specific points on specific abelian surfaces that allow an ordinary abelian surface to pass this test. For validation purposes in cryptographic applications, we must therefore assume that an adversary may choose the abelian surface, but not the randomness.

Remark 4.10. We stress that the use of the twist allows the full algorithm to work over $\mathbb{F}_p$ instead of $\mathbb{F}_{p^2}$. Although this doesn't affect asymptotic cost estimates, this significantly affects real-world performance.

⁹ For example, as $\gcd(p^2 + p + 1, p - 1) = 3$ when $p \equiv 1 \pmod 3$, such points could misclassify a supersingular Jacobian of type $b = -1$ as one of type $b = 2$.

5 Conclusive Supersingularity Testing over $\mathbb{F}_p$

In this section, we discuss conclusive variants of supersingularity testing for abelian surfaces over $\mathbb{F}_p$, in contrast to the probabilistic methods from [Section 4](#), as some applications may require *proof* that the Jacobian is supersingular. Similarly, for small characteristics p , [Algorithm 4](#) may have a non-negligible failure rate, and conclusive testing ensures certainty.

A naïve approach simply verifies the explicit order of points $P \in \mathcal{J}(\mathbb{F}_p)$ and $Q \in \mathcal{J}^t(\mathbb{F}_p)$, as a generalization of [\[12, Alg. 1\]](#), using a product tree for additional efficiency. As shown in [\[31\]](#) for elliptic curves, the use of pairings significantly improves this method. We generalize [\[31, Alg. 5\]](#) to Jacobians of genus-2 curves. Due to the existence of isotropic subgroups for $g > 1$, this generalization is non-trivial and requires a precise understanding of isotropy conditions on $\mathcal{J}(\mathbb{F}_p)$, explored in [Sections 5.1](#) and [5.2](#) using results from [Section 3.4](#). We furthermore analyze the requirements of discrete logarithms in μ_{p+1} in verifying supersingularity. Lastly, in [Section 5.4](#), we discuss a specialized variant for Jacobians where 2^f divides the exponent for a large power of f , common in cryptographic applications, which allows a significant speed-up [\[8, Alg. 2\]](#).

5.1 Isotropy on Supersingular Abelian Surfaces of type $b = \pm 2$

For the conclusive supersingularity verification, we will perform specific pairings in $A[m]$ for specific values of $m \in \mathbb{Z}_{>0}$. Depending on the isotropy conditions of these subgroups, the resulting pairing can be computed over $\mathbb{F}_{p^k}$ or $\mathbb{F}_{p^{2k}}$ where k is the embedding degree of m . We prove this case by case per b -type, starting with $b = \pm 2$, where we have a large rank-2 subgroup of $A[m]$, before we discuss the cyclic cases $b \in \{-1, 0, 1\}$.

Lemma 5.1. *Let A be a supersingular abelian surface over $\mathbb{F}_p$ of type $b = 2$ and let $m = p - 1$ or $m = \frac{p-1}{2}$ be the exponent of $A(\mathbb{F}_p)$ and let $n = p - 1$.*

- (i) *The subgroup generated by the eigenspaces $A[\pi - 1] \subseteq A(\mathbb{F}_p)$ and $A[\pi + 1] \subseteq A^t(\mathbb{F}_p)^\rho$ is of index 4 in $A[m] \subseteq A(\mathbb{F}_{p^2})$ if $A(\mathbb{F}_p) \cong (\mathbb{Z}/m\mathbb{Z})^2$, of index 8 if $A(\mathbb{F}_p) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/\frac{m}{2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and of index 1 if $A(\mathbb{F}_p) \cong (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})^2$.*
- (ii) *For every $Q \in A(\mathbb{F}_p)$ of even order k , there exists $P \in A(\mathbb{F}_p)$ such that $e_n(P, Q)$ has order $k/2$.*

Remark 5.2. Note that, according to [Theorem 3.5](#), $p \equiv 3 \pmod{4}$ implies that the exponent is always $m = p - 1$, whereas when $p \equiv 1 \pmod{4}$ both $m = p - 1$ and $m = \frac{p-1}{2}$ can happen.

Proof. (i) This follows directly from [Theorem 3.5](#) and [Lemma 3.16](#).

(ii) As $p + 1 \equiv 2 \pmod{n}$, [Lemma 3.18](#) gives $e_n((\pi + 1)R, Q) = e_n(R, Q)^2$ for all $R \in A[n]$ and $Q \in A(\mathbb{F}_p)$. Let $Q \in A(\mathbb{F}_p)$ have even order k . By non-degeneracy of e_n on $A[n]$, the homomorphism $e_n(\cdot, Q): A[n] \rightarrow \mu_n$ has image μ_k and so there is $R \in A[n]$ with $e_n(R, Q)$ of order k . Then $P = (\pi + 1)R \in A(\mathbb{F}_p)$ satisfies that $e_n(P, Q) = e_n(R, Q)^2$ has order $k/2$. $\square$

[Lemma 5.1](#) shows that abelian surfaces of type $b = 2$ are as non-isotropic as possible, except for the 2-torsion. The case $b = -2$ is the exact opposite.

Lemma 5.3. *Let A be a supersingular abelian surface over $\mathbb{F}_p$ of type $b = -2$ and let $m = p + 1$ or $m = \frac{p+1}{2}$ be the exponent of $A(\mathbb{F}_p)$.*

- (i) *The subgroup generated by eigenspaces $A[\pi - 1] \subseteq A(\mathbb{F}_p)$ and $A[\pi + 1] \subseteq A^t(\mathbb{F}_p)^\rho$ is of index 4 in $A[m] \subseteq A(\mathbb{F}_{p^2})$ if $A(\mathbb{F}_p) \cong (\mathbb{Z}/m\mathbb{Z})^2$, of index 8 if $A(\mathbb{F}_p) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/\frac{m}{2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and of index 1 if $A(\mathbb{F}_p) \cong (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})^2$.*
- (ii) *The pairing e_n is trivial on $A(\mathbb{F}_p)$ and on $A^t(\mathbb{F}_p)^\rho$.*
- (iii) *The pairing*

$$A(\mathbb{F}_p) \times A^t(\mathbb{F}_p) \rightarrow \mu_n, \quad (P, Q) \mapsto e_n(P, Q^\rho),$$

has left kernel $A[2](\mathbb{F}_p)$ and right kernel $A^t[2](\mathbb{F}_p)$.

- (iv) *Let $P_1, P_2 \in A(\mathbb{F}_p)$ and $Q_1, Q_2 \in A^t(\mathbb{F}_p)$, let ζ be a primitive n -th root of unity, and let $M = (\log_\zeta e_n(P_i, Q_j^\rho))_{i,j}$ over $\mathbb{Z}/n\mathbb{Z}$. Then*

$$|\text{im } M| \geq \frac{|\langle P_1, P_2 \rangle| \cdot |\langle Q_1, Q_2 \rangle|}{4n^2}.$$

Proof. (i) This follows directly from [Theorem 3.5](#) and [Lemma 3.16](#).

(ii) Write $G = A(\mathbb{F}_p) = A[\pi - 1]$ and $G^t = A^t(\mathbb{F}_p)^\rho = A[\pi + 1]$. As $p + 1 \equiv 0 \pmod{n}$, [Lemma 3.18](#) gives $e_n((\pi + 1)R, Q) = 1$ for all $R \in A[n]$ and $Q \in G$, and $e_n((\pi - 1)R, S) = 1$ for all $R \in A[n]$ and $S \in G^t$. Since $(\pi + 1)A[n] = G$ and $(\pi - 1)A[n] = G^t$, both G and G^t are isotropic.

(iii) Since G is isotropic of order n^2 in $A[n]$, we have that $G = G^\perp$, and similarly for G^t . Thus, a point $P \in G$ lies in the left kernel if and only if $P \in G^t$, i.e., $P \in G \cap G^t = A[2](\mathbb{F}_p)$. By symmetry, the right kernel is $A^t[2](\mathbb{F}_p)$.

