# On the computation of endomorphism rings of abelian surfaces over finite fields

Samuele Anni Gaetan Bisson Annamaria Iezzi

Elisa Lorenzo García Benjamin Wesolowski

**Abstract**

We study endomorphism rings of principally polarized abelian surfaces over finite fields from a computational viewpoint with a focus on exhaustiveness. In particular, we address the cases of non-ordinary and non-simple varieties. For each possible surface type, we survey known results and, whenever possible, provide improvements and missing results.

## 1 Introduction

Let $A$ be a principally polarized abelian surface defined over a finite field $\mathbb{F}_q$. Its endomorphisms defined over the base field form a ring $\mathrm{End}_{\mathbb{F}_q}(A)$; the corresponding endomorphism algebra $\mathbb{Q} \otimes \mathrm{End}_{\mathbb{F}_q}(A)$ is a division algebra with center $\mathbb{Q}(\pi)$, where $\pi$ denotes the Frobenius endomorphism. Tate [66] shows that the endomorphism algebra of an abelian variety uniquely identifies its isogeny class. The ring $\mathrm{End}(A)$ of endomorphisms of $A$ defined over the algebraic closure $\overline{\mathbb{F}}_q$, which we seek to compute, is sometimes strictly larger than $\mathrm{End}_{\mathbb{F}_q}(A)$ [62, Theorem 2.4]. This ring is an order in the division algebra $K = \mathbb{Q} \otimes \mathrm{End}(A)$ stable under complex conjugation and containing $\mathbb{Z}[\pi, \overline{\pi}]$, where $\overline{\pi} = q/\pi$.

Endomorphism rings of abelian varieties are finer-grained invariants than endomorphism algebras. Their computation allows one to efficiently partition isogeny classes into smaller components, making them highly relevant to both computational number theory and cryptography, with numerous applications, including the evaluation of the hardness of the discrete logarithm problem [34, 11] and the computation of class and modular polynomials [64, 10, 65].

We consider two effective variants of this problem.

**Problem 1.1.** *Given a principally polarized abelian surface defined over a finite field, obtain an abstract representation of its endomorphism ring, that is, a canonical division algebra (such as $\mathbb{Q}[x]/(x^4 + Ax^2 + B)$ in the simple, ordinary case) isomorphic to the endomorphism algebra together with an explicit subring isomorphic to the endomorphism ring.*

**Problem 1.2.** *Given a principally polarized abelian surface defined over a finite field, obtain an explicit generating set of endomorphisms which can be efficiently evaluated.*

Both problems can be related through an explicit embedding $K \to \mathbb{Q} \otimes \mathrm{End}(A)$ where $K$ is a division algebra which depends only on the isogeny class [66]. Here, our efforts focus on Problem 1.2.

This work was supported by Agence Nationale de la Recherche under grant ANR-20-CE40-0013.

SIMPLE ABELIAN SURFACES

| $p$-rank | surface type | End type | Section |
|---|---|---|---|
| 2 | $\mathrm{Jac}(C)$ | $\mathcal{O}$ | 4.1 |
| 1 | $\mathrm{Jac}(C)$ | $\mathcal{O}$ | 4.2 |

NON-SIMPLE ABELIAN SURFACES

| $p$-rank | surface type | End type | Section |
|---|---|---|---|
| 2 | $E_1 \times E_2$<br>$E_1$ and $E_2$ ordinary | $\begin{pmatrix} \mathcal{O}_1 & \mathfrak{a} \\ \widehat{\mathfrak{a}} & \mathcal{O}_2 \end{pmatrix}$ | 5.2.3 |
| 1 | $(E_1 \times E_2)/H$<br>$E_1$ ordinary, $E_2$ supersingular, $H$ finite | suborder of $\mathcal{O}_1 \times \mathcal{R}_2$ | 5.2.2 |
| 0 | $E^2$ or $E^2/\alpha$<br>with $\alpha$ an $\alpha$-group | $\begin{pmatrix} \mathcal{R} & \mathcal{R} \\ \mathcal{R} & \mathcal{R} \end{pmatrix}$ | 5.2.1 |

Table 1: Types of abelian surfaces and associated endomorphism rings, where $\mathcal{O}$ denotes an order in a CM-field, $\mathcal{R}$ a maximal order in the quaternion algebra $\mathbb{Q}_{p,\infty}$, and $\mathfrak{a}$ is an ideal. See the relevant sections for details.

Let $p$ denote the characteristic of the base field, such that we have $q = p^n$ for some positive integer $n$. For an abelian variety of dimension $g$, the $p$-torsion of $A$ satisfies $A[p] \simeq (\mathbb{Z}/p\mathbb{Z})^r$ where the integer $0 \leqslant r \leqslant g$ is called the *$p$-rank* of $A$ and is denoted by $r(A)$. The $p$-rank is invariant under isogenies and satisfies $r(A \times B) = r(A) + r(B)$ for every pair of abelian varieties $A$ and $B$ over $\mathbb{F}_q$. Abelian varieties of $p$-rank $g$ are called *ordinary* and form the generic case: the moduli space of ordinary abelian varieties of dimension $g$ has dimension $g(g+1)/2$, which is also the dimension of the entire moduli space of abelian varieties of dimension $g$. In contrast, abelian varieties whose $p$-rank vanishes are said to be *supersingular*.

Abelian varieties of dimension $g = 1$ are known as elliptic curves and are either ordinary or supersingular. Their endomorphism algebra is an imaginary quadratic field in the ordinary case and a quaternion algebra in the supersingular case. Computing their endomorphism rings was first addressed by Kohel [42] who provided explicit algorithms of exponential complexity. In the ordinary case, this was improved to subexponential-time algorithms by Bisson and Sutherland [7, 4] and, more recently, to a polynomial-time algorithm by Robert [58]. In the supersingular case, state-of-the-art algorithms remain of exponential complexity [22, 26, 55].

Abelian varieties of dimension $g = 2$ are known as abelian surfaces and their $p$-rank is either 0, 1, or 2. Abelian surfaces of $p$-rank 2 form a strata of dimension 3 of the moduli space; those of $p$-rank 1 and 0 form a strata of respective dimension 2 and 1, see [28, Theorem 2.3]. Methods for computing their endomorphism rings were designed only in the ordinary and absolutely simple case, first by Eisenträger and Lauter [23] who described an algorithm of exponential complexity in $\log(q)$ and later by Bisson [3] who obtained a subexponential algorithm.

**Our contribution.** We classify abelian surfaces according to their $p$-rank and whether they are absolutely simple. Table 1 enumerates all cases, each of which will be the topic of a specific section.

The nature of the results we obtain varies with the type of surfaces. This article's first objective is to survey the literature and, whenever possible, to improve upon the state-of-the-art or to fill in missing details. In particular we prove the existence of a general algorithm to solve problem 1.2. In the case of simple surfaces of $p$-rank 1 we show that known methods can be applied and, in the case of non-simple surfaces, we presents new algorithms to compute the associated elliptic factors.

Our algorithms vary in efficiency. Nevertheless their existence holds intrinsic value, as they contribute to a deeper understanding of the landscape and open avenues for further refinement and exploration.

Section 2 contains preliminaries on representing surfaces and computing basic invariants. Section 3 answers the problem of theoretical computability of endomorphism rings and, in particular, of generic endomorphism testing. Section 4 tackles the case of simple surfaces and discusses the lattice of orders, a classical challenge towards problem 1.2. Section 5 deals with non-simple surfaces, where the situation demands a more nuanced approach; in particular, we describe two distinct algorithms to find elliptic subcovers. Section 6 finally considers the particular case of surfaces with extra automorphisms, where elliptic factors can be explicitly given.

# 2 Preliminaries

## 2.1 Representing abelian surfaces and their endomorphisms

Unless otherwise specified, all abelian surfaces are implicitly assumed to be defined over a finite field and endowed with a principal polarization. We represent them differently depending on their type as per the following theorem.

**Proposition 2.1** ([69, Satz 2]). *Every principally polarized abelian surface is either the Jacobian variety of a genus-two curve or the product of two elliptic curves with the product polarization.*

For simple surfaces, we rely on the representation given by the celebrated theorem below.

**Theorem 2.2** ([69] and [1, Section 5.10]). *Let $A$ be a principally polarized abelian surface defined over a finite field $\mathbb{F}_q$. If $A$ is simple over the quadratic extension $\mathbb{F}_{q^2}$, then $A$ is $\mathbb{F}_q$-isomorphic to the Jacobian of a projective smooth curve of genus two.*

Non-simple surfaces are either:

- isomorphic to a product of isogenous elliptic curves;
- Jacobian varieties of algebraic curves which are not isomorphic to such a product.

The endomorphism ring of a product of two elliptic curves $E_1$ and $E_2$ satisfies

$$\mathrm{End}(E_1 \times E_2) = \begin{pmatrix} \mathrm{End}(E_1) & \mathrm{Hom}(E_2, E_1) \\ \mathrm{Hom}(E_1, E_2) & \mathrm{End}(E_2) \end{pmatrix}$$

and its computation is thus reduced to computing their individual endomorphism rings as well as an isogeny between them which may be obtained using the methods of [27]. For surfaces $A$ not isomorphic to such a product, the first step is to identify two elliptic curves $E_1, E_2$ and an isogeny $A \to E_1 \times E_2$. This is addressed in Section 5.3.

Henceforth, we thus focus on surfaces given as the Jacobian variety of a genus-two curve for which points can be represented in Mumford coordinates [50] and the group law computed using Cantor's algorithm [13]. This representation can be extended to non-simple abelian

surfaces which belong to the isogeny class of a Jacobian variety: such surfaces $A$ can be represented as a couple $(\varphi, C)$ whereby $\varphi : \mathrm{Jac}(C) \to A$ is an isogeny. Note however that this representation excludes some non-simple abelian surfaces [30, Theorem 1].

Separable isogenies of simple abelian surfaces and, in particular, their endomorphisms, may be represented by their kernel since they are finite; from a kernel, the corresponding isogeny can be efficiently evaluated using Vélu's formulas [67] and later improvements [2]. Isogenies of non-simple abelian surfaces are represented more naïvely as algebraic maps given by tuples of rational fractions.

### 2.2 Computing basic invariants

Let $A = \mathrm{Jac}(C)$ be the Jacobian variety of a genus-2 hyperelliptic curve $C$ defined over a finite field $\mathbb{F}_q$ where $q = p^n$. Let

$$f_A(t) = t^4 + a_1 t^3 + a_2 t^2 + q a_1 t + q^2 \in \mathbb{Z}[t]$$

denote the characteristic polynomial of its Frobenius endomorphism $\pi$ and set

$$\Delta := a_1^2 - 4a_2 + 8q, \qquad \delta := (a_2 + 2q)^2 - 4q a_1^2.$$

We can determine whether $A$ is absolutely simple from the coefficients of $f_A$ using [32, Theorem 6]. Moreover, the variety $A$ has $p$-rank two if and only if $p \nmid a_2$ and $\Delta$ is not a square in $\mathbb{Z}$; it has $p$-rank one if and only if $p \nmid a_1$, $v_p(a_2) \geqslant \frac{n}{2}$, $\delta$ is not a square in $\mathbb{Z}_p$ and $\Delta$ is not a square in $\mathbb{Z}$; see [47, Theorem 2.9].

