EQUIVALENT COMPUTATIONAL PROBLEMS FOR SUPERSPECIAL ABELIAN SURFACES

MICKAËL MONTESSINOS

ABSTRACT. We show reductions and equivalences between various problems related to the computation of the endomorphism ring of principally polarised superspecial abelian surfaces. Problems considered are the computation of the Ibukiyama-Katsura-Oort matrix and computation of unpolarised isomoprhisms between superspecial abelian surfaces.

1. INTRODUCTION

The problem of computing the endomorphism ring of a supersingular elliptic over a finite field has been well studied in recent years. It was proven equivalent to the Isogeny Path Problem and the One Isogeny Problem [16]. In particular, the hardness of the endomorphism ring computation underlies the security of most one-dimensional isogeny-based cryptographic protocols.

The precise statement of the problem depends on the choice of representation for the endomorphism ring of a supersingular elliptic curve. Essentially, one may either wish to know an efficient algorithm to evaluate 4 endomorphisms which form a $\mathbb{Z}$-basis of the endomorphism ring, or to know the basis of a maximal order in the quaternion $\mathbb{Q}$-algebra $B_{p,\infty}$ which ramifies at the prime p, the characteristic of the base field of the curve. The two forms of the problem were proved to be equivalent, first heuristically [7], then unconditionally under GRH [26] and finally unconditionally [16].

The main tool appearing in reductions from most problems underlying the security of isogeny-based schemes is the so-called KLPT algorithm. Its original version was published in [14], and relied on specific conditions regarding the characteristic of the base field of the elliptic curves involved, as well as some heuristic considerations. Several subsequent works improved both the performance and the assumptions of the algorithm, and a general version relying only on GRH was given in [26]. This algorithm uses quaternion arithmetic to compute an isogeny of power-smooth degree between elliptic curves with known endomorphism rings. We note however that the more recent results from [16] overcome the reliance on GRH by circumnavigating the need for using KLPT.

In recent years, applications of the algorithmic theory of principally polarised superspecial abelian varieties of dimension greater than one has emerged, both regarding the construction of cryptographic schemes [4] and the cryptanalysis of

schemes using supersingular elliptic curves [2, 15, 22]. As in the case of one di-
mensional protocols, most security assumptions rely on the difficulty of computing
polarised isogenies between principally polarised superspecial abelian surfaces (PP-
SAS). As for maximal quaternion orders, a KLPT^2 algorithm working over hermitian
matrices in $M_2(B_{p,\infty})$ and allowing for the computation of polarised isogenies of
power-smooth degrees between surfaces was given in [3].

In the higher dimensional case, since all unpolarised superspecial abelian vari-
eties are isomorphic, their endomorphisms rings are as well. In fact, they are all
isomorphic to the ring $M_2(O)$, where O is any maximal order in the quaternion al-
gebra $B_{p,\infty}$. The input to the KLPT^2 algorithm is therefore not a characterisation
of the endomorphism ring, but rather the data of a certain Hermitian matrix in
$M_2(O)$, which we call the Ibukiyama-Katsura-Oort matrix, for reasons that will be
made clear in Section 2.

Much like in the one dimensional case, a question naturally arises of what the var-
ious alternative computational representations of a usable "known endomorphism
ring" are, and of their equivalences. The knowledge the Ibukiyama-Katsura-Oort
matrix of a principally polarised superspecial abelian surface is analogous to the
knowledge of a maximal quaternion order isomorphic to the endomorphism ring of
a curve, in the sense that it is the input to the relevant KLPT^2 algorithm. Another
possible representation is the knowledge of efficient algorithms representing 16 en-
domorphisms of an abelian variety A which form a basis of the endomorphism ring.
If the variety A is represented as either a product of elliptic curves or the Jacobian
of a hyperelliptic curve of genus 2, one may hope that an efficient representation of
these endomorphisms be enough to compute their image by the Rosati involution
related to the principal polarisation implied by the representation of A.

Another problem to consider is that of the computation of an unpolarised iso-
moprhism between two PPSAS. It is known that the restriction of this problem to
PPSAS presented as products of supersingular elliptic curves may be solved when
the endomorphism rings of the curves are known [9]. This problem is also a natural
candidate for equivalence to the computation of the Ibukiyama-Katsura-Oort ma-
trix of a PPSAS: one may recover the endomorphisms of the factors of a product
surface from the Ibukiyama-Katsura-Oort matrix, and then compute isomorphisms
to other products. Conversely, computing an unpolarised isomorphism from a vari-
ety A to a reference surface A_0 may allow to recover the Ibukiyama-Katsura-Oort
matrix.

Finally, one may fix a supersingular curve E_0 with known endomorphism ring O_0,
and consider the structure of the Hermitian left O_0-module $\mathrm{Hom}(A, E_0$ associated
to a PPSAS [23]. We do not consider this problem in this work, but it is the object
of [20].