(iv) Write $H = \langle P_1, P_2 \rangle \subseteq G$ and $H^t = \langle Q_1^\rho, Q_2^\rho \rangle \subseteq G^t$. The image of M is the image of the homomorphism $H \rightarrow \text{Hom}(H^t, \mu_n)$, $P \mapsto e_n(P, \cdot)$. This is a composition of maps $H \rightarrow \text{Hom}(G^t, \mu_n)$ with the restriction $\text{Hom}(G^t, \mu_n) \rightarrow \text{Hom}(H^t, \mu_n)$. The first map has kernel $H \cap A[2](\mathbb{F}_p) = H[2]$ by (iii). The order of the kernel is therefore at most 4 (since H is generated by two elements), and the image has order at least $|H|/4$. The restriction map has kernel of order $|G^t : H^t| = n^2/|H^t|$. Hence, $|\text{im } M| \geq |H| \cdot |H^t|/(4n^2)$. $\square$

Remark 5.4. Which of the three cases in (i) of [Lemma 5.1](#) and [Lemma 5.3](#) applies is governed by the 2-rank of $A(\mathbb{F}_p)$ alone: by the index formula of [Lemma 3.16](#), the three group structures listed there are precisely those of 2-rank 2, 3 and 4, giving index 4, 8 and 1 respectively. When A is the Jacobian of a genus-2 curve $C : y^2 = f(x)$, this rank is read off directly from the factorization type of f by [Lemma 3.7](#), so the case distinction costs a single polynomial factorization rather than a group-structure computation. Moreover, [Theorem 3.5](#) forces the 2-rank to be at least 2 when $b = \pm 2$, so a factorization type of f of 2-rank 0 or 1 already certifies that $\mathcal{J}$ is *not* supersingular of type $b = \pm 2$.

The proof of supersingularity for the case $b = 2$ is therefore very efficient: we only need to verify the order of pairing values $\zeta \in \mathbb{F}_p$, and both the pairing and the verification can be computed over $\mathbb{F}_p$. This is because in this case, the eigenspaces 1 and p , resp. -1 and $-p$ collapse, so that the pairing on $A(\mathbb{F}_p)$ is as non-degenerate as possible.

For abelian surfaces of type $b = -2$ the situation is reversed: for $n = p+1$, the pairing e_n is trivial on $A(\mathbb{F}_p)$. Pairings between points of $A(\mathbb{F}_p)$ therefore carry no information, and we instead pair points of $A(\mathbb{F}_p)$ with points of $A^t(\mathbb{F}_p)^\rho$. A single pairing $e_n(P, Q^\rho)$ of order k only shows that $A(\mathbb{F}_p)$ and $A^t(\mathbb{F}_p)$ contain cyclic subgroups of order k , which is too small for the width-bound argument. We therefore take $P_1, P_2 \in A[n](\mathbb{F}_p)$ and $Q_1, Q_2 \in A^t[n](\mathbb{F}_p)$ and compute the four pairings $\zeta_{i,j} = e_n(P_i, Q_j^\rho)$. We can compute a matrix $M = (\log_\zeta \zeta_{i,j})$ with discrete logarithms in μ_n ¹⁰, and then determine the size of its image. By [Lemma 5.3\(iv\)](#), points generating large subgroups of $A(\mathbb{F}_p)$ and $A^t(\mathbb{F}_p)$ give a large image for each of the three possible group structures.

Corollary 5.5. *Let A be an abelian surface over $\mathbb{F}_p$. Write $W = 8\sqrt{p}(p+1)$, the width of the Hasse–Weil interval over $\mathbb{F}_p$.*

- *Let $n = p-1$, and let $P_1, P_2 \in A[n](\mathbb{F}_p)$ and $Q_1, Q_2 \in A^t[n](\mathbb{F}_p)$. If $e_n(P_1, P_2)$ and $e_n(Q_1, Q_2)$ have orders k, k' with $k^2, k'^2 > W$, then A is supersingular of type $b = 2$.*
- *Let $n = p+1$, let ζ be a primitive n -th root of unity, and let $P_1, P_2 \in A[n](\mathbb{F}_p)$ and $Q_1, Q_2 \in A^t[n](\mathbb{F}_p)$. Let $\zeta_{i,j} = e_n(P_i, Q_j^\rho)$, where ρ is the twisting isomorphism. If the matrix $M = (\log_\zeta \zeta_{i,j})_{i,j}$ over $\mathbb{Z}/n\mathbb{Z}$ satisfies $|\text{im } M| > W$, then A is supersingular of type $b = -2$.*

Conversely, let A be supersingular of type $b = \pm 2$ and let $n = p \mp 1$. For p large enough, there exist $P_1, P_2 \in A(\mathbb{F}_p)$ and $Q_1, Q_2 \in A^t(\mathbb{F}_p)$ satisfying the corresponding condition above.

Proof. First let $n = p-1$. If $e_n(P_1, P_2)$ has order k then $|\langle P_1, P_2 \rangle| \geq k^2 > W$. Moreover, $|\langle P_1, P_2 \rangle|$ divides n^2 , so $|A(\mathbb{F}_p)| = (p-1)^2$ by [Lemma 2.1](#). The same argument applied to Q_1, Q_2 gives $|A^t(\mathbb{F}_p)| = (p-1)^2$. It follows that A is supersingular of type $b = 2$.

Now let $n = p+1$. We have that $|\text{im } M| \leq |\langle P_1, P_2 \rangle|$ and, as the images of M and M^T have the same size, we have $|\text{im } M| \leq |\langle Q_1^\rho, Q_2^\rho \rangle| = |\langle Q_1, Q_2 \rangle|$. Both orders divide $n^2 = (p+1)^2$ and (by hypothesis) $|\text{im } M| > W$, so [Lemma 2.1](#) gives $|A(\mathbb{F}_p)| = |A^t(\mathbb{F}_p)| = (p+1)^2$.

For the converse, note that by [Theorem 3.5](#), each of the three possible group structures of $A(\mathbb{F}_p)$ contains a subgroup generated by two elements of order at least $n^2/4$, and the same holds for $A^t(\mathbb{F}_p) \cong A(\mathbb{F}_p)$. Moreover, $A(\mathbb{F}_p)$ contains a point of order at least $n/2$. Let A be of type $b = 2$, so $n = p-1$, and let $Q \in A(\mathbb{F}_p)$ be of maximal order $k_0 \in \{n, n/2\}$. By [Lemma 5.1\(ii\)](#), there is $P \in A(\mathbb{F}_p)$ with

¹⁰ For most applications in isogeny-based cryptography, smoothness of $p+1$ is a common assumption, thus discrete logarithms are efficient.

$e_n(P, Q)$ of order $k = k_0/2 \geq n/4$, and similarly on A^t of order $k' \geq n/4$. Now $k^2 \geq \left(\frac{p-1}{4}\right)^2 > W$ for $p > 2^{18}$. A similar argument holds for type $b = -2$. If moreover $A(\mathbb{F}_p) \cong (\mathbb{Z}/n\mathbb{Z})^2$, which by [Remark 5.4](#) can be read off from the 2-rank of $A(\mathbb{F}_p)$, then any bases give $k = k' = n/2$ for $b = 2$, resp. $|\text{im } M| \geq n^2/4$ for $b = -2$ by [Lemma 5.3\(iv\)](#), and the conditions hold for $p > 2^{10}$. $\square$

Remark 5.6. The converse statement ensures that such a test passes for supersingular surfaces. For cryptographic applications, primes always satisfy these bounds as they are in the range of hundreds of bits. In both cases ($b = \pm 2$), product trees and Lucas sequences can be used to speed up the verification [\[31\]](#), and many operations can remain over $\mathbb{F}_p$ as both points lie on the same $\mathbb{F}_p$ -rational Kummer surface.