We note that, alternatively, the $p$-rank can be determined by looking at the splitting pattern of $p$ in the CM-field $K$ and by the method of [51].

We will sometimes also use the $a$-number which is defined as $a(A) = \dim \mathrm{Hom}_{\mathbb{F}_p}(\alpha_p, A)$ where $\alpha_p$ is the only local-local group scheme over $\mathbb{F}_p$. See [24, Lemma 2.2] for its explicit computation.

Henceforth, we denote by $A \sim B$ the fact that the abelian varieties $A$ and $B$ are isogenous. We denote by $R \simeq R'$ the fact that the groups or algebras $R$ and $R'$ are isomorphic.

## 3 Computability of endomorphism rings

Here we present two generic methods for computing endomorphism rings of abelian surfaces. They are of theoretical interest merely because they prove their computability in the general case. However their time complexity are prohibitive and subsequent sections will present specialized methods which achieve better complexities for each subcase.

### 3.1 Generic endomorphism testing

We borrow the following definition from [71] and refer the reader to [70] for a more precise statement.

**Definition 3.1.** *Let $\varphi : A \to B$ be an isogeny between two abelian varieties defined over a finite field $\mathbb{F}_q$. An* efficient representation *of $\varphi$ with respect to a given algorithm is some data $D_\varphi \in \{0,1\}^*$ such that, on input $D_\varphi$ and $P \in A(\mathbb{F}_q)$, the algorithm returns the evaluation $\varphi(P)$ in polynomial time in* $\mathrm{length}(D_\varphi)$ *and* $\log q$.

We denote by $\alpha^\dagger$ the Rosati involution of an endomorphism $\alpha$ of an abelian variety $A$. This yields a positive definite bilinear form on $\mathrm{End}(A)$ defined by $\langle \alpha, \beta \rangle = \mathrm{tr}(\alpha \circ \beta^\dagger)$. The quadratic structure is computationally available thanks to the following lemma.

**Lemma 3.2.** *Let $A$ be a principally polarized abelian surface. Given two endomorphisms $\alpha, \beta \in \mathrm{End}(A)$, an efficient representation of $\alpha$ and $\beta^\dagger$, and an integer $D$ such that $\langle \alpha, \alpha \rangle, \langle \beta, \beta \rangle < D$, one can compute*

$$\langle \alpha, \beta \rangle = \mathrm{tr}(\alpha \circ \beta^\dagger)$$

*in polynomial time in the length of the input.*

*Proof.* This is inspired by [56, Lemma 7], which itself follows a strategy similar to Schoof's point counting algorithm. The trace of an endomorphism is the trace of its action on the Tate module $T_\ell(A)$ for any prime $\ell$. Thus the action of $\alpha \circ \beta^\dagger$ on $A[\ell]$ reveals $\mathrm{tr}(\alpha \circ \beta^\dagger) \bmod \ell$. Since $|\mathrm{tr}(\alpha \circ \beta^\dagger)| \leqslant D$, it is sufficient to evaluate the action of $\alpha \circ \beta^\dagger$ on $A[\ell]$ for small primes $\ell$ such that $\prod_\ell \ell > 2D$, then recover $\langle \alpha, \beta \rangle$ with the Chinese remainder theorem. □

**Definition 3.3.** *A* good representation *for an isogeny $\varphi : A \to B$ is a triple $(r, r^\dagger, D)$ where $r$ is an efficient representation of $\varphi$, $r^\dagger$ is an efficient representation of $\varphi^\dagger = \lambda_A^{-1} \circ \varphi^\vee \circ \lambda_B$, where $\lambda_A$ and $\lambda_B$ denote the respective polarizations of $A$ and $B$, and $D$ is an integer such that $\mathrm{tr}(\varphi \circ \varphi^\dagger) \leqslant D$.*

**Remark 3.4.** *Let $\varphi$ be an $(\ell, \ell)$-isogeny. Its kernel $K \subset A[\ell]$ is an efficient representation of $\varphi$. Furthermore, the $(\ell, \ell)$-isogeny $\varphi^\dagger$ has kernel $\varphi(A[\ell])$. We deduce that $(K, \varphi(A[\ell]), \ell)$ is a good representation of $\varphi$.*

Per Lemma 3.2, given a good representation for $\alpha, \beta \in \mathrm{End}(A)$, one can compute $\langle \alpha, \beta \rangle$ in polynomial time in the length of the input.

**Proposition 3.5.** *There exists an algorithm which, given a collection of endomorphisms $\alpha = (\alpha_i)_{i=1}^n \in \mathrm{End}(A)$ in good representation, outputs a good representation of a basis of $\mathrm{span}_{\mathbb{Q}}(\alpha) \cap \mathrm{End}(A)$. In particular, if $\alpha$ has full rank, the output is a basis of $\mathrm{End}(A)$.*

*Proof.* From Lemma 3.2, one can compute the Gram matrix $G = (\langle \alpha_i, \alpha_j \rangle)_{i,j}$ for any collection $\alpha$. Up to selecting a subset, we can assume the $\alpha_i$ linearly independent, hence $G$ is of dimension and rank $n$. Let $S = \mathrm{span}_{\mathbb{Z}}(\alpha)$ and $R = \mathrm{span}_{\mathbb{Q}}(\alpha) \cap \mathrm{End}(A)$. We have $S \subset R$, and $[R : S] = \mathrm{vol}(S)/\mathrm{vol}(R)$ (where the volume is with respect to the scalar product $\langle -, - \rangle$). We have $\mathrm{vol}(S)^2 = \det(G) \in \mathbb{Z}$, and similarly, $\mathrm{vol}(R) \in \mathbb{Z}$ since $\langle -, - \rangle$ is integral on $\mathrm{End}(A)$. In particular, $[R : S]^2$ is a divisor of $\det(G)$. The algorithm then proceeds as follows. For each prime $\ell$ whose square divides $\det(G)$:

(Step 1) Let $L \subset S$ be a list of representatives of the finite quotient $S/\ell S$.

(Step 2) For each $\beta \in L$, if $\beta(A[\ell]) = 0$, then we have $\beta/\ell \in R$, we find a basis of $S + \mathbb{Z} \cdot \beta$, and update $S$ and $G$ accordingly to correspond to this larger ring. Return to (Step 1) with the same prime $\ell$.

(Step 3) If no $\beta$ with $\beta(A[\ell]) = 0$ was found we have $\ell \nmid [R : S]$ (i.e., we have reached maximality locally at $\ell$), return to (Step 1) with the next prime $\ell$.

Termination follows from the fact that upon each return to (Step 1), either $[R : S]$ has been divided by a factor $\ell$ (which can only happen finitely many times before reaching $[R : S] = 1$), or one progresses forward in the list of prime factors of $\det(G)$. Correctness follows from the fact that for each $\ell$, one eventually reaches (Step 3), at which point $[R : S]$ is guaranteed not be be divisible by $\ell$ anymore; so once the list of prime factors of $\det(G)$ is exhausted, we get that $[R : S]$ has no prime factor, hence $[R : S] = 1$. □

Note that, the list $L$ computed in (Step 1) is of exponential length in $\log(\ell)$ and hence in the input size. Testing whether $\beta(A[\ell]) = 0$ in (Step 2), when done naively, is also of exponential complexity.

By Proposition 3.5, it only remains to prove that there exists an algorithm that produces a full-rank collection of endomorphisms of $A$. One can compute the rank of any collection as the rank of the Gram matrix. Since the rank of $\mathrm{End}(A) \otimes \mathbb{Q}$ is known, there is an algorithm to check whether a collection has full rank.

**Theorem 3.6.** *There exists an explicit algorithm that, given a principally polarized abelian surface $A$ defined over a finite field $\mathbb{F}_q$, outputs a basis of its endomorphism ring* $\mathrm{End}_{\mathbb{F}_q}(A)$.

*Proof.* At this point, we are only concerned with showing that $\mathrm{End}_{\mathbb{F}_q}(A)$ is computable, with no concern for efficiency. We therefore propose the following naïve strategy. Given a principally polarized abelian surface $A$, exhaustively enumerate all endomorphisms of $A$ by enumerating all possible maps (as tuples of rational fractions of increasing degrees) and testing which are indeed endomorphisms (e.g., testing that the maps indeed send $A$ to itself using Gröbner bases). This results in a sequence $(\alpha_i)_{i=0}^n$ such that $\mathrm{End}_{\mathbb{F}_q}(A) = \{\alpha_i\}_i$, and the algorithm generates each $\alpha_i$ in that order.

From any initial sequence $(\alpha_i)_{i=0}^n$, one can compute the corresponding Gram matrix, and a basis of the lattice it generates. The main difficulty is in deciding at which $n$ to stop (i.e., when $\mathrm{span}_{\mathbb{Z}}(\alpha_i)_{i=0}^n = \mathrm{End}_{\mathbb{F}_q}(A)$). This is where Proposition 3.5 comes in: it is sufficient to reach a point where $\mathrm{rk}(\mathrm{span}_{\mathbb{Z}}(\alpha_i)_{i=0}^n) = \mathrm{rk}(\mathrm{span}_{\mathbb{Z}}(\mathrm{End}_{\mathbb{F}_q}(A)))$, and the algorithm of Proposition 3.5 takes care of the rest. The quantity $\mathrm{rk}(\mathrm{span}_{\mathbb{Z}}(\alpha_i)_{i=0}^n)$ is the rank of the Gram matrix, computable by Lemma 3.2. The quantity $\mathrm{rk}(\mathrm{span}_{\mathbb{Z}}(\mathrm{End}_{\mathbb{F}_q}(A)))$ is the rank of the endomorphism algebra, which can be computed in polynomial time. □

Note that all endomorphisms are defined over extensions of the base field of bounded degree [62, Theorem 2.4]. Therefore, to compute the ring $\mathrm{End}(A)$ of endomorphisms defined over the algebraic closure, one only needs to run the above algorithm over a bounded extension of the base field.

## 3.2 Lifting to characteristic zero

Several algorithms have been designed for the computation of endomorphism rings of abelian varieties defined over a field of characteristic zero [12, 18, 44] and have been used to verify the correctness of the endomorphism data in the $L$-functions and modular forms database (LMFDB) [43] which contains 66, 158 curves of genus two with small minimal absolute discriminant as of February 2025.

Since abelian surfaces of positive $p$-rank defined over finite fields admit a canonical lift [45], the computation of the abstract structure of their endomorphism rings may be transported to characteristic zero. Nevertheless, the computation of such canonical lifts is exponential in $\log(p)$ [59, 46, 60]; furthermore, it is unclear whether characteristic-zero methods for computing endomorphism rings yield better overall complexity than their finite fields counterpart as we are unaware of rigorous complexity bounds for those methods.

Note that, one could avoid the computation of the canonical lift, by taking any lift of the curve with extra endomorphisms [52] and thus obtain the right order up to an index a power of $p$ (see Corollary 6.1.2. in [29]).