1.1. **Our contributions.** Let A be a PPSAS. If A is presented as a product of
supersingular elliptic curves, we prove that the following problems are equivalent
under GRH and the assumptions necessary to use the KLPT^2 algorithm:

- Computing the Ibukiyama-Katsura-Oort matrix of A;
- Computing an effective representation of endomorphisms of A that form a
  basis of $\mathrm{End}(A)$ as a $\mathbb{Z}$-module;
- Computing an unpolarised isomorphism from E_0^2 (or any product of curves
  with known endomorphism rings) to A

If A is presented as the Jacobian surface of a genus 2 hyperelliptic curve instead, we prove that the problem of computing the Ibukiyama-Kastura-Oort matrix of A is equivalent to the problem of computing a so-called good representation of its endomorphism ring, which contains effective representations of endomorphisms of A as above, but also some additional information. We also prove that the problems of computing an effective representation of the endomorphism ring of A and computing an unpolarised isomorphism to any other PPSAS with known Ibukiyama-Katsura-Oort matrix both reduce to the computation of the Ibukiyama-Katsura-Oort matrix of A.

Theses results are stated formally as Theorem 3.5, and a diagram presenting the various reductions is given there.

It should be noted that, albeit polynomial, the reduction from computing the Ibukiyama-Katsura-Oort matrix of a variety from its endomorphism ring with additional information is not practical. Indeed, the algorithm for computing an isomorphism between the endomorphism algebra $\text{End}(A) otimes \mathbb{Q}$ and $M_2(B_{p,\infty})$ has a very large constant part in its complexity.

We provide an implementation of the algorithm from Lemma 5.1 at the following address:

https://gitlab.com/Mickanos/isomorphisms-to-superspecial-jacobians

1.2. **Methods.** The two main technical contributions of this work are the reduction from computing unpolarised isomorphisms to computing Ibukiyama-Katsura-Oort matrices, and from computing Ibukiyama-Katsura-Oort matrices to computing the endomorphism ring of a PPSAS and some additional information.

The problem of computing unpolarised isomorphisms between products of supersingular elliptic curves knowing their endomorphism rings being solved, it is enough to provide an algorithm which, given a superspecial Jacobian surface and its Ibukiyama-Katsura-Oort matrix, compute an isomorphism to any product of elliptic curves, together with their endomorphism rings.

This is done by first computing a chain of $(2,2)$-isogenies from a square E_0^2, where E_0 is a curve with known endomorphism ring. Then, given the kernel K of a $(2,2)$ isogeny $E_1 \times E_2 \to J(C)$, one computes an unpolarised automorphism of $E_1 \times E_2$ which sends K to a group K' which is the kernel of a pair of parallel 2-isogenies going respectively from E_1 and E_2 to some curves E_3 and E_4. One then recovers an isomorphism from $E_3 \times E_4$ to $J(C)$ by completing a square diagram.

Considering a PPSAS A with a known basis of endomorphisms, and the data of the action of these endomorphisms on the space of global differentials, as well as the matrix of the Rosati involution with respect to that basis, a natural strategy for recovering the Ibukiyama-Katsura-Oort matrix is to compute an isomorphism $\theta : \text{End}(A) \otimes \mathbb{Q} \to \text{End}(E_0^2) \otimes \mathbb{Q}$, where E_0 is the base curve of the Ibukiyama-Katsura-Oort correspondence, and then carry the Rosati involution through that isomorphism. One then finds an element $\gamma \in \text{End}(E_0^2)$ such that $\gamma \iota(\text{End}(A))\gamma^{-2} = \text{End}(E_0^2)$ and carries over the Rosati involution of $\text{End}(A)$ first through ι and then conjugates it by γ as well.

This strategy fails to account for the existence of automorphisms of $\text{End}(A)$ which are not induced by an automorphism of A, as then the isomorphism that was constructed from $\text{End}(A)$ to $\text{End}(E_0^2)$ may itself not be induced by an unpolarise disomorphism from A to E_0^2. Whether a given isomorphism of endomorphism rings

is as above can be detected by checking the effect of endomorphisms on global differentials, and then corrected by post-composing another such "faulty" automorphism of E_0^2 if necessary.

1.3. **Concurrent works.**
- The problem of computing unpolarised isomorphisms between products of supersingular elliptic curves is treated in [9]. It is proved that this problem reduces to computing the endomorphism rings of all curves involved.
- Computations equivalent to the computation of the Ibukiyama-Katsura-Oort matrix of a PPSAS are discussed in [20], where more emphasis is put on the Hermitian module $\mathrm{Hom}(A, E_0)$ associated to a PPSAS A. In contrast, this last work does not show an equivalence between the computation of the Ibukiyama-Katsura-Oort matrix of a PPSAS and the computation of its endomorphism ring, eithe in good or effective representation.