5.2 Isotropy on Cyclic Supersingular Abelian Surfaces

Due to their cyclic structure, similar pairing-based techniques for abelian surfaces of type $b \in \{-1, 0, 1\}$ would immediately verify the full group structure of $A(\mathbb{F}_p)$ and $A^t(\mathbb{F}_p)$, i.e., if $P \in A(\mathbb{F}_p)$ and $Q \in A^t(\mathbb{F}_p)$ have a pairing of order n , this verifies both $A(\mathbb{F}_p)$ and $A^t(\mathbb{F}_p)$ have a subgroup of order n . Unfortunately, such pairings will always be trivial, as in general the n -th roots of unity only live in $\mathbb{F}_{p^3}$, $\mathbb{F}_{p^4}$ or $\mathbb{F}_{p^6}$. To perform conclusive supersingularity verification, we must therefore extend the field we work in.

Lemma 5.7 (The case $b = 0$). *Let A be an abelian surface over $\mathbb{F}_p$ of type $b = 0$ and let $m = p^2 + 1$ be the exponent of $A(\mathbb{F}_p)$.*

- (i) *The subgroup generated by the four eigenspaces $A[\pi - 1] \subseteq A(\mathbb{F}_p)$, $A[\pi + 1] \subseteq A^t(\mathbb{F}_p)^\rho$, $A[\pi - p] \subseteq A^t(\mathbb{F}_{p^2})^{\rho'}$ generate a subgroup of index 8 of the full m -torsion $A[m] \subseteq A(\mathbb{F}_{p^4})$.*
- (ii) *Let $P \in A[\pi - 1]$ and $Q \in A[\pi + 1]$, then $e_m(P, Q)$ is trivial.*
- (iii) *For any generators P, Q, R, S of the four eigenspaces (see above), the pairings $e_m(P, R)$ and $e_m(Q, S)$ have order exactly $m/2$.*

Proof. (i) follows from [Theorem 3.5](#) and [Lemma 3.16](#). Write $m = 2m'$ with m' odd (possible as $p^2 \equiv 1 \pmod{8}$). As in the proof of [Lemma 3.16](#), $A(\mathbb{F}_p)$ is cyclic and every eigenspace meets $A[2]$ in $A[2](\mathbb{F}_p) = \langle T \rangle \cong \mathbb{Z}/2\mathbb{Z}$. (ii) By [Lemma 3.17](#), $e_m(P, Q) \in \mu_2$, and its value is $e_2([m']P, [m']Q) = e_2(T, T) = 1$. (iii) The same computation gives $e_2([m']P, [m']R) = 1$, so $e_m(P, R)$ has order dividing m' . For the converse, note that $[A[m] : H] = 8$ is a power of 2, so $H \supseteq A[m']$ and the four eigenspaces restrict to a basis of $A[m'] \cong (\mathbb{Z}/m'\mathbb{Z})^4$. By [Lemma 3.17](#) the pairings $e_m(P, Q), e_m(P, S), e_m(Q, R), e_m(R, S)$ all have order dividing 2, hence are trivial on m' -torsion. The Gram matrix of $e_{m'}$ on this basis therefore has only the entries $e_{m'}(P, R)$ and $e_{m'}(Q, S)$ off the diagonal, and non-degeneracy of $e_{m'}$ forces both to be primitive. Thus, $e_m(P, R)$ has order exactly $m' = m/2$, and likewise for $e_m(Q, S)$. $\square$

The cases $b = \pm 1$ have similar issues: here $m = p^2 \mp p + 1$ is divisible by 3 exactly when $p \equiv \mp 1 \pmod{3}$, and in that case the eigenvalues $1, -1, p, -p$ are no longer distinct modulo 3, resulting in pairings of order $m/3$. However, this will still be enough to give a proof of supersingularity.

Lemma 5.8 (The case $b = 1$). *Let A be an abelian surface over $\mathbb{F}_p$ of type $b = 1$ and let $m = p^2 - p + 1$ be the exponent of $A(\mathbb{F}_p)$.*

- (i) *The subgroup generated by the four eigenspaces $A[\pi - 1] \subseteq A(\mathbb{F}_p)$, $A[\pi + 1] \subseteq A^t(\mathbb{F}_p)^\rho$, $A[\pi - p] \subseteq A^t(\mathbb{F}_{p^3})^\rho$, and $A[\pi + p] \subseteq A(\mathbb{F}_{p^3})$ generate a subgroup of index 9 if $p \equiv 2 \pmod{3}$, and of index 1 otherwise, of the full m -torsion $A[m] \cong (\mathbb{Z}/m\mathbb{Z})^4 \subseteq A(\mathbb{F}_{p^6})$.*
- (ii) *Let $P \in A[\pi - 1]$ and $Q \in A[\pi + 1]$. Then $e_m(P, Q)$ is trivial or has order 3.*
- (iii) *For any generators P, Q, R, S of the four eigenspaces above, the pairings $e_m(P, R)$ and $e_m(Q, S)$ have order $m/3$ or m .*

Proof. (i) This follows directly from Theorem 3.5 and Lemma 3.16. Note $3 \mid m$ if and only if $p \equiv 2 \pmod{3}$ and m is odd. (ii). Since $\gcd(m, 2) = 1$ and $\gcd(m, p + 1) \leq 3$ by Lemma 3.17, we get $e_m(P, Q) \in \mu_3$. (iii). Write $m = 3^e m'$ with $3 \nmid m'$. Arguing as in Lemma 5.7(iii), the index in (i) is a power of 3, so the four eigenspaces restrict to a basis of $A[m']$. By Lemma 3.17, the pairings $e_m(P, Q)$, $e_m(P, S)$, $e_m(Q, R)$, $e_m(R, S)$ all have order dividing 3, hence are trivial on m' -torsion. The non-degeneracy of $e_{m'}$ forces $e_{m'}(P, R)$ to be primitive. The 3-part is not determined: modulo 3 the eigenvalues $\pm 1, \pm p$ collapse in pairs, and e_3 need not vanish between the two resulting order 3 eigengroups.¹¹ If $3 \nmid m$, then $e = 0$ and the order is m . A similar argument holds for $e_m(Q, S)$. $\square$

Lemma 5.9 (The case $b = -1$). *Let A be an abelian surface over $\mathbb{F}_p$ of type $b = -1$ and let $m = p^2 + p + 1$ be the exponent of $A(\mathbb{F}_p)$.*

- (i) *The subgroup generated by the four eigenspaces $A[\pi - 1] \subseteq A(\mathbb{F}_p)$, $A[\pi + 1] \subseteq A^t(\mathbb{F}_p)^\rho$, $A[\pi - p] \subseteq A(\mathbb{F}_{p^3})$, and $A[\pi + p] \subseteq A^t(\mathbb{F}_{p^3})^{\rho'}$ generate a subgroup of index 9 if $p \equiv 1 \pmod{3}$, and of index 1 otherwise, of the full m -torsion $A[m] \cong (\mathbb{Z}/m\mathbb{Z})^4 \subseteq A(\mathbb{F}_{p^6})$.*
- (ii) *Let $P \in A[\pi - 1]$ and $Q \in A[\pi + 1]$. Then $e_m(P, Q)$ is trivial.*
- (iii) *For any generators P, Q, R, S of the four eigenspaces above, the pairings $e_m(P, R)$ and $e_m(Q, S)$ have order $m/3$ or m .*

Proof. As for Lemma 5.8, where $\gcd(m, p + 1) = 1$ gives triviality in (ii). $\square$

Corollary 5.10. *Let A be an abelian surface over $\mathbb{F}_p$, let $b \in \{-1, 0, 1\}$, let $n = p^2 - bp + 1$. Let $P \in A[n](\mathbb{F}_p)$, $Q \in A^t[n](\mathbb{F}_p)$ and $R, S \in A[n]$,¹² and*

¹¹ Experiments suggest the 3-part of $e_m(P, R)$ and $e_m(P, Q)$ is trivial, i.e., that $e_m(P, R)$ has order exactly $m/3$; Corollary 5.10 does not depend on this.