**Lemma 3.7.** *Let $A$ be an abelian variety defined over a number field $K$ and $\mathfrak{p}$ be a prime of good reduction of norm $p$. The reduction map $\iota : \mathrm{End}\, A \to \mathrm{End}\, A_{\mathfrak{p}}$ is injective and $[(\iota(\mathrm{End}\, A) \otimes \mathbb{Q}) \cap \mathrm{End}\, A_{\mathfrak{p}} : \mathrm{End}\, A]$ is a power of $p$.*

**Example 3.8.** *Consider the hyperelliptic curve defined over the field* $\mathbb{F}_{11}$ *by*

$$C : y^2 = x^6 + 6x^5 + 4x^4 + 2x^3 + 5x^2 + 7x + 2.$$

*Its Frobenius endomorphism* $\pi$ *has characteristic polynomial* $t^4 + 10t^2 + 121$ *and we find that the order* $\mathbb{Z}[\pi, \overline{\pi}]$ *has index* $2^5$ *in the ring of integers of the quartic field* $K = \mathbb{Q}(\pi)$.

*A lift of this curve which admits extra endomorphisms is*

$$C' : y^2 + x^3 y = x^3 + 2;$$

*which is referenced by LMFDB as "Genus 2 curve* `5184.a.46656.1`*". The endomorphism ring of its Jacobian variety is* $\mathrm{End}_{\mathbb{Q}}(\mathrm{Jac}(C')) = \mathbb{Z}[\sqrt{-2}]$*; thus, the endomorphism ring of* $\mathrm{Jac}(C)$ *contains the order* $\mathcal{O} = \mathbb{Z}[\pi, \overline{\pi}, \sqrt{-2}]$ *which has index* 2 *in the maximal order* $\mathcal{O}_K$*. This reduces the possibilities for* $\mathrm{End}(\mathrm{Jac}(C))$ *to just two cases:* $\mathcal{O}$ *and* $\mathcal{O}_K$*. By computing* $(2,2)$*-isogenies, we eliminate the case* $\mathcal{O}_K$ *and deduce that* $\mathrm{End}(\mathrm{Jac}(C)) = \mathcal{O}$.

# 4 Simple abelian surfaces

Simple abelian surfaces are either of $p$-rank 2 (ordinary) or of $p$-rank 1.

## 4.1 Simple, ordinary case

When $A$ is ordinary, its endomorphism algebra $K = \mathbb{Q}(\pi)$ is a quartic CM-field, that is, an imaginary quadratic extension of a totally real number field $K^+$. The endomorphism ring $\mathrm{End}(A)$ is an order of $K$ containing $\mathbb{Z}[\pi, \overline{\pi}]$ and stable under complex conjugation. Conversely, all such orders are endomorphism rings, see [68]. In particular, the conductor of $\mathrm{End}(A)$ divides the index $\nu = [\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$ where $\mathcal{O}_K$ denotes the ring of integers of $K$.

Classically, the problem of computing $\mathrm{End}(A)$ has been split into two subproblems: first, to determine whether a given order $\mathcal{O}$ is contained in the endomorphism ring $\mathrm{End}(A)$; second, to select suitable candidate orders $\mathcal{O}$ so as to determine $\mathrm{End}(A)$. The latter is covered in Section 4.1.2; from a high level perspective, it computes the localization of $\mathrm{End}(A)$ locally at each prime $\ell$ dividing the conductor $\nu$, from which $\mathrm{End}(A)$ is eventually deduced.

### 4.1.1 Testing candidate orders

Assume a candidate order $\mathcal{O}$ of $K$ is fixed and we wish to determine whether $\mathcal{O} \subset \mathrm{End}(A)$ holds. Depending on the prime $\ell$ and other factors, we might elect to choose one of the methods below.

**The method of Eisenträger–Lauter [23].** This method exploits the following observation: let $\alpha$ be an endomorphism of $A$ and let $\ell$ be an integer coprime to $p$; then we have $\alpha/\ell \in \mathrm{End}(A)$ if and only if $A[\ell] \subset \ker(\alpha)$ holds. This can be computed efficiently when the $\ell$-torsion subgroup $A[\ell]$ is defined over relatively small extension fields. Generically, however, the torsion $A[\ell]$ may be defined over extensions of degree as large as $\ell^g$ and the primes $\ell$ themselves, being factors of $\nu$, are only bounded by $2^{g(2g-1)} q^{g^2/2}$. This algorithm thus has an exponential complexity in the worst case.

**The method of Bisson [3].** This approach exploits complex multiplication theory and, more specifically, the faithful action of the polarized class group $\mathfrak{C}(\mathcal{O})$ of Shimura [61] on the set of isomorphism classes of principally polarized abelian varieties with endomorphism ring $\mathcal{O}$. The main idea is to construct polarized ideals which are trivial in $\mathfrak{C}(\mathcal{O})$, to evaluate the corresponding isogenies, and to check that those are in fact endomorphisms. When we have $\mathcal{O} \subset \mathrm{End}(A)$, this is always the case. Conversely, if all principal polarized ideals map to endomorphisms, one shows [6] that the order $\mathcal{O}$ is never "far" from being a suborder of $\mathrm{End}(A)$. Applying the method of Eisenträger–Lauter locally at small primes allows one to overcome this and obtain a full converse. This yields an algorithm of heuristic, subexponential complexity to determine whether the inclusion $\mathcal{O} \subset \mathrm{End}(A)$ holds.

An abelian variety $A$ is said to have *maximal real multiplication* if its endomorphism ring $\mathrm{End}(A)$ contains $\mathcal{O}_{K^+}$. In this particular case, assuming furthermore that the narrow class group of $K^+$ is trivial, Springer [63] improves Bisson's method by exploiting the classical class group instead of the polarized class group. This yields an algorithm which relies on fewer heuristics.

**The method of Robert [58].** Robert exploits Kani's diamond lemma [39] to obtain a polynomial-time algorithm testing whether certain maps of elliptic curve are in fact endomorphisms. Although it is written in the case of ordinary elliptic curves, there is no obstacle to its generalization to simple, ordinary abelian surfaces. However, this does not necessarily give a polynomial-time algorithm for computing endomorphism rings, since this depends on the number of orders to test, a problem to which we now turn.

### 4.1.2 Ascending the lattice of orders

The general idea of [3, Algorithm 6.2] is as follows: starting from $\mathcal{O}' = \mathbb{Z}[\pi, \overline{\pi}]$, iterate over orders $\mathcal{O}$ which are *directly above* $O'$ (that is, such that $\mathcal{O}' \subset \mathcal{O}$ and no other order strictly lies between them); if $\mathcal{O} \subset \mathrm{End}(A)$, then set $\mathcal{O}' \leftarrow O$ and repeat until there are no more orders to test; eventually, return $\mathrm{End}(A) = \mathcal{O}'$.

For elliptic curves, the CM-field $K$ is a quadratic CM-field. Locally at any prime $\ell$, its lattice of orders is thus linear and there is only one order to consider above every given one; this can be efficiently exploited, see [4, Section 5]. Coupled with Robert's testing method, this yields a polynomial-time algorithm for computing the endomorphism ring of ordinary elliptic curves.

In quartic CM-fields, however, there can be exponentially many such orders stable under complex conjugation. In particular, this is always the case when $\ell^3 \mid [\mathcal{O}_K : \mathcal{O}]$; see [25, Lemma 5.3]. One may try to limit the number of orders to test by first computing the real part of the endomorphism ring.

Denote by $K^+$ the maximal totally real subfield of $K$, let $\mathcal{O} = \mathrm{End}(A)$ and let $\mathcal{O}_+ = \mathcal{O} \cap \mathcal{O}_{K^+}$. Note that $\mathcal{O}_+$ can be computed in polynomial time, as $K^+$ is quadratic and therefore its lattice of orders is linear locally at each prime $\ell$. Let $\mathcal{O}^\#$ be the largest order in $\mathcal{O}_K$ such that $\mathcal{O}^\# \cap \mathcal{O}_{K^+} = \mathcal{O}_+$, which exists as a consequence of the following lemma.

**Lemma 4.1.** *For $i = 1, 2$, let $\mathcal{O}_i$ be two suborders of $\mathcal{O}_K$ stable under complex conjugation such that $\mathcal{O}_i \cap \mathcal{O}_{K^+} = \mathcal{O}_+$. Locally at any prime $\ell \neq 2$ we have $(\mathcal{O}_1 + \mathcal{O}_2) \cap \mathcal{O}_{K^+} = \mathcal{O}_+$.*

*Proof.* Let $x \in (\mathcal{O}_1 + \mathcal{O}_2) \cap \mathcal{O}_{K^+}$. We have $x = x_1 + x_2 \in \mathbb{R}$ with $x_i \in \mathcal{O}_i$. Thus $2x = x + \bar{x} = x_1 + \bar{x}_1 + x_2 + \bar{x}_2 \in (\mathcal{O}_1 \cap \mathcal{O}_{K^+}) + (\mathcal{O}_2 \cap \mathcal{O}_{K^+}) = O_+$. □

We thus have the inclusions of orders displayed in Figure 1.

However, the result below, which is a generalization of [25, Lemma 5.3], shows that there are still exponentially many orders within the resulting bounds for $\mathrm{End}(A)$.

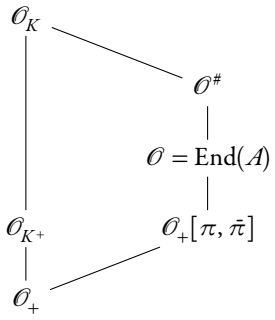


Figure 1: Inclusions between orders in a quartic CM-field and their intersections with the totally real subfield.

**Lemma 4.2.** *Let $K$ be a quartic CM-field; denote by $K^+$ its totally real subfield. Let $\mathcal{O}$ be an order in $K$ stable under complex conjugation $\sigma$. Let $\ell$ be an odd prime. The number of orders which are stable under complex conjugation, contained in $\mathcal{O} \cap K^+ + \ell\mathcal{O}$ and containing $\mathcal{O} \cap K^+ + \ell^2\mathcal{O}$, is greater than $\ell$.*

*Proof.* These orders correspond to submodules over $\mathbb{F}_\ell[\{1, \sigma\}]$ of $(\mathcal{O} \cap K^+ + \ell\mathcal{O})/(\mathcal{O} \cap K^+ + \ell^2\mathcal{O})$. By Maschke's theorem, $\mathbb{F}_\ell[\{1, \sigma\}]$ is semisimple: it admits two absolutely irreducible modules, $V_+$ and $V_-$, each of dimension one over $\mathbb{F}_\ell$. Thus, the quotient above is isomorphic to $V_+^{n_+} \oplus V_-^{n_-}$ where $n_+$ and $n_-$ are non-negative integers whose sum equals the dimension of the quotient, that is, two. Since the action of $\sigma$ on $V_-$ is nontrivial and it stabilizes the direct sum, the integer $n_-$ is even. Thus, one of $n_+$ or $n_-$ equals two and the corresponding module $V^n$ has $\frac{\ell^2-1}{\ell-1} = \ell + 1$ submodules. □

We conclude that classical methods for computing the endomorphism rings by ascending the lattice of orders cannot have subexponential worst-case complexity in the general case.

## 4.2 Simple, $p$-rank-1 case

Recall that $p$-rank-1 abelian surfaces may be efficiently detected via the following result.