1.4. **Structure of this work.** The remainder of this article is organised in the following way:
- Section 2 recalls the definitions of the main concepts that we use, states some known results and show a few general lemmas necessary to our results.
- Section 3 states the various computational problems that we consider, as well as our main result, Theorem 3.5, which gives the relationship between these problems.
- Section 4 shows reduction of the computation of the endomorphism ring of a PPSAS to various problems.
- Section 5 completes the work of [9] in showing that the computation of unpolarised isomorphisms between PPSAS reduces to the computation of their Ibukiyama-Katsura-Oort matrices.
- Section 6 shows that the computation of the Ibukiyama-Katsura-Oort matrix reduces to the computation of a good representation of the ring of endomorphisms.

1.5. **Open problems.** The situation we paint in this work is somewhat neater when we restrict to products of supersingular elliptic curves. This is due to the existence of strong results for supersingular elliptic curves, which we are able to take advantage of when working with a product. In contrast, we do not prove that all the computational problems considered are equivalent when Jacobian surfaces are included.

We leave to future work the consideration of how more appropriate representations of maps from a Jacobian variety may allow to complete our equivalence diagram.

1.6. **Notations.** We let p be an odd prime number and $q = p^2$, and we fix the finite field $k = \mathbb{F}_q$. Unless stated otherwise, every variety that we consider is defined over k. We assume that p is so that the KLPT^2 algorithm may be used. The current state of the art exposed in [3] is stated with the hypothesis that $p = 3 \mod 4$, although it is suggested that any p such that there is a maximal order O_0 of the quaternion algebra $B_{p,\infty}$ with discriminant p which contains a quadratic order with very small discriminant.

We also adopt some notations related to the context of KLPT^2: we fix a supersingular elliptic curve E_0/k with known endomorphism ring, for instance E_0 :

$y^2 = x^3 + x$ if it is assumed that $p = 3 \mod 4$. Then, we let O_0 be the usual maximal order of $B_{p,\infty}$ isomorphic to $\text{End}(O_0)$. We set $A_0 = E_0^2$, and identify the maximal order $M_2(O_0)$ of $M_2(B_{p,\infty})$ in the natural way from the identification of O_0 as $\text{End}(E_0)$.

If $M \in M_2(B_{p,\infty})$, we write M^* for the conjugate transpose, where the conjugation is the special involution of the quaternion algebra $B_{p,\infty}$.

Throughout this work, we refer to "the assumptions for applying the KLPT^2 algorithm". This is phrased in anticipation of future works providing a relaxation of the assumptions and heuristics from [3]. We state the assumption of the generalised Riemann hypothesis separately, as it is also a condition for applying the KLPT algorithm, although it seems unlikely that an unconditional version of KLPT^2 would appear before an undoncitional version of KLPT.

2. Preliminaries

2.1. Principally polarised superspecial abelian surfaces.

2.1.1. *Polarisations and the Rosati involution.* We briefly recall here the basic definitions and results of the theory of polarisations of abelian varieties. We direct the reader to [6, 17] for a more detailed exposition.

Let A be an abelian variety, then there exists a variety $\widehat{A}$ $\widehat{A}(k) \simeq \text{Pic}^0(A)$. An isogeny $f \colon A \to A'$ admits a dual isogeny $\widehat{A'} \to \widehat{A}$ induced by the pullback operation f^* on divisors of A'.

Definition 2.1. A *polarisation* on A is an isogeny $\lambda \colon A \to \widehat{A}$ for which there exists an ample divisor D on $A_{\overline{k}}$ such that $\lambda(P) = [t_{-P}(D) - D]$.

The *degree* of a polarisation is its degree as an isogeny. A *principal polarisation* is a polarisation of degree 1, and therefore an isomorphism.

A *(principally) polarised abelian variety* is the data (A, λ) of an abelian variety A together with a (principal) polarisation λ on A.

We next define the condition for an isogeny to be a morphism between polarised abelian varieties:

Definition 2.2. Let (A, λ) and (A', λ') be polarised abelian varieties. An isogeny $f \colon A \to A'$ is *polarised* if the following equation holds for some $N \in \mathbb{Z}$:

$$\widehat{\varphi} \circ \lambda' \circ \varphi = [N]_{\widehat{A}} \circ \lambda.$$

Two polarisations λ, λ' on an abelian variety A are *equivalent* if there is a polarised isomorphism from (A, λ) to (A, λ').