¹² In practice, R and S are taken in the eigenspaces as in Lemma 3.15, so that they are defined (possibly on a twist) over $\mathbb{F}_{p^k}$, where k is the embedding degree of n , and all pairing values lie in $\mu_n \subseteq \mathbb{F}_{p^k}^\times$.

suppose that $\zeta_1 = e_n(P, R)$ and $\zeta_2 = e_n(Q^\rho, S)$ have orders k_1 and k_2 with $k_1 k_2 > 8 \gcd(n, 2) \cdot (p^3 + p)$. Then A is supersingular of type b .

Conversely, let A be supersingular of type $b \in \{-1, 0, 1\}$ and $p > 2^7$, and let $P \in A[\pi - 1]$, $Q^\rho \in A[\pi + 1]$, $R \in A[\pi - p]$ and $S \in A[\pi + p]$ be generators of the four eigenspaces. Then these points satisfy the above condition.

Proof. We have $k_1 \mid \text{ord}(P)$ and $k_2 \mid \text{ord}(Q)$, so the subgroup $H = \langle P, Q^\rho \rangle \subseteq A(\mathbb{F}_{p^2})$ satisfies

$$|H| = \frac{\text{ord}(P) \text{ord}(Q)}{|\langle P \rangle \cap \langle Q^\rho \rangle|} \geq \frac{k_1 k_2}{\gcd(2, n)} > 8(p^3 + p),$$

which is the width of the Hasse–Weil interval over $\mathbb{F}_{p^2}$. Moreover, $|H|$ divides n^2 , so Lemma 2.1 gives $|A(\mathbb{F}_{p^2})| = n^2$. As A is defined over $\mathbb{F}_p$, Theorem 3.12 shows that A is supersingular of type b .

For the converse, $A(\mathbb{F}_p)$ has exponent n . If $b = 0$, then $k_1 = k_2 = n/2$ by Lemma 5.7, and the condition $n^2/4 > 16(p^3 + p)$ holds for $p \geq 67$. If $b = \pm 1$, then n is odd and $k_1, k_2 \geq n/3$ by Lemma 5.8 and Lemma 5.9, and $n^2/9 > 8(p^3 + p)$ holds for $p \geq 79$. $\square$

Remark 5.11. In Corollary 5.10, the points R and S only serve as witnesses: a pairing $e_n(P, R)$ of order k_1 certifies that P has order at least k_1 , and similarly for Q . Supersingularity then follows from the width bound on $\langle P, Q^\rho \rangle$. Such witnesses cannot be found in $A(\mathbb{F}_{p^2})$, as pairings between points of $A(\mathbb{F}_{p^2})$ take values in $\mu_n \cap \mathbb{F}_{p^2}^\times = \mu_{\gcd(n, p^2-1)}$, which has order at most 3. This is why we pass to $\mathbb{F}_{p^k}$, where non-degeneracy of e_n guarantees that suitable witnesses exist.

Proof of Superspeciality. The above results give a proof on the type b of $\mathcal{J}$, and therefore also on $\varphi_{\mathcal{J}}(x)$. Again, following Lemma 2.2, whenever $b = \pm 2$ this immediately also proves that $\mathcal{J}$ is superspecial, and otherwise, following Theorem 3.26, we compute the automorphism group of the associated hyperelliptic curve.

5.3 Conclusive testing of extremal abelian surfaces over $\mathbb{F}_{p^2}$

The pairing-based approach for abelian surfaces of type $b = \pm 2$ directly extends to conclusive pairing-based superspeciality verification of minimal and maximal abelian surfaces over $\mathbb{F}_{p^2}$. However, in these situations, we should no longer assume $\mathbb{F}_p$ -rationality of any points, and hence no longer have the isotropy conditions on $\mathcal{J}(\mathbb{F}_p)$ and $\mathcal{J}^t(\mathbb{F}_p)$ to our advantage. Given a to-be-verified basis $B = \{P_1, \dots, P_4\}$ of $\mathcal{J}(\mathbb{F}_{p^2})$, our approach is to use pairings to determine the size of $H = \langle P_1, \dots, P_4 \rangle$, which implies minimality or maximality as soon as $|H|$ is larger than the width of the Hasse–Weil interval. We describe a simple informal algorithm for maximal abelian surfaces, and the variant for minimal abelian surfaces is self-evident.

Algorithm 5 Let A be an abelian surface over $\mathbb{F}_{p^2}$, and $g \in \mu_{p+1} \subseteq \mathbb{F}_{p^2}^*$ a fixed generator of μ_{p+1} . Repeat the following steps until termination.

1. Sample 4 random points $P_1, \dots, P_4 \xleftarrow{\$} A(\mathbb{F}_{p^2})$
2. If $[p+1]P_i \neq \mathbf{0}_A$ for any i , return **false**
3. Compute $\zeta_{i,j} = e_{p+1}(P_i, P_j)$ and set $Z = (\log_g(\zeta_{i,j}))$ as a matrix over $\mathbb{Z}$
4. Compute the invariant factors d_i of the Smith normal form of Z
5. Set $N_Z = \prod_{i=1}^4 \frac{p+1}{\gcd(d_i, p+1)}$. If $N_Z > 8p^3 + 8p$, return **true**. Otherwise, repeat.

Lemma 5.12. *Algorithm 5 returns **true** only for maximal supersingular abelian surfaces over $\mathbb{F}_{p^2}$, and **false** otherwise.*

Proof. If $[p+1]P_i \neq \mathbf{0}_A$ for any i , then A is clearly non-maximal. Then, when the four points P_i span a subgroup H with $|H| > 8p^3 + 8p$ by the width-bound argument on the Hasse–Weil interval, we have that A must have order $(p+1)^4$, i.e., maximal. We can measure the size of H using the image of Z as a linear map. This can be done effectively¹³ using the invariants $d_1, \dots, d_4$ of the Smith normal form of Z as a matrix over $\mathbb{Z}$: the image of Z is then of size $\prod \frac{p+1}{\gcd(d_i, p+1)}$. $\square$

Remark 5.13. Given a prime p , it is theoretically possible to derive the expected number of iterations required in Algorithm 5. Experimental data for primes of the form $p = 2^k \cdot 5 - 1$ shows that we succeed on the first try with probability over 99% already from $k = 18$. Thus, in practical applications, Algorithm 5 works on the first try.

Remark 5.14. We have written Algorithm 5 with simplicity in mind, however, theoretically, as Algorithm 5 samples random points, it may never terminate as the algorithm could sample low-order points over and over with exponentially small probability. This may be resolved by deterministically sampling points that span an increasingly larger subgroup consistently. For example, if A is a Jacobian $\mathcal{J}$, the deterministic sampling of divisors reduces to deterministically sampling points (x_0, y_0) on the associated hyperelliptic curve C , which can be done by sampling $x_0 = \omega^n$ for a generator ω of k^* and increasing n . However, in practice, such an algorithm is tedious to work with, and does not significantly speed-up validation in practical situations.

5.4 Conclusive Testing for Cryptographic Primes

Isogeny-based cryptography often relies on efficient computations of $(2, 2)$ -isogenies, hence the base field $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$ is chosen so that a large power of 2 divides $p-1$ or $p+1$, and one then works with principally polarized abelian surfaces with group structure $(p-1)^k$, resp. $(p+1)^k$, where $k = 2$ when working over $\mathbb{F}_p$, or $k = 4$ when working over $\mathbb{F}_{p^2}$. This allows one to efficiently compute long chains of $(2, 2)$ -isogenies using rational maximally isotropic $(2^f, 2^f)$ -subgroups, with $2^f \mid p \pm 1$. This large amount of rational $2^\bullet$ -torsion allows us to simplify conclusive testing significantly, by a generalisation of a similar supersingularity test

¹³ See <https://math.stackexchange.com/questions/3252961/image-of-a-linear-transformation-with-a-matrix-in-mathbb-z-m>.

for elliptic curves [8, Alg. 2]. The core idea is to use the $2^\bullet$ -torsion instead of a $2^\bullet$ -pairing to show that both A and A^t have a certain group structure, no matter what the isotropy conditions on this $2^\bullet$ -torsion are. In fact, as we drop the pairing, the results in this subsection do not require the principal polarization either: they rely only on the orders of rational points and the width-bound argument of Lemma 2.1. We analyse these cases first over $\mathbb{F}_p$ and then over $\mathbb{F}_{p^2}$, to give a conclusive test of extremality, hence, superspeciality, hence supersingularity.