**Lemma 4.3** ([51, Lemma 1])**.** *A simple abelian surface $A$ defined over $\mathbb{F}_q$, with $q = p^n$, has $p$-rank 1 if and only if the following conditions are satisfied:*

1. *the field $K = \mathbb{Q}(\pi)$ is a quartic CM-field,*
2. *the prime $p$ splits in $K$ as $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}}_1\mathfrak{p}_2^e$, where $e \in \{1, 2\}$, and*
3. *we have $\pi\mathcal{O}_K = \mathfrak{p}_1^n\mathfrak{p}_2^{en/2}$, with $e$ as in Condition (2).*

In particular, endomorphism rings of $p$-rank-1 surfaces are specific orders among those of ordinary surfaces. The techniques of Section 4.1.2 therefore apply equally to the case of $p$-rank-1 surfaces.

To compute the endomorphism rings, these techniques may be coupled with the method of Eisenträger and Lauter [23] or even of Bisson [3]. Indeed, by the theory of Shimura and Taniyama [61], isogenies between $p$-rank-1 surfaces correspond to ideals of orders of the endomorphism algebra. Since this algebra is of the same type as those of ordinary surfaces,

the free action of [3, Section 2], the endomorphism ring testing routine of [3, Section 5], the resulting method [3, Algorithm 6.2], the main result [3, Theorem 7.1] and its proof all apply without and modification to abelian surfaces of $p$-rank-1.

**Example 4.4.** *Consider the Jacobian variety $A$ of the genus-two curve*

$$y^2 = 23535x^6 + 6448x^5 + 20387x^4 + 3811x^3 + 11376x^2 + 11282x + 21340$$

*defined over the finite field with* 36877 *elements. It is absolutely simple, has $p$-rank 1, and satisfies $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]] = 431$ with the* 431*-torsion of $A$ being defined over an extension of degree* 5003910*. In the ring of integers of $K$, we have $3 = \mathfrak{a}\overline{\mathfrak{a}}$ where $\mathfrak{a}$ is a prime ideal of norm* 9*. The element $(\mathfrak{a}, 3)$ is of order* 736 *in the polarized class group $\mathfrak{C}(\mathcal{O}_K)$ but not in $\mathfrak{C}(\mathbb{Z}[\pi, \overline{\pi}])$. We compute the sequence of* 736 *isogenies of type* $(3, 3)$ *corresponding to the ideal $\mathfrak{a}$ and land on the Jacobian variety of a genus-two curve whose invariants are different to that of $A$. Hence we deduce* $\mathrm{End}(A) \subsetneq \mathcal{O}_K$ *and therefore* $\mathrm{End}(A) = \mathbb{Z}[\pi, \overline{\pi}]$*. The AVIsogenies Magma package [5] performs this computation in just about three minutes overall on a single Intel i5-8365U CPU core.*

# 5 Non-simple abelian surfaces

The endomorphism algebra of non-simple abelian surfaces has dimension greater than 4. Since $\mathbb{Q}(\pi, \bar{\pi})$ has only dimension 1 or 2, the strategy consisting in ascending the lattice of orders described previously does not apply, which is why we rely on the more explicit results below.

## 5.1 Using coprime isogenies

Suppose we want to compute a basis of $\mathrm{End}(A)$. In this section, we prove that this problem reduces to computing the endomorphism rings of two other abelian surfaces $B$ and $C$ connected to $A$ by isogenies of coprime degrees. One could thus compute random isogenies from $A$ with codomain two abelian varieties $B$ and $C$ of which the endomorphism rings are known or simpler to compute.

**Proposition 5.1.** *Suppose we are given a good representation of isogenies $\varphi : A \to B$ and $\psi : A \to C$ of coprime degrees, of their duals, and of a basis of* $\mathrm{End}(B)$ *and* $\mathrm{End}(C)$*. Then, one can compute a good representation of a basis of* $\mathrm{End}(A)$ *in polynomial time in the length of the input.*

*Proof.* Recall that, for any isogeny $\psi : A \to B$, there is unique isogeny $\widehat{\psi} : B \to A$ such that $\psi\widehat{\psi} = [\deg(\psi)]$.

Let $(\eta_i)_i \subset \mathrm{End}(B)$ and $(\nu_i)_i \subset \mathrm{End}(C)$ be the provided bases. Let $\beta_i = \widehat{\varphi} \circ \eta_i \circ \varphi$, and $\gamma_i = \widehat{\psi} \circ \nu_i \circ \psi$. The lattices in $\mathrm{End}(A)$ generated by $(\beta_i)_i$ and $(\gamma_i)_i$ are $\Lambda_B = \widehat{\varphi} \circ \mathrm{End}(B) \circ \varphi$ and $\Lambda_C = \widehat{\psi} \circ \mathrm{End}(C) \circ \psi$ respectively. We have $\deg(\varphi)^2 \mathrm{End}(A) \subset \Lambda_B \subset \mathrm{End}(A)$, and $\deg(\psi)^2 \mathrm{End}(A) \subset \Lambda_C \subset \mathrm{End}(A)$. We deduce that $[\mathrm{End}(A) : \Lambda_B]$ and $[\mathrm{End}(A) : \Lambda_C]$ are coprime, since $\deg(\varphi)$ and $\deg(\psi)$ are. This implies $\Lambda_B + \Lambda_C = \mathrm{End}(A)$, hence $\mathrm{End}(A)$ is generated by the union of $(\beta_i)_i$ and $(\gamma_i)_i$. From Lemma 3.2, we can compute the Gram matrix of this generating set, from which we deduce a basis. □

Sometimes we will not have such coprime degree isogenies at our disposal, for instance in the $p$-rank 0 and $a$-number 1 case. Nevertheless, in the case of non-simple varieties, we may use the following well-known results.

**Lemma 5.2.** *Let $s_1 : A \to B$ and $s_2 : A \to C$ be isogenies. There exists a third isogeny $s_3 : C \to B$ such that $s_1 = s_3 s_2$ if and only if* $\ker(s_2) \subset \ker(s_1)$.

**Corollary 5.3.** *Let $s_1 : A \to B$ and $s_3 : C \to B$ be isogenies. There exists a third isogeny $s_2 : A \to C$ such that $s_1 = s_3 s_2$ if and only if* $\ker(\widehat{s}_3) \subset \ker(\widehat{s}_1)$.

## 5.2 Structure of the endomorphism algebra

Recall that an abelian variety $A$ is non simple if and only if it is isogenous to a product of elliptic curves over the algebraic closure. The non-simplicity of $A$ can be detected by computing the characteristic polynomial $f_A$ of its Frobenius endomorphism [32, Theorem 6] and so the isogeny classes of the elliptic factors follow.

There are three possibilities to consider for the $p$-rank: 0, 1, and 2. The $p$-rank can be computed as described in Section 4 via [47, Theorem 2.9].

### 5.2.1 $p$-rank-0 case

Recall the following result from Oort.

**Proposition 5.4** ([53, Theorem 4.2])**.** *For any given three supersingular elliptic curves $E, E_1, E_2$ defined over an algebraically closed field, there is an isogeny $E^2 \sim E_1 \times E_2$.*

Fix $E$ a supersingular elliptic curve. Following Oort [54], for every $(i, j) \in \overline{\mathbb{F}}_p^2$, we denote by $A_{i,j}$ the abelian surface defined over $\overline{\mathbb{F}}_p$ through the following diagram:

$$0 \to \alpha_p \xrightarrow{(i,j)} E \times E \to A_{i,j} \to 0.$$

In the $p$-rank-0 case, there are two possibilities for the $a$-number: 1 and 2.

**Proposition 5.5** ([31, Proposition 11.1], restating results from [54])**.** *Let $A$ be an abelian surface of $p$-rank 0. We have $a(A) = 2$ if and only if $A \simeq E \times E$. We have $a(A) = 1$ if and only if $A \simeq A_{ij}$ for some $[i : j] \in \mathbb{P}^1(\overline{\mathbb{F}}_p) \setminus \mathbb{P}^1(\mathbb{F}_{p^2})$. Furthermore, if $a(A) = 1$ then $a(A/\alpha_p) = 2$.*

As a consequence, in the $p$-rank 0 case, the endomorphism algebra is isomorphic to $\mathcal{M}_2(\mathcal{B}_{p,\infty})$. In particular, in the $a$-number 2 case we can solve Problem 1.1 since we have $\mathrm{End}(E \times E) \simeq \mathcal{M}_2(R)$ where $R$ is any maximal order in the quaternion algebra $\mathcal{B}_{p,\infty}$. The computational difficulty here is to find an explicit isomorphism or isogeny from $A$ to $E \times E$. We will address this problem in Section 5.3.

For the remainder of this section, we address the problem of explicitly computing endomorphisms in the $a$-number 1 case. Let $A = A_{i,j} \sim (E \times E)/(i, j)(\alpha_p)$ and denote by $\varphi : E \times E \to A$ the corresponding isogeny. We have

$$p \cdot \mathrm{End}(E \times E) \subset \mathrm{End}(A) \subset \frac{1}{p} \mathrm{End}(E \times E)$$

where $\beta \in \mathrm{End}(E \times E)$ goes to $\frac{1}{p}\varphi \circ \beta \circ \varphi^{-1}$ and $\gamma \in \mathrm{End}(A)$ goes to $\frac{1}{p}\varphi^{-1} \circ \gamma \circ \varphi$.

Given $\begin{pmatrix} x & y \\ z & w \end{pmatrix} \in \mathrm{End}(E \times E)$ we want to determine whether it is of the form $\frac{1}{p}\varphi^{-1} \circ \gamma \circ \varphi$ for some $\gamma \in \mathrm{End}(A)$. To this extent, we use the Lemma 5.2 together with the following result.

**Lemma 5.6.** *If $x$ is an endomorphism, denote by $\widehat{x}$ its dual and let $|x| = x \circ \widehat{x}$ and* $\mathrm{tr}(x) = x + \widehat{x}$. *Given $x$, $y$, $w$ and $z$ four elements of* $\mathrm{End}(E)$, *we have*

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} \widehat{x}|w| - \widehat{z}w\widehat{y} & \widehat{z}|y| - \widehat{x}y\widehat{w} \\ \widehat{y}|z| - \widehat{w}z\widehat{x} & \widehat{w}|x| - \widehat{y}x\widehat{z} \end{pmatrix} = \left(|x||w| + |y||z| - \mathrm{tr}(x\widehat{z}w\widehat{y})\right) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

**Theorem 5.7.** *Let $A$ be an abelian surface of $p$-rank* 0 *and $a$-number* 1. *Its endomorphism ring is*

$$\mathrm{End}(A) \simeq \left\{ \begin{pmatrix} x & -\frac{i}{j}x + u\pi \\ z & -\frac{i}{j}z + v\pi \end{pmatrix} : x, z, u, v \in \mathrm{End}(E) \right\}.$$

*where the fraction $\frac{i}{j}$ denotes the corresponding integer modulo $p$.*

*Proof.* Let $m = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \in \mathrm{End}(E \times E)$. We know that $m \in \mathrm{End}(A)$ if and only if $\ker\varphi \subset \ker m$ and

$$\ker(\varphi) \subset \ker \begin{pmatrix} \widehat{x}|w| - \widehat{z}w\widehat{y} & \widehat{z}|y| - \widehat{x}y\widehat{w} \\ \widehat{y}|z| - \widehat{w}z\widehat{x} & \widehat{w}|x| - \widehat{y}x\widehat{z} \end{pmatrix}.$$

Applying Lemma 5.2 to $s_1 = m$ and $s_2 = \varphi$, the first condition implies that $y$ and $w$ are of the form

$$y = -\frac{i}{j}x + u\pi \qquad \text{and} \qquad w = -\frac{i}{j}z + v\pi$$

for some endomorphisms $u$ and $v$. Then we have $\widehat{y} = -\frac{i}{j}\widehat{x} + V\widehat{u} = -\frac{i}{j}\widehat{x} + u'V$. Similarly, we have $\widehat{w} = -\frac{i}{j}\widehat{z} + v'V$. Therefore, the second condition always holds if the first one does. □

### 5.2.2 $p$-rank-1 case

First of all, let us recall that if an abelian surface decomposes as a product of an ordinary and a supersingular elliptic curve, this decomposition occurs on the base field.