The choice of a polarisation on A is reflected on the ring $\text{End}(A)$ by the corresponding Rosati involution. While the Rosati involution is defined over $\text{End}(A) \otimes \mathbb{Q}$ for any polarisation, we shall only need the notion for principal polarisations:

Definition 2.3. Let (A, λ_A) and (B, λ_B) be principally polarised abelian varieties. Let $\varphi \colon A \to B$ be a homomorphism of algebraic groups. Then, we set

$$r_{\lambda_A, \lambda_B} \colon \quad \text{Hom}(A, B) \quad \to \quad \text{Hom}(A, B)$$
$$f \quad \mapsto \quad \lambda_A^{-1} \circ \widehat{f} \circ \lambda_B.$$

In particular, if $A = B$ and $\lambda_A = \lambda_B = \lambda$, we write $r_\lambda = r_{\lambda_A,\lambda_B}$. In this case, the map r_λ is the well known *Rosati involution* on $\mathrm{End}(A)$.

If (A, λ) is a principally polarised abelian variety and the polarisation is clear from contex, we also write r_A for the Rosati involution on $\mathrm{End}(A)$. Then, it is well known that and a fundamental fact that the bilinear map

$$\begin{array}{ccc} \mathrm{End}(A) \times \mathrm{End}(A) & \to & \mathbb{Z} \\ (f, g) & \mapsto & \langle f, g \rangle := \mathrm{Tr}(f \circ r_A(g)) \end{array}$$

is positive definite. [17, Theorem 17.3]

Example 2.4. We give some examples of abelian varieties with canonical principal polarisations:

- An elliptic curve E has a canonical principal polarisation with ample divisor $[O]$, the (arbitrarily chosen) neutral element. Concretely, it is given by the identification $P \mapsto [P-O]$, which is often used to define the group law on E. The corresponding Rosati involution then simply sends an endomorphism f to its traditionally defined dual $\widehat{f}$.
- A product of elliptic curves $E_1 \times \cdots \times E_n$ admits a canonical polarisation, which is the product of the canonical polarisations of the E_i. Its ample divisor is then $\sum_{i=1}^n E_1 \times \cdots \times E_{i-1} \times \{\infty_i\} \times E_{i+1} \times \cdots \times E_n$.
- The Jacobian variety of an algebraic curve admits a natural principal polarisation. If C is an algebraic curve of genus 2 and $\infty \in C$ is a fixed point, there is an injective map $u \colon C \to J(C)$ sending a point P to $[P-\infty]$. Then, $u(C)$ is an ample divisor of $J(C)$ which defines the canonical polarisation.

2.1.2. *Superspecial abelian varieties.* Superspecial abelian varieties come as one of the possible generalisations of supersingular elliptic curves to larger dimension.

Definition 2.5. An abelian variety A is superspecial if there is a supersingular elliptic curve E and $g \in \mathbb{N}$ such that $A_{\overline{k}} \simeq E_{\overline{k}}^g$.

A well known result by Deligne, Ogus and Shioda states that all superspecial abelian variety of equal dimension are isomorphic over k.

In fact, we may choose our models so that an even stronger statement is true:

Definition 2.6. An abelian variety is called *maximal* if $\#A(k) = (p+1)^{2\dim A}$.

Proposition 2.7. [13, Section 5] *Let A be a maximal abelian variety. Then, we have the following:*

(1) *A is superspecial;*
(2) *If E is a maximal elliptic curve, there is a k-rational isomorphism from A to $E^{\dim A}$;*
(3) *If B is another maximal abelian variety of same dimension, A is isomorphic to B, and any homomorphism $A_{\overline{k}} \to B_{\overline{k}}$ is the base extension of a homomorphism $A \to B$.*

Furthermore, every superspecial abelian variety defined over $\overline{k}$ admits a maximal model defined over k.

We state a well known classifying result on principally polarised superspecial abelian surfaces.

Lemma 2.8. *Let A be a PPSAS. Then there is a polarised isomorphism from A to either the Jacobian of a genus 2 hyperelliptic curve or the product of two supersingular elliptic curve. Furthermore, two Jacobians $J(C)$ and $J(C')$ are isomorphic if and only if the curves C and C' are isomorphic, and two products are isomorphic if and only if their factors are so up to reordering.*

Proof. The first result follows from [8, Theorem 1] and Proposition 2.7. It follows from the criterion of Matsusaka-Ran [6, Theorem 14.46] that a PPSAS may not be both isomorphic to a Jacobian of a genus 2 hyperelliptic curve and to a product of supersingular elliptic curves, and that two such products are isomorphic if and only if their factors are isomorphic up to reordering. The statement on isomorphisms of Jacobians is the Torelli theorem [18, Corollary 12.2]. □

2.1.3. *The Ibukiyama-Katsura-Oort classification.* Ibukiyama, Katsura and Oort introduced a bijection between the set of polarisations on the abelian variety E_0^2 and a certain set of matrices lying in $M_2(O_0)$ [11]. We recall their main definitions and results, although we mainly follow the notations and exposition from [3, Section 2.3].