Over $\mathbb{F}_p$. We describe this in more detail for abelian surfaces of type $b = -2$, that is, assuming $A(\mathbb{F}_p)$ has order $(p+1)^2$. If P and Q have order 2^f and $[2^{f-1}]P \neq [2^{f-1}]Q$, then $\langle P, Q \rangle \cong (\mathbb{Z}/2^f\mathbb{Z})^2$ gives us a subgroup of size 2^{2f} in $A(\mathbb{F}_p)$. By the width-bound argument, when $2^{2f} > 8 \cdot \sqrt{p} \cdot (p+1)$, which is satisfied as soon as $f > \frac{3}{2} + \frac{3}{4} \log_2 p$, the order of $A(\mathbb{F}_p)$ must be $(p+1)^2$. The next lemma generalizes this argument when relaxing the assumption that P, Q have full order 2^f .

Lemma 5.15. *Let A be an abelian surface over $\mathbb{F}_p$ and let f be the largest integer such that $2^f \mid p+1$. Let $P, Q \in A[2^f](\mathbb{F}_p)$ of order 2^{k_P} and 2^{k_Q} respectively, with $k_P \geq k_Q$. If $[2^{k_P-1}]P \neq [2^{k_Q-1}]Q$ and $k_P + k_Q > 3 + \frac{3}{2} \log_2 p$, then A is supersingular.*

Proof. Since $[2^{k_P-1}]P \neq [2^{k_Q-1}]Q$, we have that $\langle P, Q \rangle \cong \mathbb{Z}_{2^{k_P}} \times \mathbb{Z}_{2^{k_Q}} \hookrightarrow A(\mathbb{F}_p)[p+1]$. Let $A[p+1](\mathbb{F}_p) \cong \mathbb{Z}_{h_0} \times \mathbb{Z}_{h_1} \times \mathbb{Z}_{h_2} \times \mathbb{Z}_{h_3}$ with $h_{i+1} \mid h_i$. Then we have that $h_0 \cdot h_1 \geq 2^{k_P+k_Q} > 8\sqrt{p}(p+1)$. The argument in the proof of Lemma 4.3 shows that $a_p = 0$ and $|A(\mathbb{F}_p)| = (p+1)^2$, so A is supersingular of type $b = -2$. $\square$

Finding such points P and Q is simple: randomly sampling $P, Q \xleftarrow{\$} A(\mathbb{F}_p)$, and using $[h]P, [h]Q$ where $h = \frac{p+1}{2^f}$ almost always works on the first try, as such points almost always have order 2^f or 2^g with g only a bit smaller than f . Thus, for f close to $\log_2 p$, the condition on k_Q is almost always satisfied. Interestingly, one can also sample directly in $A(\mathbb{F}_p) \setminus [2]A(\mathbb{F}_p)$, see e.g. [15, 32], to enforce $k_Q = f$ or $k_Q = f-1$, depending on the exponent of A . In total, this gives a highly efficient conclusive proof of supersingularity using only simple and efficient $\mathbb{F}_p$ -arithmetic for primes such that $2^f \mid p+1$ and $f \approx \log_2 p$. The case $b = 2$ follows similarly as Lemma 5.15, by repeating the above procedure for both $A(\mathbb{F}_p)$ and $A^t(\mathbb{F}_p)$ with $2^f \mid p-1$.

Over $\mathbb{F}_{p^2}$. We again explain the argument only for the maximal case where $A(\mathbb{F}_{p^2})$ has order $(p+1)^4$, and omit the analogous minimal case.

Lemma 5.16. *Let A be an abelian surface over $\mathbb{F}_{p^2}$, let f be the largest integer such that $2^f \mid p+1$ and let $P_1, P_2, P_3, P_4 \in A[p+1]$ be such that $Q_i := [\frac{p+1}{2^f}]P_i$ has order 2^{k_i} for $1 \leq i \leq 4$, and the points $[2^{k_i-1}]Q_i$ span $A(\mathbb{F}_{p^2})[2]$. If $\sum k_i > 3 + 3 \log_2 p$, then A is maximal, hence superspecial.*

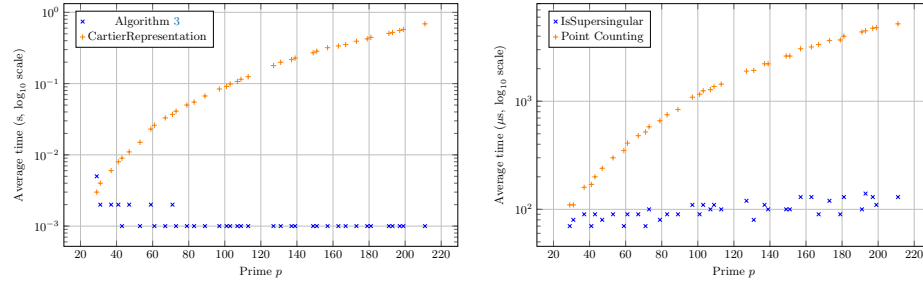
Proof. As for Lemma 5.15, now requiring $2^{\sum k_i} > 8p(p^2+1)$. $\square$

Sampling such a generating set $\{P_1, \dots, P_4\}$ can be done efficiently but is rather technical, see [32, Thm. 1]. Nevertheless, similar to the $\mathbb{F}_p$ -case, sampling random points $P_1, \dots, P_4$ is highly likely to succeed on a first try, as long as the 2-adic order of each of $P_1, \dots, P_4$ exceeds $\frac{3}{4}(1 + \log_2 p)$, and the 2-torsion points below P_i span $A[2]$, so that they are independent.

6 Benchmarking Results

We now compare the performance of our algorithms, which we have implemented in **Magma** [7], to existing methods in the literature to verify supersingularity. We are not aware of other probabilistic methods to verify supersingularity. We therefore compare both **IsSupersingular** as well as the pairing-based conclusive methods to point counting on A . For superspeciality, we compare to the computation of the Cartier–Manin matrix (via **CartierRepresentation**) in **Magma**. Lastly, we also compare the speed-up achieved for primes of the form $p = c \cdot 2^f - 1$ for Jacobians of type $b = -2$, using the $2^\bullet$ -torsion test from Lemma 5.15, as this situation is common in isogeny-based cryptography.

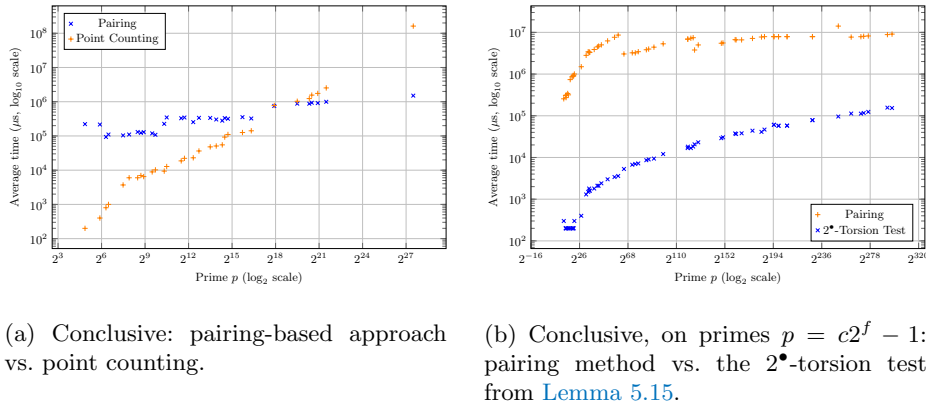
Performance of probabilistic approaches. For superspeciality, we track the average computation time to probabilistically verify superspeciality of 100 supersingular Jacobians over $\mathbb{F}_p$ for primes p from 29 up to 211 with Algorithm 3. We compare this to the computation of the Cartier–Manin matrix in **Magma**. For supersingularity, we track the average computation time to probabilistically verify supersingularity of 1000 supersingular Jacobians over $\mathbb{F}_p$, for primes p from 29 up to 211 with **IsSupersingular** (Algorithm 4). We compare this to a point counting approach based on Lemma 3.8 in **Magma**. The results are given in Fig. 1.