**Corollary 5.8** ([32] and [47, Corollary 2.17]). *If an abelian surface $A$ defined over $\mathbb{F}_q$ decomposes over $\overline{\mathbb{F}}_q$ as the product of two elliptic curves, one supersingular, the other ordinary, then $A$ decomposes over the base field $\mathbb{F}_q$.*

The following result describes the algebra and the endomorphism ring in the case of $p$-rank 1.

**Proposition 5.9.** *Let $A/\mathbb{F}_q$ be a non-simple abelian surface of $p$-rank* 1. *It is isomorphic to a quotient $(E_1 \times E_2)/H$ where $E_1$ is an ordinary elliptic curve, $E_2$ is a supersingular one, and $H$ is a finite subgroup. In other words, we have an exact sequence*

$$1 \to H \to E_1 \times E_2 \xrightarrow{\varphi} A \to 1$$

*which gives an isomorphism of endomorphism algebras*

$$\mathbb{Q} \otimes \mathrm{End}(A) \simeq \mathbb{Q} \otimes (\mathrm{End}(E_1) \times \mathrm{End}(E_2)).$$

*More precisely, the endomorphism ring* $\mathrm{End}(A)$ *is the suborder of* $\mathrm{End}(E_1) \times \mathrm{End}(E_2)$ *made of elements $s$ such that $H \subset \ker s$.*

*Proof.* The decomposition of the characteristic polynomial of the Frobenius endomorphism implies that we have an isogeny $A \sim (E_1 \times E_2)/H$ where $E_1$ is an ordinary elliptic curve and $E_2$ is a supersingular one. The rest of the statement follows naturally from the exact sequence. □

As in the previous case, the computational difficulty is finding an isogeny between $A$ and $E_1 \times E_2$; see Section 5.3.

### 5.2.3 $p$-rank-2 case

In this case, the surface $A$ decomposes over the algebraic closure as the product of two ordinary elliptic curves.

**Proposition 5.10** ([37]). *Non-simple abelian surfaces $A/\mathbb{F}_q$ of $p$-rank 2 are isomorphic to a product $E_1 \times E_2$ of two ordinary elliptic curves and their endomorphism ring is isomorphic to*

$$\begin{pmatrix} \mathrm{End}(E_1) & \mathrm{Hom}(E_2, E_1) \\ \mathrm{Hom}(E_1, E_2) & \mathrm{End}(E_2) \end{pmatrix}.$$

When $A$ is the Jacobian variety of a genus-two curve and has $p$-rank 2, it is an indecomposable variety and, therefore, admits a principal polarization different from the product one. Therefore, in this case, we have $\mathrm{Hom}(E_1, E_2) \neq 0$.

**Remark 5.11.** *Since $E_1$ and $E_2$ are ordinary, computing $\mathrm{Hom}(E_1, E_2)$ reduces to the isogeny path problem. Indeed, if $\mathrm{End}(E_1) = \mathrm{End}(E_2)$, computing $\mathrm{Hom}(E_1, E_2)$ is equivalent to computing the ideal class of the class group corresponding to isogenies from $E_1$ to $E_2$. If $\mathrm{End}(E_1) \neq \mathrm{End}(E_2)$, one would first compute vertical isogenies from each $E_i$ to an elliptic curve $E_i'$ with endomorphism ring $\mathrm{End}(E_1) + \mathrm{End}(E_2)$ and the problem is then reduced to the previous case.*

## 5.3 Computing elliptic factors

Let $A = \mathrm{Jac}(C)$ be the Jacobian variety of a genus-two curve defined over a finite field $\mathbb{F}_q$. In this section, all results are stated over the algebraic closure $\overline{\mathbb{F}}_q$ for simplicity; they can be exploited effectively by working on the base field and then extending it as necessary : as already mentioned, all endomorphisms are defined over extensions of the base field of bounded degree [62, Theorem 2.4].

When $A$ is non-simple, we look for its elliptic factors as elliptic subcovers, following the work of Kani [35, 39, 38, 36].

Suppose that $C$ admits a non-constant morphism $f : C \to E$ to an elliptic curve $E$. If $f$ does not factor over an isogeny of $E$, then we say that $f$ is an elliptic subcover of $C$. Note that this last condition imposes no essential restriction since every nonconstant $f : C \to E$ factors over a unique elliptic subcover.

A classical theorem due to Picard [57] and Bolza [9] states that a curve $C$ of genus two has either none, two or infinitely many elliptic subcovers. This is in part due to the fact that the elliptic subcovers occur in pairs: given an elliptic subcover $f : C \to E$, there is a canonical "complementary" elliptic subcover $f' : C \to E'$ of the same degree $\deg(f) = \deg(f')$ such that the induced maps on the associated Jacobian varieties fit into an exact sequence

$$0 \to \mathrm{Jac}(E) \xrightarrow{f_*} \mathrm{Jac}(C) \xrightarrow{f'_*} \mathrm{Jac}(E') \to 0.$$

**Proposition 5.12.** *Let $A$ be a non-simple Jacobian variety of dimension 2. There exists an $(n, n)$-isogeny, preserving the polarization, to a product of elliptic curves with the product polarization.*

The case in which $C$ has infinitely many elliptic subcovers happens precisely when the Jacobian of $C$ is $\overline{\mathbb{F}}_q$-isogenous to $E^2$, for some elliptic curve $E/\overline{\mathbb{F}}_q$. In particular, in the non-simple $p$-rank 1 case the eliptic curves $E_1$ and $E_2$ and the group $H$ in Proposition 5.9 are uniquely determined and the isogeny $A \to E_1 \times E_2$ is an $(n,n)$-isogeny.

### 5.3.1 Bounding the degree and the field of definition of the subcover

A bound on the degree of the isogeny may be derived from the following results.

**Theorem 5.13.** *Let $(A, \lambda_A)$ be a principally polarized abelian surface, denote by $\mathrm{NS}(A, \lambda_A)$ its Néro-Severi group and let $n$ be an integer. We have a one–to–one correspondence between*

- *the set of all elliptic subcovers $E$ of $A$ of degree $n = \deg(E)$, and*
- *the set of primitive classes $[D] \in \mathrm{NS}(A, \lambda_A)$ with invariant $\Delta(D) = n^2$*

*given by the embedding $E \to [E] \in \mathrm{NS}(A, \lambda_A)$.*

For all $D \in \mathrm{NS}(A, \lambda_A)$, set $q_{(A,\lambda_A)}(D) = (D.\lambda_A)^2 - 2(D.D)$.

**Theorem 5.14** ([38, Theorem 2])**.** *The curve $C/\overline{\mathbb{F}}_q$ has an elliptic subcover of degree $n$ if and only if the refined Humbert invariant $q_{\mathrm{Jac}(C)}$ primitively represents $n^2$.*

Kani focuses on computing $q_{\mathrm{Jac}(C)}$ given $(E, E', \deg(f))$ and on computing how many curves correspond to a given triple $(E, E', \deg(f))$. We are instead interested in the opposite direction: given $C$, compute the triples $(E, E', \deg(f))$, the Humbert invariant $q_C$ or simply bounding $\deg(f)$. Unfortunately, we are unaware of an efficient algorithm to compute $q_{\mathrm{Jac}(C)}$. See for example [41] for a discussion on how such an efficient algorithm could be use to break different isogeny based post-quantum cryptosystems.

A bound on the fields of definition follows from a bound on $\deg(f)$.

**Proposition 5.15.** *Let $C/\mathbb{F}_q$ be a genus-two curve and denote by $A = \mathrm{Jac}(C)$ its Jacobian variety. Let $\varphi : A \to B$ be a separable $(n,n)$-isogeny. Then $B$ is a principally polarized abelian variety defined over $\mathbb{F}_{q^r}$ where*

$$r = n^3 \prod_{\substack{\ell \text{ prime} \\ \ell \mid n}} \frac{1}{\ell^3}(\ell+1)(\ell^2+1)$$

*and the isogeny $\varphi$ is defined over $\mathbb{F}_{q^s}$ with $s = w\,r$ where $w = \#\,\mathrm{Aut}(C)$.*

*Proof.* The kernel of a separable $(n,n)$-isogeny is a maximal isotropic subgroup of $A[n]$, and hence $B$ is naturally equipped with a principal polarization [21, Proposition 2.1]. The value of $r$ follows from counting the number of maximal isotropic groups in $A[n]$. The value of $s$ is obtained by counting automorphisms of $A$ preserving the polarization, which is equal to $\#\,\mathrm{Aut}(C)$ because $C$ is hyperelliptic. □

**Remark 5.16.** *If $B \sim E_1 \times E_2$ with the product polarization then $E_i$ are defined over $\mathbb{F}_{q^{2r}}$.*

We now give two methods to obtain elliptic subcovers of a given Jacobian varietity of a genus-two curve.

### 5.3.2 First method: finding $(n, n)$-isogenies to a product of elliptic curves

According to Proposition 5.12, in the non-simple case there are $(n, n)$-isogenies from $A$ to a product of elliptic curves with the product polarization. Since $(n, n)$-isogenies can be computed efficiently [17, 5, 49, 15], we obtain the following algorithm.

**Algorithm 5.17** (Finding $(n, n)$-isogenies)**.**

*Input:* *A curve $C$ of genus two with non-simple Jacobian variety.*

*Output:* *An elliptic factor.*

1. *Set $n \leftarrow 2$.*
2. *Compute the torsion subgroup* $\mathrm{Jac}(C)[n]$.
3. *For all maximal isotropic subgroups of* $\mathrm{Jac}(C)[n]$*:*
4. *Compute the corresponding $(n, n)$-isogeny* $\mathrm{Jac}(C) \to B$.
5. *If $B$ splits:*
6. *Return its elliptic factor.*
7. *Set $n \leftarrow n + 1$ and go back to Step 2.*

For Step 5, see for example [16]. This algorithm terminates and a bound on its runtime may be derived from Section 5.3.1.