Since all superspecial abelian surfaces are isomorphic to one another, classifying principal polarisations over $A_0 = E_0^2$ up to equivalence is the same as classifying principally polarised superspecial abelian surfaces up to polarised isomorphism.

We let λ_0 be the natural product polarisation on A_0. Then, if λ is a principal polarisation on A_0, we set

$$\mu(\lambda) = \lambda_0^{-1}\lambda \in \operatorname{End}(A_0) = M_2(O_0).$$

We then have the following result.

Proposition 2.9 ([3, Theorem 2.7]). *The map μ is injective, and its image in $M_2(O_0)$ (using the identification $\operatorname{End}(E_0) \simeq O_0$) is*

$$\operatorname{Mat}(A_0) := \left\{ \begin{pmatrix} s & r \\ \bar{r} & t \end{pmatrix}, \quad s,t \in \mathbb{N}, r \in O_0, st - r\bar{r} = 1 \right\}$$

In several formulas, the principal polarisation λ may be replaced almost verbatim with $g = \mu(\lambda)$ in order to reframe computations within $M_2(O_0)$.

We cite two such cases:

Lemma 2.10. *Let λ be a principal polarisation on O_0, and let $\gamma \in M_2(O_0)$ represent an endomorphism of A_0. We then have*

$$r_\lambda(\gamma) = \mu(\lambda)^{-1}\gamma^*\mu(\lambda).$$

Let λ, λ' be principal polarisations, and let $\gamma \in M_2(O_0)$ be an endomorphism. Then γ is a polarised isogeny from (A_0, λ) to (A_0, γ') if and only if the following equation holds for some $N \in \mathbb{N}$:

$$\gamma^*\mu(\lambda')\gamma = N\mu(\lambda).$$

In particular, it is easy to recover the matrix $\mu(\lambda)$ from the data of the Rosati involution r_λ:

Lemma 2.11. *There is a polynomial-time algorithm which, given a matrix for the Rosati involution r_λ with respect to some principal polarisation λ of A_0, computes $\mu(\lambda)$.*

Proof. Let B be a basis of $M_2(O_0)$. Then, $\mu(\lambda)$ is the solution in $\mathrm{Mat}(A_0)$ of the following system of linear equations (in variable g):

$$gr_\lambda(\gamma) - \gamma^* g = 0, \quad \forall \gamma \in B.$$

Such a system can be solved in polynomial-time in $\mathbb{Q}\,\mathrm{Mat}(A_0)$, and then a solution may be rescaled to lie in $\mathrm{Mat}(A_0)$. $\square$

Remark 2.12. It follows directly from Lemma 2.10 that two principal polarisations λ and λ' on A_0 are equivalent if and only if there exists $\gamma \in GL_2(O_0)$ such that

$$\gamma^* \mu(\lambda')\gamma = \mu(\lambda).$$

This defines an equivalence relationship on $\mathrm{Mat}(A_0)$. In particular, if (A, λ_A) is any PPSAS, it is isomorphic to (A_0, λ) for some principal polarisation λ, and we write $\mu(A_0)$ for $\mu(\lambda)$. It is then understood that $\mu(A_0)$ is only defined up to equivalence in $\mathrm{Mat}(A_0)$. We call $\mu(A_0)$ the *Ibukiyama-Katsura-Oort matrix of A*.

2.2. **Computational Representations.**

2.2.1. *Principally polarised superspecial abelian surfaces.* While it is possible to give equations for superspecial abelian surfaces, it is generally preferable to represent them as either products of supersingular elliptic curves or Jacobians of hyperelliptic curves of genus 2. In both cases, the isomorphy class of the principally polarised abelian surface is precisely described by the isomorphy classes of the curves that induce it.

Recall that the isomorphy class of an elliptic curve E is described by its j-invariant, $j(E) \in k$. Likewise, the isomorphy class of a hyperelliptic curve of genus 2 is described by its Igusa invariant [12].

In both cases, knowing the invariants allows us to provide a model for the curve, and compute arithmetical operations. In general, we assume that the models used in this work are all maximal, so that every homomorphism is defined over k.

In the sequel, any PPSAS is computationally represented by either an unordered pair of j-invariants or by a projective vector of Igusa invariants.

2.2.2. *Isogenies between abelian surfaces.* Since principally polarised abelian surfaces are not directly represented as embedded projective varieties, isogenies may not simply be represented using rational functions.