(a) Superspeciality: Algorithm 3 vs. Cartier–Manin matrix computation. (b) Supersingularity: IsSupersingular vs. point counting.

Fig. 1: Performance of probabilistic verification: average time to test 100 Jacobians for superspeciality (left), 1000 for supersingularity (right).

Performance of conclusive approaches. For supersingularity, we track the average total computation time to conclusively verify supersingularity of 100 supersingular Jacobians of type $b = -2$ over $\mathbb{F}_p$, for primes p of the form $p = c2^f - 1$ with $c \in \{5, 3 \cdot 5, 3^2 \cdot 5, 3 \cdot 5 \cdot 7\}$. We first compare the pairing-based methods from Section 5 to the point counting approach based on Lemma 3.8 in Magma, for p from 29 up to $188743679 \approx 2^{27}$ (f between 2 and 22). We then show the improvement of the $2^\bullet$ -torsion test (Lemma 5.15) over the conclusive test from Section 5 in Figure 2, for p from 2^{13} up to 2^{297} (f from 9 up to 293).



(a) Conclusive: pairing-based approach vs. point counting. (b) Conclusive, on primes $p = c2^f - 1$: pairing method vs. the $2^\bullet$ -torsion test from Lemma 5.15.

Fig. 2: Performance of conclusive verification: average time to test 100 Jacobians.

7 Future Work

This work covers probabilistic and conclusive supersingularity and superspeciality testing in dimension 2 over $\mathbb{F}_p$. A natural direction for follow-up work is to determine similar efficient criteria for supersingular abelian varieties of dimension $g > 2$, which comes down to a specific case of the Ekedahl–Oort stratification of particular interest to cryptography. Similarly, the case of abelian surfaces over $\mathbb{F}_{p^2}$ has only been partially answered by this work, as the results in Sections 4 and 5 translate easily to $\mathbb{F}_{p^2}$ for the Jacobians of type $b \in \{\pm 1, \pm 2\}$. The exploration of supersingularity verification for abelian surfaces with other Weil polynomials is left for future work.

Furthermore, the following specializations of the approaches in this work are possible.

Kummer surfaces. When using Kummer surfaces, we do not distinguish P and $-P$. This means we must specialize certain results in this work to such a specific setting, as some results require this precision. For example, we may find ordinary abelian surfaces with $|\mathcal{J}(\mathbb{F}_p)| = (p+1)^2$ and $|\mathcal{J}^t(\mathbb{F}_p)| = (p-1)(p+1)$. This

does not seem too problematic, but a more careful examination of such cases is required to claim with certainty that our probabilistic tests remain convincing. Note that the conclusive tests from [Section 5](#) remain applicable, as such pairings directly verify the *group structure* instead of the order.

Optimized arithmetic. In this work, we have refrained from a detailed analysis of the cost of scalar multiplication and pairings on Jacobians, and instead have simply written $[n]P$ or $e_n(P, Q)$. In practice, one may apply well-known techniques, such as differential addition chains or cubical arithmetic, to determine a precise cost of our algorithms in terms of finite field operations, as has been done in the case of elliptic curves [\[2, 8, 30, 31\]](#).

Non-ordinary abelian surfaces. To complete the efficient Ekedahl-Oort classification for abelian surfaces over $\mathbb{F}_p$, one may study the case of non-ordinary abelian surfaces, i.e., p -rank 1. As such abelian surfaces have similarly specific Weil polynomials, similar methods as proposed in this work should apply, although with different technical derivations and pairing properties.

References

- [1] Marius A. Aardal, Gora Adj, Diego F. Aranha, Andrea Basso, Isaac Andrés Canales Martínez, Jorge Chávez-Saab, Maria Corte-Real Santos, Pierrick Dartois, Luca De Feo, Max Duparc, Jonathan Komada Eriksen, Tako Boris Fouotsa, Décio Luiz Gazzoni Filho, Basil Hess, David Kohel, Antonin Leroux, Patrick Longa, Luciano Maino, Michael Meyer, Kohei Nakagawa, Hiroshi Onuki, Lorenz Panny, Sikhar Patranabis, Christophe Petit, Giacomo Pope, Krijn Reijnders, Damien Robert, Francisco Rodríguez-Henríquez, Sina Schaeffler, and Benjamin Wesolowski. *SQIsign*. Tech. rep. National Institute of Standards and Technology, 2025. URL: <https://sqisign.org> (cit. on p. 1).
- [2] Gustavo Banegas, Valerie Gilchrist, and Benjamin Smith. “Efficient supersingularity testing over $\text{GF}(p)$ and CSIDH key validation”. In: *Transactions on Mathematical Cryptology* 2.1 (2022), pp. 21–35 (cit. on pp. 2, 36).
- [3] Andrea Basso, Giacomo Borin, Wouter Castryck, Maria Corte-Real Santos, Riccardo Invernizzi, Antonin Leroux, Luciano Maino, Frederik Vercauteren, and Benjamin Wesolowski. “PRISM: Simple and Compact Identification and Signatures from Large Prime Degree Isogenies”. In: *Public-Key Cryptography - PKC 2025 - 28th IACR International Conference on Practice and Theory of Public-Key Cryptography, Røros, Norway, May 12-15, 2025, Proceedings, Part III*. Ed. by Tibor Jager and Jiaxin Pan. Vol. 15676. Lecture Notes in Computer Science. Springer, 2025, pp. 300–332. ISBN: 978-3-031-91825-4. DOI: [10.1007/978-3-031-91826-1_10](https://doi.org/10.1007/978-3-031-91826-1_10). URL: https://doi.org/10.1007/978-3-031-91826-1_10 (cit. on p. 1).