### 5.3.3 Second method: computing regular differentials

Let $C : y^2 = F(x)$ be a genus-two curve. Assume that there is an elliptic curve $E : v^2 = u^3 + au + b$ and a map $C \to E$ given by $(x, y) \mapsto (u, v) = (f(x, y), g(x, y)) = (f_1(x) + yf_2(x), g_1(x) + yg_2(x))$. We necessarily have $g(x, y)^2 = f(x, y)^3 + af(x, y) + b$ modulo the equation of $C$. This implies

$$\begin{cases} g_1^2 + Fg_2^2 = b + af_1 + f_1^3 + 3f_1f_2^2F, \\ 2g_1g_2 = af_2 + 3f_1^2f_2 + f_2^3F. \end{cases} \tag{1}$$

Using the ideas of [20, Section 6.2], we notice that the pushforward of a regular differential of $E$ has to be regular differential of $C$ and hence a linear combination of $\frac{dx}{y}$ and $\frac{xdx}{y}$. This gives:

$$\begin{cases} F(2f_2' + f_2) = 2g_1(\alpha x + \beta), \\ 2f_1' = 2g_2(\alpha x + \beta). \end{cases} \tag{2}$$

From which, generically, that is, if $\alpha \neq 0$, we obtain $g_2 = \frac{f_1'}{\alpha x + \beta}$ for a choice of linear factor of $f_1'$ and $g_1 = \frac{F(2f_2' + f_2)}{2(\alpha x + \beta)}$ for a choice of $f_2$ such that $\alpha x + \beta \mid F(2f_2' + f_2)$. Together with Equation (1), this implies $\deg(f_1) = \deg(f_2) + 3$, generically.

We thus obtain the following algorithm.

**Algorithm 5.18** (Exploiting regular differentials).

*Input:* *A curve $C : y^2 = F(x)$ of genus two with non-simple Jacobian variety.*

*Output:* *An elliptic factor.*

1. *Set $d \leftarrow 1$.*
2. *Let $w$ and $r$ be as in Proposition 5.15.*
3. *For all $f_1 \in \mathbb{F}_{q^{wr}}[x]$ of degree $d+3$:*
4. *For all linear factors $t$ of its derivative $f_1'$:*
5. *For all $f_2 \in \mathbb{F}_{q^{2r}}[x]$ of degree $d$ such that $t \mid F(2f_2' + f_2)$:*
6. *Let $g_1 = \frac{F(2f_2'+f_2)}{2t}$ and $g_2 = \frac{f_1'}{t}$.*
7. *If Equation (1) is satisfied, return the elliptic factor.*
8. *Set $d \leftarrow d+1$ and go back to Step 2.*

## 5.4 Supersingular case

The methods of the previous sections apply also to this case with $n = p$, the characteristic of the base field. It may however be unpractical to compute $(p, p)$-isogenies. We now provide an alternative method based on random walk techniques which may also be adapted to other settings where the isogeny graph has the rapid mixing property.

**Proposition 5.19.** *There is an algorithm that on input two supersingular elliptic curves $E_1$ and $E_2$ over $\mathbb{F}_{p^2}$ outputs a basis of* $\mathrm{End}(E_1 \times E_2)$ *in expected time* $\sqrt{p}(\log p)^{O(1)}$.

*Proof.* From [55, Theorem 8.8], there is an algorithm which finds bases of $\mathrm{End}(E_1)$ and $\mathrm{End}(E_2)$ in time $\tilde{O}(\sqrt{p})$. Within that same running time, one can compute an isogeny $\varphi : E_1 \to E_2$ of degree $2^e$ for some $e \in \mathbb{N}$ in efficient representation (see, for instance, [55, Proposition 8.7]; that is simply a baby-step giant-step resolution of the 2-isogeny path problem). We can ensure that $\varphi$ has cyclic kernel, i.e., it is a non-backtracking path in the 2-isogeny graph (by greedily pruning backtracking sub-paths).

Then, one can compute in polynomial time a basis of the ideal $I = \mathrm{Hom}(E_2, E_1) \circ \varphi \subset \mathrm{End}(E_1)$ as follows. This ideal consists in all endomorphisms $\alpha$ such that $\deg\varphi$ divides $\alpha \circ \widehat{\varphi}$, i.e. such that $(\alpha \circ \widehat{\varphi})(E_1[2^e]) = 0$. Let

$$I_i = I + 2^i \,\mathrm{End}(E_1) = \left\{\alpha \in \mathrm{End}(E_1) \mid 2^i \text{ divides } \alpha \circ \widehat{\varphi}\right\},$$

so that $I_0 = \mathrm{End}(E_1)$ and $I_e = I$. We compute $I_i$ iteratively as follows:

1. Let $I_0 = \mathrm{End}(E_1)$.
2. For each $0 \leqslant i < e$, compute $I_{i+1} = \left\{\alpha \in I_i \mid \frac{\alpha\circ\widehat{\varphi}}{2^i}(E_1[2]) = 0\right\}$, the division $\frac{\alpha\circ\widehat{\varphi}}{2^i}$ being evaluated iteratively by [48, Theorem 3].

We then have a basis of $\mathrm{Hom}(E_2, E_1) = (I \circ \widehat{\varphi})/[\deg\varphi]$. Similarly, we have a basis of $\mathrm{Hom}(E_1, E_2)$. We conclude from the fact that

$$\mathrm{End}(E_1 \times E_2) = \begin{pmatrix} \mathrm{End}(E_1) & \mathrm{Hom}(E_2, E_1) \\ \mathrm{Hom}(E_1, E_2) & \mathrm{End}(E_2) \end{pmatrix}.$$

□

**Corollary 5.20.** *Assuming that [19, Hypothesis 1] holds, there is an algorithm that on input a superspecial Jacobian $A$ over $\mathbb{F}_{p^2}$ outputs a basis of* $\mathrm{End}(A)$ *in expected time* $p(\log p)^{O(1)}$.

*Proof.* For $\ell \in \{2,3\}$, assuming that [19, Hypothesis 1] holds, there is a bound $n = O(\log(p))$ such that a random path $\varphi_\ell : A \to B_\ell$ of length $n$ in the $(\ell,\ell)$-isogeny graph reaches a target $B$ that is close to uniformly distributed in the set of superspecial abelian surfaces over $\mathbb{F}_{p^2}$. Then $B_\ell$ is a product $E_1 \times E_2$ with probability $\Omega(p^{-1})$. Therefore, one can find such isogenies $\varphi_2$ and $\varphi_3$ in time $p(\log p)^{O(1)}$ from $A$ to products of elliptic curves $B_2$ and $B_3$. One can compute $\mathrm{End}(B_\ell)$ within the claimed running time with Proposition 5.19, and, deduce $\mathrm{End}(A)$ with Proposition 5.1 □

# 6 Surfaces with extra automorphisms

When the curve $C$ admits automorphisms other than $\pm\mathrm{id}$, finding a decomposition of its Jacobian variety $\mathrm{Jac}(C)$ is easier as the following result shows.

**Theorem 6.1** ([40, Theorem B]). *Let $C$ be a curve and let $G$ be a finite subgroup of the automorphism group $\mathrm{Aut}(C)$ such that $G = H_1 \cup \cdots \cup H_n$, where the $H_i$'s are subgroups of $G$ with $H_i \cap H_j = \{\mathrm{id}\}$ for $i \neq j$. Then we have an isogeny*

$$\mathrm{Jac}(C)^{n-1} \times \mathrm{Jac}(C/G)^g \sim \mathrm{Jac}(C/H_1)^{h_1} \times \cdots \times \mathrm{Jac}(C/H_n)^{h_n}$$

*where $g = |G|$, $h_i = |H_i|$ and $C/G$, $C/H_1$,..., $C/H_n$ denote the curves obtained by quotienting $C$ by the subgroups $G, H_1, \ldots, H_n$ respectively.*

In the specific case of genus-two curves, we have the more explicit statement below.

**Theorem 6.2** ([33, Theorem 2]). *Assume that the polynomial $f(x)$ factors completely over the finite field $\mathbb{F}_q$, i.e.*

$$f(x) = c\prod_{i=1}^{6}(x - a_i)$$

*with $a_i \in \mathbb{F}_q$ and $a_i \neq a_j$ when $i \neq j$. Assume that*

$$(a_2 - a_4)(a_1 - a_6)(a_3 - a_5) = (a_2 - a_6)(a_1 - a_5)(a_3 - a_4).$$

*and set*

$$\lambda = \frac{(a_1 - a_3)(a_2 - a_4)}{(a_2 - a_3)(a_1 - a_4)}, \qquad \mu = \frac{(a_1 - a_3)(a_2 - a_5)}{(a_2 - a_3)(a_1 - a_5)}, \qquad \text{and}$$
$$\theta = c(a_2 - a_3)(a_1 - a_4)(a_1 - a_5)(a_1 - a_6).$$

*Assume moreover that there exists a square root of $\lambda(\lambda - \mu)$ in the finite field $\mathbb{F}_q$. Then the Jacobian of the hyperelliptic curve $C : y^2 = f(x)$ decomposes over $\mathbb{F}_q$ as*

$$\mathrm{Jac}(C) \sim E_+ \times E_-$$

*where $E_+$ and $E_-$ are the elliptic curves defined by the equations*

$$y^2 = \frac{\theta(1-\mu)}{1-\lambda}x(x-1)\left(x - \frac{(1-\lambda)\left(\mu - 2\lambda \pm 2\sqrt{\lambda(\lambda-\mu)}\right)}{\mu - 1}\right).$$

We now consider each specific case depending on the automorphism group type. For each such type, Table 2 gives the associated family of genus-two curves; see [14] and [8] for details.

| Aut($C$) | Family |
|---|---|
| $C_2 \times C_5$ | $y^2 = x^5 - 1$ |
| $\tilde{S}_4$ | $y^2 = x^5 - x$ |
| $2D_{12}$ | $y^2 = x^6 - 1$ |
| $D_{12}$ | $y^2 = x^6 + t x^3 + 1$ |
| $D_8$ | $y^2 = x^5 + t x^3 + x$ |
| $V_4$ | $y^2 = x^6 + t x^4 + s x^2 + 1$ |

Table 2: List of genus-two curves with extra automorphisms.

## 6.1 Automorphism groups admitting a subgroup of type $V_4$

Except for those with automorphism group $C_2 \times C_5$, all families in the table above are specializations of the family of curves

$$C_{t,s} : y^2 = x^6 + t x^4 + s x^2 + 1$$

over a finite field $\overline{\mathbb{F}}_p$ with $p$ odd. The quotient by the automorphism $(x, y) \mapsto (-x, y)$ produces the degreee-two morphism

$$\phi : \begin{cases} C_{t,s} \longrightarrow E_{t,s} : v^2 = u^3 + t u^2 + s u + 1 \\ (x, y) \longmapsto (u, v) = (x^2, y). \end{cases}$$

The complementary elliptic subcover of degree two is

$$\phi' : \begin{cases} C_{t,s} \longrightarrow E_{s,t} : v^2 = u^3 + s u^2 + t u + 1 \\ (x, y) \longmapsto (u, v) = (1/x^2, y/x^3), \end{cases}$$

which can also be described as the quotient of $C_{t,s}$ by the automorphism $(x, y) \mapsto (-x, -y)$.