We follow the definitions from [26, 1] and introduce the following definitions:

Definition 2.13. Let $\varphi\colon A \to B$ be a homomorphism between two abelian varieties defined over a finite field $\mathbb{F}_q$. An *efficient representation* of φ with respect to a given algorithm is some data $D_\varphi \in \{0,1\}^*$ such that, on input D_φ and $P \in A(\mathbb{F}_q)$, the algorithm returns the evaluation $\varphi(P)$ in polynomial time in $\mathrm{length}(D_\varphi)$ and $\log q$.

When A and B are principally polarised abelian varieties, some additional information may be required in order to relate the isogeny to the polarisations of A and B. For this reason, we also use the definition of a good representation of an isogeny, as is introduced in [1]. We add one extra piece of information to be carried, about the behaviour of the isogeny over differentials of B. The reason for this addition will be made clear in Section 6.

Definition 2.14. Let A, λ_A and λ_B be principally polarised abelian varieties defined over a finite fild $\mathbb{F}_q$. Let $\varphi\colon A \to B$ be a homomorphism. A *good representation*

of φ is a tuple $\theta, \theta^\dagger, D, \theta^*$, where θ is an efficient representation of φ, $\theta^\dagger$ is an efficient representation of $r_{\lambda_A, \lambda_B}(\varphi)$, D is an integer such that $\mathrm{Tr}(\varphi \circ r_{\lambda_A, \lambda_B}(\varphi)) \leq D$ and θ^* is a matrix representing the $\mathbb{F}_q$-linear map from $H^0(B, \Omega_B)$ to $H^0(A, \Omega_A)$ by φ with respect to any bases of these vector spaces.

We provide two examples, which will be omnipresent in the sequel:

Example 2.15. Let E_1, E_2, E_1', E_2' be supersingular elliptic curves and let $\varphi \colon E_1 \times E_2 \to E_1' \times E_2'$ be a homomorphism. This homomorphism decomposes as a matrix $(\varphi_{ij})_{1 \leq i, j \leq 2}$, where $\varphi_{ij} \in \mathrm{Hom}(E_j, E_i')$. Then, the data of efficient representations θ_{ij} respectively of the φ_{ij} is an efficient representation of φ.

Furthermore, letting λ and λ' be the product polarisations respectively on $E_1 \times E_2$ and $E_1' \times E_2'$, then as discussed in [3, Section 2.2], we have

$$r_{\lambda, \lambda'}(\varphi) = (\widehat{\varphi}_{ji}).$$

Since differentials are compatible with products of varieties, we also have that $\varphi^* = (\varphi_{ij}^*)$ as a block matrix.

Example 2.16 ((2,2)-isogenies). A $(2, 2)$-isogeny is an isogeny between abelian surfaces, whose kernel is maximally isotropic with respect to the Weil pairing, and therefore isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. If A is a principally polarised abelian surfaces, there exists formula which, given such a subgroup K, yield a polarised $(2, 2)$-isogeny as well as its codomain. There are also explicit criteria to decide whether the codomain is a Jacobian variety or a product of elliptic curves. The explicit formulas and criteria are given in [4, Section 3.2] and [10, Proposition 4 and its proof]. If (A, λ_A) and (B, λ_B) are principally polarised abelian surfaces, and $K \subset A$ is a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and B is the codomain of the $(2, 2)$ isogny with kernel K, then K is a good representation of the isogeny with kernel K.

For our purposes, we note that if $A = E_1 \times E_2$ is a product of elliptic curves, and the subgroup $K \subset A[2]$ admits generators of the form $(P, 0)$ and $(0, Q)$, then the codomain of the polarised $(2, 2)$-isogeny with kernel K is the product $E_1/P \times E_2/Q$.

Remark 2.17. Not all subgroups $K \subset A$ that are isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ are the kernel of an isogeny. Indeed, if $A = E_1 \times E_2$ is a product of elliptic curves, the subgroup $E_1[2] \times \{\infty_2\}$, for instance, is not maximally isotropic with respect to the Weil pairing.

2.2.3. *Endomorphism rings.* Throughout this work, we regularly use the phrase "known endomorphism ring" about elliptic curves and principally polarised abelian surfaces.

In order to make this statement precise, we introduce the following definition:

Definition 2.18. Let A be a abelian variety. By an *efficient representation* (resp. a *good representation*) of the endomorphism ring of A, we mean efficient representations (resp. good representations) of endoomrphisms of A that form a basis of $\mathrm{End}(A)$ as a $\mathbb{Z}$-module. We also say that the endomorphism ring of A is *weakly known* (resp. *known*) if we are given efficient representations (resp. good representations) of endomoprhism of A forming a basis of $\mathrm{End}(A)$ as a $\mathbb{Z}$-module.

It is clear that if the endomorphism ring of A is known, then it is weakly known. In the case of a supersingular elliptic curve E, it is known that, under GRH, there is an equivalence between weakly knowing and knowing the endomorphism ring.