- [4] Andrea Basso, Pierrick Dartois, Max Duparc, Jonathan Komada Eriksen, Sabrina Kunzweiler, Michael Meyer, Giacomo Pope, Krijn Reijnders, Damien Robert, Ryan Rueger, and Sina Schaeffler. *MIKE: a fast and compact post-quantum NIKE*. In preparation. (cit. on p. 1).
- [5] Andrea Basso and Luciano Maino. “POKÉ: A Compact and Efficient PKE from Higher-Dimensional Isogenies”. In: *Advances in Cryptology - EUROCRYPT 2025 - 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Madrid, Spain, May 4-8, 2025, Proceedings, Part II*. Ed. by Serge Fehr and Pierre-Alain Fouque. Vol. 15602. Lecture Notes in Computer Science. Springer, 2025, pp. 94–123. ISBN: 978-3-031-91123-1. DOI: [10.1007/978-3-031-91124-8_4](https://doi.org/10.1007/978-3-031-91124-8_4). URL: https://doi.org/10.1007/978-3-031-91124-8_4 (cit. on p. 1).
- [6] Oskar Bolza. “On binary sextics with linear transformations into themselves”. In: *American Journal of Mathematics* (1887), pp. 47–70 (cit. on pp. 19, 20).
- [7] Wieb Bosma, John Cannon, and Catherine Playoust. “The Magma algebra system I: The user language”. In: *Journal of Symbolic Computation* 24.3-4 (1997), pp. 235–265 (cit. on p. 34).
- [8] Fabio Campos, Jorge Chávez-Saab, Jesús-Javier Chi-Domínguez, Michael Meyer, Krijn Reijnders, Francisco Rodríguez-Henríquez, Peter Schwabe, and Thom Wiggers. “Optimizations and Practicality of High-Security CSIDH”. In: *IACR Communications in Cryptology* 1.1 (Apr. 9, 2024). ISSN: 3006-5496. DOI: [10.62056/anjbksdja](https://doi.org/10.62056/anjbksdja) (cit. on pp. 2, 26, 33, 36).
- [9] Gabriel Cardona. “On the number of curves of genus 2 over a finite field”. In: *Finite Fields and Their Applications* 9.4 (2003), pp. 505–526. ISSN: 1071-5797. DOI: [https://doi.org/10.1016/S1071-5797\(03\)00039-X](https://doi.org/10.1016/S1071-5797(03)00039-X). URL: <https://www.sciencedirect.com/science/article/pii/S107157970300039X> (cit. on p. 19).
- [10] Wouter Castryck and Thomas Decru. “An efficient key recovery attack on SIDH”. In: *Annual international conference on the theory and applications of cryptographic techniques*. Springer. 2023, pp. 423–447 (cit. on p. 1).
- [11] Wouter Castryck, Adrian Dina, Péter Kutas, and Gioella Lorenzon. *Post-quantum commutative group actions from oriented superspecial abelian surfaces*. In preparation. (cit. on p. 1).
- [12] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. “CSIDH: An Efficient Post-Quantum Commutative Group Action”. In: *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part III*. Ed. by Thomas Peyrin and Steven D. Galbraith. Vol. 11274. Lecture Notes in Computer Science. Springer, 2018, pp. 395–427. ISBN: 978-3-030-03331-6. DOI: [10.1007/978-3-030-03332-3_15](https://doi.org/10.1007/978-3-030-03332-3_15). URL: https://doi.org/10.1007/978-3-030-03332-3_15 (cit. on pp. 1, 2, 26).

- [13] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. CRC press, 2005 (cit. on p. 6).
- [14] Gunther Cornelissen. “Two-torsion in the Jacobian of hyperelliptic curves over finite fields”. In: *Archiv der Mathematik*, v.77, 241–246 (2001) 77 (Sept. 2001). DOI: [10.1007/PL00000487](https://doi.org/10.1007/PL00000487) (cit. on p. 11).
- [15] Maria Corte-Real Santos and Krijn Reijnders. “Return of the Kummer: a Toolbox for Genus-2 Cryptography”. In: *IACR Communications in Cryptology* 2.4 (Jan. 8, 2026). ISSN: 3006-5496. DOI: [10.62056/a0zogy17s](https://doi.org/10.62056/a0zogy17s) (cit. on p. 33).
- [16] Thomas Decru and Krijn Reijnders. *Expander properties of superspecial isogeny digraphs with level structure*. Cryptology ePrint Archive, Paper 2026/500. 2026. URL: <https://eprint.iacr.org/2026/500> (cit. on p. 41).
- [17] Sanath Devalapurkar and John Halliday. “The Dieudonné modules and Ekedahl-Oort types of Jacobians of hyperelliptic curves in odd characteristic”. In: *arXiv preprint arXiv:1712.04921* (2017) (cit. on p. 4).
- [18] Javad Doliskani. “On division polynomial PIT and supersingularity”. In: *Applicable Algebra in Engineering, Communication and Computing* 29.5 (2018), pp. 393–407 (cit. on p. 2).
- [19] Enric Florit and Benjamin Smith. “An atlas of the Richelot isogeny graph”. In: *Theory and Applications of Supersingular Curves and Supersingular Abelian Varieties*. Vol. B90. RIMS Kôkyûroku Bessatsu. Res. Inst. Math. Sci. (RIMS), Kyoto, 2022, pp. 195–219. URL: <http://hdl.handle.net/2433/276282> (cit. on pp. 20, 41).
- [20] Pierrick Gaudry and Éric Schost. “Genus 2 point counting over prime fields”. In: *Journal of Symbolic Computation* 47.4 (2012). Special Issue for Joachim von zur Gathen at 60, pp. 368–400. ISSN: 0747-7171. DOI: <https://doi.org/10.1016/j.jsc.2011.09.003>. URL: <https://www.sciencedirect.com/science/article/pii/S0747717111001386> (cit. on p. 4).
- [21] Everett W Howe, Enric Nart, and Christophe Ritzenthaler. “Jacobians in isogeny classes of abelian surfaces over finite fields”. In: *Annales de l’Institut Fourier*. Vol. 59. 1. 2009, pp. 239–289 (cit. on pp. 10, 18–20).
- [22] Bruce W Jordan, Allan G Keeton, Bjorn Poonen, Eric M Rains, Nicholas Shepherd-Barron, and John T Tate. “Abelian varieties isogenous to a power of an elliptic curve”. In: *Compositio Mathematica* 154.5 (2018), pp. 934–959 (cit. on pp. 2, 8, 22).
- [23] Ahmad Kazemifard, Alireza Naghipour, and Saeed Tafazolian. “A note on superspecial and maximal curves”. In: *Bulletin of the Iranian Mathematical Society* 39.3 (2013), pp. 405–413 (cit. on p. 18).
- [24] Jean Kieffer. *Counting points on abelian surfaces over finite fields with Elkies’s method*. 2022. arXiv: [2203.02009](https://arxiv.org/abs/2203.02009) [math.NT]. URL: <https://arxiv.org/abs/2203.02009> (cit. on p. 4).

- [25] Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski. “A direct key recovery attack on SIDH”. In: *Annual international conference on the theory and applications of cryptographic techniques*. Springer. 2023, pp. 448–471 (cit. on p. 1).
- [26] Stefano Marseglia. “Weil polynomials of small degree”. In: *Indagationes Mathematicae* (2025) (cit. on p. 7).
- [27] Ben Moonen. “Computing discrete invariants of varieties in positive characteristic I. Ekedahl-Oort types of curves”. In: *Journal of Pure and Applied Algebra* 226.11 (2022), p. 107100 (cit. on p. 4).
- [28] Frans Oort. “A stratification of a moduli space of abelian varieties”. In: *Moduli of abelian varieties*. Springer, 2001, pp. 345–416 (cit. on p. 4).
- [29] Jonathan Pila. “Frobenius maps of abelian varieties and finding roots of unity in finite fields”. In: *Mathematics of Computation* 55.192 (1990), pp. 745–763 (cit. on p. 4).
- [30] Giacomo Pope, Krijn Reijnders, Damien Robert, Alessandro Sferlazza, and Benjamin Smith. “Simpler and Faster Pairings from the Montgomery Ladder”. In: *IACR Communications in Cryptology* 2.2 (July 7, 2025). ISSN: 3006-5496. DOI: [10.62056/ah2i893y6](https://doi.org/10.62056/ah2i893y6) (cit. on p. 36).
- [31] Krijn Reijnders. “Effective Pairings in Isogeny-based Cryptography”. In: *LATINCRYPT 2023*. Springer. 2023, pp. 109–128. DOI: [10.1007/978-3-031-44469-2_6](https://doi.org/10.1007/978-3-031-44469-2_6) (cit. on pp. 2, 26, 29, 36).
- [32] Krijn Reijnders. “The Tate Profile”. In: *Progress in Cryptology - LATINCRYPT 2025 - 9th International Conference on Cryptology and Information Security in Latin America, LATINCRYPT 2025, Medellin, Colombia, October 1-3, 2025, Proceedings*. Springer. 2025 (cit. on pp. 33, 34).
- [33] Damien Robert. “Breaking SIDH in polynomial time”. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2023, pp. 472–503 (cit. on p. 1).
- [34] Damien Robert. *Fast pairings via biextensions and cubical arithmetic*. Cryptology ePrint Archive, Paper 2024/517. 2024. URL: <https://eprint.iacr.org/2024/517> (cit. on p. 2).
- [35] Damien Robert. “The module action for isogeny based cryptography”. In: *IACR Cryptol. ePrint Arch.* 2024 (2024), p. 1556. URL: <https://eprint.iacr.org/2024/1556> (cit. on p. 1).
- [36] Peter Roquette. “Abschätzung der Automorphismenanzahl von Funktionskörpern bei primzahlcharakteristik”. In: *Mathematische Zeitschrift* 117.1 (1970), pp. 157–163 (cit. on p. 22).
- [37] Sergey Rybakov. “The groups of points on abelian varieties over finite fields”. In: *Central European Journal of Mathematics* 8.2 (2010), pp. 282–288. DOI: [10.2478/s11533-010-0003-x](https://doi.org/10.2478/s11533-010-0003-x). URL: <https://doi.org/10.2478/s11533-010-0003-x> (cit. on p. 9).
- [38] Tanush Shaska. “Determining the automorphism group of a hyperelliptic curve”. In: *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*. 2003, pp. 248–254 (cit. on p. 20).