These two covers produce a $(2, 2)$-isogeny

$$\Phi = \phi^* \times \phi'^* : \begin{cases} E_{t,s} \times E_{s,t} \longrightarrow \mathrm{Jac}(C_{t,s}) \\ (P - \infty, Q - \infty) \longmapsto \displaystyle\sum_{R \in \phi^{-1}(P)} R - \sum_{R \in \phi^{-1}(\infty)} R + \sum_{R \in \phi'^{-1}(Q)} R - \sum_{R \in \phi'^{-1}(\infty)} R, \end{cases}$$

whose kernel is contained in $(E_{t,s} \times E_{s,t})[2]$. Write $u^3 + t u^2 + s u + 1 = (u - \alpha_1)(u - \alpha_2)(u - \alpha_3)$. Then $u^3 + s u^2 + t u + 1 = (u - \frac{1}{\alpha_1})(u - \frac{1}{\alpha_2})(u - \frac{1}{\alpha_3})$. Set $P_i^{\pm} = (\pm\sqrt{\alpha_i}, 0)$, so that $\phi^{-1}((\alpha_i, 0)) = P_i^+ - \infty + P_i^- - \infty$. Under the usual identification of $E$ with its Jacobian variety, the kernel of $\Phi$ is

$$\{\infty \times \infty\} \cup \left\{ (\alpha_i, 0) \times \left( \frac{1}{\alpha_i}, 0 \right) : i \in \{1, 2, 3\} \right\}.$$

Indeed, we have $\Phi\left((\alpha_i, 0) \times \left(\frac{1}{\alpha_i}, 0\right)\right) = \mathrm{div}(x^2 - \alpha_i) = 0$.

**Remark 6.3.** *The elliptic curves $E_{t,s}$ and $E_{s,t}$ are in general not isogenous to each other.*

We can now use the results of Section 5.1 to determine the endomorphism ring of $\mathrm{Jac}(C)$. Consider the dual $(2,2)$-isogeny $\widehat{\Phi} : \mathrm{Jac}(C_{t,s}) \to E_{t,s} \times E_{s,t}$. It allows us to bound the endomorphism ring from above and below as follows

$$2\,\mathrm{End}\left(E_{t,s} \times E_{s,t}\right) \subset \mathrm{End}\left(\mathrm{Jac}(C_{t,s})\right) \subset \frac{1}{2}\,\mathrm{End}\left(E_{t,s} \times E_{s,t}\right)$$

where the inclusions are given by the maps:

$$\begin{cases} 2\,\mathrm{End}(E_{t,s} \times E_{s,t}) \longrightarrow \mathrm{Jac}\left(C_{t,s}\right) \\ \qquad\qquad 2\psi \longmapsto \Phi \circ \psi \circ \widehat{\Phi} \end{cases}$$

$$\begin{cases} \mathrm{End}\left(\mathrm{Jac}(C_{t,s})\right) \longrightarrow \frac{1}{2}\,\mathrm{End}\left(E_{t,s} \times E_{s,t}\right) \\ \qquad\qquad \varphi \longmapsto \frac{1}{2}\widehat{\Phi} \circ \varphi \circ \Phi \end{cases}$$

In order to finally identify $\mathrm{End}(\mathrm{Jac}(C_{t,s}))$ among orders which satisfy those bounds, we check which elements $\frac{1}{2}\psi \in \frac{1}{2}\,\mathrm{End}\left(E_{t,s} \times E_{s,t}\right)$ can be written as $\frac{1}{2}\widehat{\Phi} \circ \varphi \circ \Phi$, that is, when $\psi = \widehat{\Phi} \circ \varphi \circ \Phi$.

## 6.2 Automorphism type $C_2 \times C_5$

To conclude this section, we focus on the remaining case of the curve $C : y^2 = x^5 - 1$ defined over a finite field $\mathbb{F}_p$ with $p \neq 2, 5$.

We clearly have the inclusion $\mathbb{Z}[\zeta_5] \subset \mathrm{End}(\mathrm{Jac}(C))$. In the simple case, that is, when $p$ is totally split in $\mathbb{Z}[\zeta_5]$, this is an equality. In the non-simple case, we can use the results of Section 5.1 since thanks to [72, Theorem 1.2] we do know the $p$-rank and the $a$-number of the Jacobian variety.

# References


[1] Leonard Max Adleman and Ming-Deh A. Huang. *Primality testing and abelian varieties over finite fields*. Volume 1512. Lecture Notes in Mathematics. Springer, 1992. ISBN: 3-540-55308-8. DOI: 10.1007/BFb0090185. URL: https://doi.org/10.1007/BFb0090185.

[2] Daniel Julius Bernstein, Luca De Feo, Antonin Leroux, and Benjamin Smith. "Faster computation of isogenies of large prime degree." In: *Proceedings of the Fourteenth Algorithmic Number Theory Symposium*. Volume 4. The Open Book Series. Mathematical Sciences Publishers, 2020, pages 39–55. DOI: 10.2140/obs.2020.4.39.

[3] Gaetan Bisson. "Computing endomorphism rings of abelian varieties of dimension two." In: *Mathematics of Computation* 84.294 (2015), pages 1977–1989. DOI: 10.1090/S0025-5718-2015-02938-X.

[4] Gaetan Bisson. "Computing endomorphism rings of elliptic curves under the GRH." In: *Journal of Mathematical Cryptology* 5.2 (2012), pages 101–113. DOI: 10.1515/jmc.2011.008.

[5] Gaetan Bisson, Romain Cosset, and Damien Robert. *AVIsogenies*. A library for computing isogenies between abelian varieties. Registered software IDDN.FR.001.440011.000.R.P.2010.000.10000. 2010. URL: https://www.math.u-bordeaux.fr/~damienrobert/avisogenies/.

[6] Gaetan Bisson and Marco Streng. "On polarised class groups of orders in quartic CM-fields." In: *Mathematical Research Letters* 24.2 (2017), pages 247–270. DOI: 10.4310/MRL.2017.v24.n2.a1.

[7] Gaetan Bisson and Andrew Victor Sutherland. "Computing the endomorphism ring of an ordinary elliptic curve over a finite field." In: *Journal of Number Theory* 131.5 (2011): *Elliptic Curve Cryptography*. Edited by Neal I. Koblitz and Victor S. Miller, pages 815–831. DOI: 10.1016/j.jnt.2009.11.003.

[8] Oskar Bolza. "On binary sextics with linear transformations into themselves." In: *American Journal of Mathematics* 10.1 (1887), pages 47–70. ISSN: 0002-9327. DOI: 10.2307/2369402.

[9] Oskar Bolza. "Zur Reduction hyperelliptischer Integrale erster Ordnung auf elliptische mittels einer Transformation dritten Grades." In: *Mathematische Annalen* 50 (1898), pages 314–324. ISSN: 0025-5831. DOI: 10.1007/BF01448072.

[10] Reinier Bröker, Kristin Estella Lauter, and Andrew Victor Sutherland. "Modular polynomials via isogeny volcanoes." In: *Mathematics of Computation* 81.278 (2012), pages 1201–1231. DOI: 10.1090/S0025-5718-2011-02508-1.

[11] Ernest Hunter Brooks, Dimitar Jetchev, and Benjamin Wesolowski. "Isogeny graphs of ordinary abelian varieties." In: *Research in Number Theory* 3.28 (2017). DOI: 10.1007/s40993-017-0087-5.

[12] Nils Bruin, Jeroen Sijsling, and Alexandre Zotine. "Numerical computation of endomorphism rings of Jacobians." In: The Open Book Series 2.1 (2019). Edited by Renate Scheidler and Jonathan Sorenson, pages 155–171. DOI: 10.2140/obs.2019.2.155.

[13] David Geoffrey Cantor. "Computing in the Jacobian of a hyperelliptic curve." In: *Mathematics of Computation* 48.177 (1987), pages 95–101. DOI: 10.1090/S0025-5718-1987-0866101-0.

[14] Gabriel Cardona and Jordi Quer. "Field of moduli and field of definition for curves of genus 2." In: *Computational Aspects of Algebraic Curves*. Volume 13. Lecture Notes Series on Computing. World Scientific Publishing, 2005, pages 71–83. DOI: 10.1142/9789812701640_0006.

[15] Wouter Castryck and Thomas Decru. "Multiradical isogenies." In: *Arithmetic, geometry, cryptography, and coding theory 2021*. Volume 779. Contemporary Mathematics. American Mathematical Society, 2022, pages 57–89. DOI: 10.1090/conm/779/15671.

[16] Maria Corte-Real Santos, Craig Costello, and Sam Frengley. "An algorithm for efficient detection of $(N, N)$-splittings and its application to the isogeny problem in dimension 2." In: *Public-Key Cryptography – PKC 2024*. Edited by Qiang Tang and Vanessa Teague. 2024, pages 157–189. ISBN: 978-3-031-57725-3. DOI: 10.1007/978-3-031-57725-3_6.

[17] Romain Cosset and Damien Robert. "Computing $(\ell, \ell)$-isogenies in polynomial time on Jacobians of genus 2 curves." In: *Mathematics of Computation* 84 (2015), pages 1953–1975. DOI: 10.1090/S0025-5718-2014-02899-8.

[18] Edgar Costa, Nicolas Mascot, Jeroen Sijsling, and John Voight. "Rigorous computation of the endomorphism ring of a Jacobian." In: *Mathematics of Computation* 88.317 (2019), pages 1303–1339. ISSN: 0025-5718. DOI: 10.1090/mcom/3373.

[19] Craig Costello and Benjamin Smith. "The supersingular isogeny problem in genus 2 and beyond." In: *Post-quantum cryptography*. Volume 12100. Lecture Notes in Computer Science. Springer, Cham, 2020, pages 151–168. DOI: 10.1007/978-3-030-44223-1_9.

[20] Jean-Marc Couveignes and Tony Ezome. "Computing functions on Jacobians and their quotients." In: *LMS Journal of Computation and Mathematics* 18.1 (2015), pages 555–577. DOI: 10.1112/S1461157015000169.

[21] Igor Dolgachev and David Lehavi. "On isogenous principally polarized abelian surfaces." In: *Curves and abelian varieties*. Volume 465. Contemporary Mathematics. American Mathematical Society, 2008, pages 51–69. ISBN: 978-0-8218-4334-5. DOI: 10.1090/conm/465/09100.

[22] Kirsten Eisenträger, Sean Hallgren, Chris Leonardi, Travis Morrison, and Jennifer Park. "Computing endomorphism rings of supersingular elliptic curves and connections to path-finding in isogeny graphs." In: *ANTS XIV—Proceedings of the Fourteenth Algorithmic Number Theory Symposium*. Volume 4. Open Book Ser. Math. Sci. Publ., Berkeley, CA, 2020, pages 215–232. DOI: 10.2140/obs.2020.4.215.

[23] Kirsten Eisenträger and Kristin Estella Lauter. "A CRT algorithm for constructing genus 2 curves over finite fields." In: *Arithmetic, Geometry and Coding Theory — AGCT 2010*. Edited by François Rodier and Serge Vladut. Volume 21. Séminaires et Congrès. Société Mathématique de France, 2009, pages 161–176.

[24] Arsen Elkin and Rachel Pries. "Hyperelliptic curves with $a$-number 1 in small characteristic." In: *Albanian Journal of Mathematics* 1.4 (2007), pages 245–252. ISSN: 1930-1235.

[25] Claus Fieker, Tommy Hofmann, and Sogo Pierre Sanon. "On the computation of the endomrophism rings of abelian surfaces." In: *Journal of Number Theory* 229 (221), pages 39–52. DOI: 10.1016/j.jnt.2021.04.024.

[26] Jenny Fuselier, Annamaria Iezzi, Mark Kozek, Travis Morrison, and Changningphaabi Namoijam. "Computing supersingular endomorphism rings using inseparable endomorphisms." In: *Journal of Algebra* 668 (2025), pages 145–189. ISSN: 0021-8693. DOI: https://doi.org/10.1016/j.jalgebra.2025.01.012.