Lemma 2.19 ([26, Theorems 8.1 and 8.3]). *Under GRH, there is a polynomial-time algorithm which takes as input a supersingular elliptic curve E with weakly known endomorphism ring and outputs a good representation of $\operatorname{End}(E)$.*

We introduce a notation for the isomorphism of endomorphism rings induced by an unpolarised isomorphism of abelian varieties:

Definition 2.20. Let $\varphi\colon A_1 \to A_2$ be an unpolarised isomorphism of abelian varities. We then define the following isomorphism of rings:

$$\varphi_*\colon \quad \begin{matrix} \operatorname{End}(A_1) & \to & \operatorname{End}(A_2) \\ f & \mapsto & \varphi \circ f \circ \varphi^{-1} \end{matrix}$$

2.3. **Some subroutines.**

Lemma 2.21. *Let E_1, E_2, E_3, E_4 be superspecial elliptic curves, and let φ be an isomorphism from $E_1 \times E_2 \to E_3 \times E_4$ represented as in Example 2.15. Then the isomorphism φ^{-1} may be computed in polynomial time.*

Proof. By [9, Corollary 4.11] and its proof, we may compute an isomorphism $\tilde{\varphi}\colon E_3 \times E_4 \to E_1 \times E_2$ such that $\varphi \circ \tilde{\varphi}$ is an automorphism of the form

$$\varphi \circ \tilde{\varphi} = \begin{pmatrix} a & \widehat{\psi} \\ \psi & d \end{pmatrix},$$

where $a, d \in \mathbb{Z}$ and $\psi\colon E_3 \to E_4$ is an isogeny. Then, by [9, Remark 5.1], we have

$$(\varphi \circ \tilde{\varphi})^{-1} = \begin{pmatrix} d & -\widehat{\psi} \\ -\psi & a \end{pmatrix}.$$

It follows that $\varphi^{-1} = \tilde{\varphi} \circ (\varphi \circ \tilde{\varphi})^{-1}$ may be computed in polynomial time. $\square$

Lemma 2.22. *Let E_1, E_2 be elliptic curves and let A be an abelian surface. Let $f\colon E_1 \times E_2 \to A$ be a $(2,2)$-isogeny, and let $P \in A$. Then a point $P \in E_1 \times E_2$ such that $f(P) = Q$ may be computed in polynomial time.*

Proof. Let $K = \operatorname{Ker}(f)$, and let $K' = f((E_1 \times E_2)[2])$. Let g be the $(2,2)$-isogeny with kernel L and codomain $E_1 \times E_2$. Then we have $f \circ g = [2]_A$. For a point $Q \in A$, compute $Q' \in A$ such that $2Q' = Q$, and then set $P = g(Q')$. $\square$

Lemma 2.23. *Let A_1, A_2 be principally polarised superspecial abelian varieties, with known Ibukiyama-Katsura-Oort matrices $\mu(A_1)$ and $\mu(A_2)$. Then, assuming the hypotheses for the KLPT2 algorithm, we may compute in polynomial time a chain $(f_i)_{0 \le i \le e}$ of $(2,2)$ isogenies $f_i\colon A_i' \to A_{i+1}'$ such that $A_0' = A_1$ and $A_{e+1}' = A_2$.*

Proof. This is a combination of Algorithms KLPT^2 and $\mathsf{MatrixToIsogeny22}$ from [3]. $\square$

Lemma 2.24. *There exists a polynomial-time algorithm which, given structure constants for two central simple $\mathbb{Q}$-algebras of degree bounded by 4 and a basis of a maximal order in each of them, computes an isomorphism between these algebras.*

Proof. This is stated for quaternion algebras in [5, Proposition 4.1], but the argument adapts readily to central simple algebras of larger, albeit bounded, degree. $\square$

Lemma 2.25. *If the endomorphism ring of A is known with basis B, the structure constants of $\operatorname{End}(A)$ with respect to its basis B may be computed in polynomial time.*

Proof. Applying the Cauchy Schwarz inequality, if $f, g \in \text{End}(A)$, we may compute a good representation of $f \circ g$ in polynomial time.