- [39] Jia Shi. *Lifting L -polynomials of genus 2 curves*. 2026. arXiv: [2508.11028](https://arxiv.org/abs/2508.11028) [[math.NT](https://arxiv.org/abs/2508.11028)]. URL: <https://arxiv.org/abs/2508.11028> (cit. on p. 4).
- [40] Joseph H Silverman. *The arithmetic of elliptic curves*. Vol. 106. 2. Springer, 2009 (cit. on pp. 5, 8, 19).
- [41] Andrew Sutherland. “A generic approach to searching for Jacobians”. In: *Mathematics of Computation* 78.265 (2009), pp. 485–507 (cit. on p. 11).
- [42] Andrew V Sutherland. “Identifying supersingular elliptic curves”. In: *LMS Journal of Computation and Mathematics* 15 (2012), pp. 317–325 (cit. on pp. 1, 3).
- [43] Jacques V  lu. “Isog  nies entre courbes elliptiques”. In: *Comptes-Rendus de l’Acad  mie des Sciences* 273 (1971), pp. 238–241 (cit. on p. 5).
- [44] Hui June Zhu. “Group structures of elementary supersingular abelian varieties over finite fields”. In: *Journal of Number Theory* 81.2 (2000), pp. 292–309 (cit. on p. 10).

A Non-trivial Automorphisms of Jacobians

In general, automorphisms of two-dimensional Jacobians are induced by automorphisms of the associated hyperelliptic curves of genus 2. Any Jacobian will have the automorphism $[-1]$, and one therefore often analyzes the *reduced automorphism group* $\text{RA}(C)$, resp., $\text{RA}(\mathcal{J})$.

For dimension 2, the non-trivial reduced automorphism groups are well-understood. An overview of these is given by Florit and Smith [19], and summarized in [16, App. A]. We follow the latter to describe those non-trivial automorphisms used in this work: τ , ρ , ω , $\zeta^{(5)}$, and $\zeta^{(6)}$. We denote a primitive n -th root of unity in $\mathbb{F}_q^*$ by ζ_n .

- The automorphism τ can be described as $x \mapsto 1/x$ on a suitable model for C , which always exists. Its image in $\text{RA}(C)$ has order 2, and its lifts to $\text{Aut}(C)$ satisfy $\tau^2 = \iota$, the hyperelliptic involution.
- The automorphism ρ can be described as $x \mapsto \frac{(2\zeta_3+1)(v^2-1)x+3(v+1)^2}{3(v-1)^2x+(2\zeta_3+1)(v^2-1)}$ for some $v \in \mathbb{F}_q$ on a suitable model for C , which always exists. It has order 3.
- The automorphism ω can be described as $x \mapsto \frac{x-(\sqrt{2}+1)}{(\sqrt{2}-1)x+1}$ on a suitable model for C , which always exists. It has order 4.
- The automorphism $\zeta^{(5)}$ can be described as $x \mapsto \zeta_5 x$ on the curve $C : y^2 = x^5 - 1$. It has order 5.
- The automorphism $\zeta^{(6)}$ can be described as $x \mapsto \zeta_6 x$ on the curve $C : y^2 = x^6 + 1$. It has order 6.

B Classification of Superspecial Jacobians over $\mathbb{F}_{p^2}$

We may repeat a similar computation as we performed in Section 3.5 for Jacobians over $\mathbb{F}_{p^2}$. Namely, given a maximal, resp., minimal, Jacobian, we may compute the characteristic polynomial of a non-quadratic twist C^σ for a non-trivial automorphism $\sigma \in \text{RA}(C)$. This gives us the list of characteristic polynomials of twisted superspecial curves, resp., Jacobians, over $\mathbb{F}_{p^2}$. Similar to the case over $\mathbb{F}_p$, we may use the results in [16, 19] to determine the partial $\text{RA}(C)$ from these results, or a similar characterization of such Jacobians in terms of the associated $(2, 2)$ -isogenous product of elliptic curves. Over $\mathbb{F}_{p^2}$, we write that $\mathcal{J}$ is of type (a, b) if

$$\varphi_{\mathcal{J}}(x) = x^4 - apx^3 + bp^2x^2 - ap^3x + p^4.$$

The quadratic twist maps $(a, b) \mapsto (-a, b)$, hence we may classify these up to $\pm a$.

Theorem B.1. *Let $\mathcal{J}$ be a Jacobian over $\mathbb{F}_{p^2}$. Then $\mathcal{J}$ is superspecial if and only if*

- $\mathcal{J}$ is minimal or maximal, or
- $\mathcal{J}/\mathbb{F}_{p^2}$ is a twisted superspecial

1. of type $(0, -2)$, e.g. $\varphi_{\mathcal{J}}(x) = (x - p)^2(x + p)^2$, and $\sigma \in \text{RA}(C)$ (whose lift in $\text{Aut}(C)$ is an involution not equal to the hyperelliptic involution).
2. of type $(\pm 2, 3)$, e.g. $\varphi_{\mathcal{J}}(x) = (x^2 \pm px + p^2)^2$, and $\rho \in \text{RA}(C)$
3. of type $(0, 2)$, e.g. $\varphi_{\mathcal{J}}(x) = (x^2 + p^2)^2$, and $\tau \in \text{RA}(C)$
4. of type $(\pm 1, 1)$, e.g. $\varphi_{\mathcal{J}}(x) = (x^4 \pm px^3 + p^2x^2 \pm p^3x + p^4)$, and $\zeta^{(5)} \in \text{RA}(C)$
5. of type $(0, 1)$, e.g. $\varphi_{\mathcal{J}}(x) = (x^2 - px + p^2)(x^2 + px + p^2)$, and $\zeta^{(6)} \in \text{RA}(C)$
6. of type $(0, 0)$, e.g. $\varphi_{\mathcal{J}}(x) = (x^4 + p^4)$, and $\omega \in \text{RA}(C)$

Superspeciality Verification. With the above result, superspeciality verification over $\mathbb{F}_{p^2}$ is surprisingly easy: either check that $\mathcal{J}$ is minimal or maximal using the results from [Section 4](#), or compute the automorphism group of the associated hyperelliptic curve, and find a minimal or maximal twist.

Lifting $\mathbb{F}_p$ Curves. Recall that a curve over $\mathbb{F}_p$ with characteristic polynomial $\varphi(x) = \prod (x - \alpha_i)$ lifts to a curve over $\mathbb{F}_{p^2}$ with characteristic polynomial $\varphi(x) = \prod (x - \alpha_i^2)$. This gives us that curves of type $b = \pm 2$ over $\mathbb{F}_p$ become of type $(\pm 4, 6)$ over $\mathbb{F}_{p^2}$, curves of type $b = \pm 1$ become type $(\pm 2, 3)$, and curves of type 0 become type $(0, 2)$.