[27] Steven D. Galbraith. "Constructing isogenies between elliptic curves over finite fields." In: *JMS Journal of Computation and Mathematics* 2 (1999), pages 118–138. DOI: 10.1112/S1461157000000097.

[28] Darren Glass and Rachel Pries. "Hyperelliptic curves with prescribed $p$-torsion." In: *Manuscripta Mathematica* 117.3 (2005), pages 299–317. ISSN: 0025-2611. DOI: 10.1007/s00229-005-0559-0.

[29] Eyal Zvi Goren and Kristin Estella Lauter. "Genus 2 curves with complex multiplication." In: *International Mathematics Research Notices* 5 (2012), pages 1068–1142. ISSN: 1073-7928. DOI: 10.1093/imrn/rnr052.

[30] Everett William Howe, Daniel Maisner, Enric Nart, and Christophe Ritzenthaler. "Principally polarizable isogeny classes of abelian surfaces over finite fields." In: *Mathematical Research Letters* 15.1 (2008), pages 121–127. ISSN: 1073-2780. DOI: 10.4310/MRL.2008.v15.n1.a11.

[31] Everett William Howe, Enric Nart, and Christophe Ritzenthaler. "Jacobians in isogeny classes of abelian surfaces over finite fields." In: *Annales de l'Institut Fourier* 59.1 (2009), pages 239–289. DOI: 10.5802/aif.2430.

[32] Everett William Howe and Hui June Zhu. "On the Existence of Absolutely Simple Abelian Varieties of a Given Dimension over an Arbitrary Field." In: *Journal of Number Theory* 92.1 (2002), pages 139–163. DOI: 10.1006/jnth.2001.2697.

[33] Annamaria Iezzi, Motoko Qiu Kawakita, and Marco Timpanella. "New sextics of genus 6 and 10 attaining the Serre bound." In: *Advances in Geometry* 24.1 (2024), pages 99–109. ISSN: 1615-715X,1615-7168. DOI: 10.1515/advgeom-2023-0031.

[34] David Jao, Stephen David Miller, and Ramarathnam Venkatesan. "Do All Elliptic Curves of the Same Order Have the Same Difficulty of Discrete Log?" In: *Advances in Cryptology - ASIACRYPT 2005*. Edited by Bimal Roy. Volume 3788. Lecture Notes in Computer Science. Springer, 2005, pages 21–40. DOI: 10.1007/11593447_2.

[35] Ernst Kani. "Elliptic curves on abelian surfaces." In: *Manuscripta Mathematica* 84.2 (1994), pages 199–223. ISSN: 0025-2611. DOI: 10.1007/BF02567454.

[36] Ernst Kani. "Elliptic subcovers of a curve of genus 2. I. The isogeny defect." In: *Annales Mathématiques du Québec* 43.2 (2019), pages 281–303. ISSN: 2195-4755. DOI: 10.1007/s40316-018-0105-6.

[37] Ernst Kani. "Products of CM elliptic curves." In: *Collectanea Mathematica* 62.3 (2011), pages 297–339. DOI: 10.1007/s13348-010-0029-1.

[38] Ernst Kani. "The moduli spaces of Jacobians isomorphic to a product of two elliptic curves." In: *Collectanea Mathematica* 67.1 (2016), pages 21–54. ISSN: 0010-0757. DOI: 10.1007/s13348-015-0148-9.

[39] Ernst Kani. "The number of curves of genus two with elliptic differentials." In: *Journal für die Reine und Angewandte Mathematik* 485 (1997), pages 93–121. ISSN: 0075-4102. DOI: 10.1515/crll.1997.485.93.

[40] Ernst Kani and Michael Rosen. "Idempotent relations and factors of Jacobians." In: *Mathematische Annalen* 284.2 (1989), pages 307–327. ISSN: 0025-5831. DOI: 10.1007/BF01442878.

[41] Eda Kırımlı and Chloe Martindale. "The computational refined Humbert invariant problem is equivalent to the computational isogeny problem." Preprint. 2025.

[42] David Russell Kohel. "Endomorphism rings of elliptic curves over finite fields." PhD thesis. University of California at Berkeley, 1996. URL: http://iml.univ-mrs.fr/~kohel/pub/thesis.pdf.

[43] The LMFDB Collaboration. *The L-functions and modular forms database*. http://www.lmfdb.org. 2025.

[44] Davide Lombardo. "Computing the geometric endomorphism ring of a genus-2 Jacobian." In: *Mathematics of Computation* 88.316 (2019), pages 889–929. ISSN: 0025-5718. DOI: 10.1090/mcom/3358.

[45] Jonathan Lubin, Jean-Pierre Serre, and John Tate. "Elliptic curves and formal groups." In: *Lecture notes prepared in connection with the seminars held at the Summer Institute on Algebraic Geometry held at the Whitney Estate, Woods Hole, Massachussets, July 6 – July 31* (1964).

[46] Abdoulaye Maiga and Damien Robert. "Computing the 2-adic Canonical Lift of Genus 2 Curves." In: *ICMC 2021 - 7th International Conference on Mathematics and Computing*. Indian Institute of Engineering Science and Technology. Shibpur / Virtual, India, Mar. 2021. URL: https://hal.inria.fr/hal-03119147.

[47] Daniel Maisner and Enric Nart. "Abelian Surfaces over Finite Fields as Jacobians." In: *Experimental Mathematics* 11.3 (2002), pages 321–337.

[48] Arthur Herlédan Le Merdy and Benjamin Wesolowski. *The supersingular endomorphism ring problem given one endomorphism*. Cryptology ePrint Archive, Paper 2023/1448. https://eprint.iacr.org/2023/1448. 2023.

[49] Enea Milio. "Computing isogenies between Jacobians of curves of genus 2 and 3." In: *Mathematics of Computation* 89.323 (2020), pages 1331–1364. ISSN: 0025-5718. DOI: 10.1090/mcom/3486.

[50] David Mumford. *Tata Lectures on Theta, II*. Volume 43. Progress in Mathematics. Birkhäuser, 1984. ISBN: 3764331100.

[51] Laura Hitt O'Connor, Gary McGuire, Michael Naehrig, and Marco Streng. "A CM construction for curves of genus 2 with p-rank 1." In: *Journal of Number Theory* 131.5 (2011), pages 920–935. DOI: 10.1016/j.jnt.2010.05.002.

[52] Frans Oort. "Lifting an endomorphism of an elliptic curve to characteristic zero." In: *Indagationes Mathematicae* 76.5 (1973), pages 466–470. DOI: 10.1016/1385-7258(73)90071-1.

[53] Frans Oort. "Subvarieties of moduli spaces." In: *Inventiones Mathematicae* 24 (1974), pages 95–119. ISSN: 0020-9910. DOI: 10.1007/BF01404301.

[54] Frans Oort. "Which abelian surfaces are products of elliptic curves?" In: *Mathematische Annalen* 214 (1975), pages 35–47. ISSN: 0025-5831. DOI: 10.1007/BF01428253.

[55] Aurel Page and Benjamin Wesolowski. "The Supersingular Endomorphism Ring and One Endomorphism Problems are Equivalent." In: *Advances in Cryptology – EUROCRYPT 2024*. Edited by Marc Joye and Gregor Leander. Cham: Springer Nature Switzerland, 2024, pages 388–417.

[56] Christophe Petit and Kristin Estella Lauter. *Hard and Easy Problems for Supersingular Isogeny Graphs*. IACR Cryptology ePrint Archive, Report 2017/962. https://eprint.iacr.org/2017/962. 2017.

[57] Émile Picard. "Sur la réduction du nombre des périodes des intégrales abéliennes et, en particulier, dans le cas des courbes du second genre." In: *Bulletin de la Société Mathématique de France* 11 (1883), pages 25–53. ISSN: 0037-9484. URL: http://www.numdam.org/item?id=BSMF_1883__11__25_1.

[58] Damien Robert. *Some applications of higher dimensional isogenies to elliptic curves*. 2022. iacr: 2022/1704.

[59] Damien Robert and Abdoulaye Maiga. "Computing the Canonical Lift of Genus 2 Curves in Odd Characteristics." working paper or preprint. July 2022. URL: https://hal.archives-ouvertes.fr/hal-03738314.

[60] Damien Robert and Abdoulaye Maiga. "Towards computing canonical lifts of ordinary elliptic curves in medium characteristic." working paper or preprint. 2022. URL: https://hal.science/hal-03702658/.

[61] Goro Shimura and Yutaka Taniyama. *Complex multiplication of abelian varieties and its applications to number theory*. Volume 6. Publications of the Mathematical Society of Japan. The Mathematical Society of Japan, 1961.

[62] Alice Silverberg. "Fields of definition for homomorphisms of abelian varieties." In: *Journal of Pure and Applied Algebra* 77.3 (1992), pages 253–262. DOI: 10.1016/0022-4049(92)90141-2.

[63] Caleb Springer. "Computing the endomorphism ring of an ordinary abelian surface over a finite field." In: *Journal of Number Theory* 202 (2019), pages 430–457. DOI: 10.1016/j.jnt.2019.01.013.

[64] Andrew Victor Sutherland. "Computing Hilbert class polynomials with the Chinese remainder theorem." In: *Mathematics of Computation* 80.273 (2011), pages 501–538. DOI: 10.1090/S0025-5718-2010-02373-7.

[65] Andrew Victor Sutherland. "On the evaluation of modular polynomials." In: *Algorithmic Number Theory Symposium — ANTS-X*. Edited by Everett William Howe and Kiran Sridhara Kedlaya. Volume 1. The Open Book Series 1. Mathematical Sciences Publishers, 2013, pages 531–555. DOI: 10.2140/obs.2013.1.531.

[66] John Torrence Tate. "Endomorphisms of abelian varieties over finite fields." In: *Inventiones mathematicae* 2.2 (1966), pages 134–144. DOI: 10.1007/BF01404549.

[67] Jacques Vélu. "Isogénies entre courbes elliptiques." In: *Comptes Rendus de l'Académie des Sciences de Paris*. A 273 (1971), pages 238–241.

[68] William Charles Waterhouse. "Abelian varieties over finite fields." In: *Annales Scientifiques de l'École Normale Supérieure* 2.4 (1969), pages 521–560.

[69] André Weil. "Zum Beweis des Torellischen Satzes." In: *Nachrichten der Akademie der Wissenschaften in Göttingen, Mathematisch-Physikalische Klasse* 1.IIa (1957), pages 33–53.

[70] Benjamin Wesolowski. "Random Walks in Number-Theoretic Cryptology." Habilitation à diriger les recherches. École Normale Supérieure de Lyon, 2024. URL: https://www.bweso.com/hdr.pdf.

[71] Benjamin Wesolowski. "The supersingular isogeny path and endomorphism ring problems are equivalent." In: *FOCS 2021 – 62nd Annual IEEE Symposium on Foundations of Computer Science*. IEEE, 2021, pages 1100–1111. DOI: 10.1109/FOCS52979.2021.00109.

[72] Alexey Zaytsev. "Generalization of Deuring reduction theorem." In: *Journal of Algebra* 392 (2013), pages 97–114. ISSN: 0021-8693. DOI: 10.1016/j.jalgebra.2013.06.017.