By [1, Lemma 3.2], we may compute the products $\langle f, g \rangle_A$, where f and g are either elements of B or products of elements of B. Set $B = (b_i)_{1 \leq i \leq 16}$ and fix $f, g \in B$, we may then compute the Gram matrix G of the family $B \cup f \circ g$. Since B forms a basis of $\text{End}(A)$, we may then recover the coordinates of $f \circ g$ with respect to B. Indeed, let $v = (v_i)_{1 \leq i \leq 17} \in \text{Ker}(G)$. We have

$$0 = v^t G v = \langle v_{17} f \circ g + \sum_{i=1}^{16} v_i b_i, f \circ g + \sum_{i=1}^{16} v_i b_i \rangle_A.$$

It follows that $f \circ g = \sum_{i=1}^{16} \frac{v_i}{v_{17}} b_i$. We may thus recover the coordinates of the $b_i \circ b_j$ with respect to B, i.e. the structure constants of $\text{End}(A)$ with respect to B. □

Lemma 2.26. *There is a polynomial-time algorithm which, given supersingular elliptic curves E_1 and E_2, as well as an efficient representation of $\text{End}(A)$ where $A = E_1 \times E_2$, outputs efficient representations of $\text{End}(E_1)$ and $\text{End}(E_2)$.*

Proof. We only detail the computation of $\text{End}(E_1)$, as that of $\text{End}(E_2)$ is similar. Let $f_1, \ldots, f_{16}$ be the basis of $\text{End}(A)$ such that efficient representations of the f_i are known. Then, by restricting to $E_1 \times \{\infty_2\}$ and composing with the projection map $A \to E_1$, we may deduce efficient representations of 16 endomorphisms of E_1 which generate its endomorphism ring as a $\mathbb{Z}$-module. Applying [26, Lemma 8.2], we may compute the $\langle f_i, f_j \rangle_{E_1}$, and therefore a Gram matrix of any subfamily of $(f_1, \ldots, f_{16})$. We may therefore test that a subfamily is free and extract a basis of $\text{End}(E_1)$. □

3. The computational problems

Problem 3.1 (Explicit Ibukiyama-Katsura-Oort correspondence)**.** Given a principally polarised superspecial abelian surface A, compute its Ibukiyama-Katsura-Oort representative, $\mu(A)$.

Problem 3.2 (Explicit isomorphism problem)**.** Given two principally polarised superspecial abelian surface A_1 and A_2, compute an unpolarised isomorphism $\varphi \colon A_1 \to A_2$ and its inverse φ^{-1}.

Problem 3.3 (Good Endomorphism ring computation)**.** Given a principally polarised superspecial abelian surface A, compute a good representation of its endomorphism ring.

Problem 3.4 (Effective endomorphism ring computation)**.** Given a principally polarised superspecial abelian surface A, compute a weak representation of its endomorphism ring.

Theorem 3.5. *Let (A, λ_A) be a PPSAS. Under GRH and the assumptions for applying the KLPT^2 algorithm, Problems 3.1 to 3.4 are equivalent if A is assumed to be a product of supersingular elliptic curves (and if A_1 and A_2 are assumed to be products for Problem 3.2). In the general case, Problem 3.1 and Problem 3.3 are equivalent, and furthermore, Problem 3.4 reduces to Problem 3.2 and Problem 3.2 reduces to Problem 3.1.*

Proof. The various reductions are the object of the remainder of this article. We provide diagrams indicating the location of each reduction. In these diagrams, arrows point from a problem to the problem it reduces to.

In the case where the varieties are assumed to be products of supersingular elliptic curves, the reductions are as follows:

```
┌─────────────────┐   [9, Theorem 3.2]   ┌─────────────────────┐
│  Problem 3.1    │ ◄─────────────────── │    Problem 3.2      │
│  Explicit IKO   │                      │  Explicit isomorphism│
└─────────────────┘                      └─────────────────────┘
        │                                           ▲
   Theorem 6.9                               Proposition 3.6
        ▼                                           │
┌─────────────────┐                      ┌─────────────────────────┐
│  Problem 3.3    │ ───────────────────► │      Problem 3.4        │
│ Good endomorphism│  Proposition 4.1     │ Effective endomorphism ring│
│      ring        │                      │                         │
└─────────────────┘                      └─────────────────────────┘
```
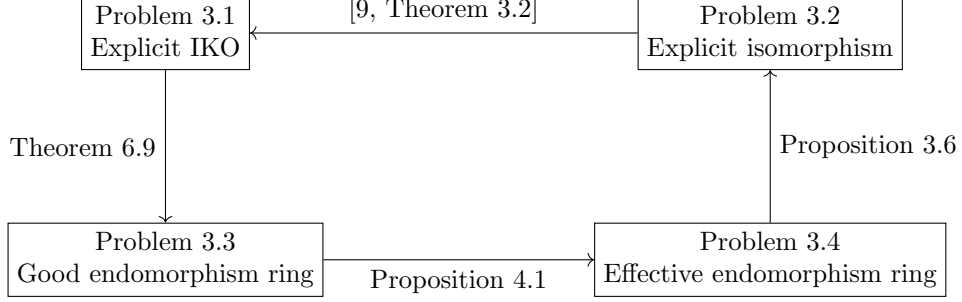
For the general case, we provide the following reductions:

```
┌─────────────────┐    Theorem 5.3    ┌─────────────────────┐
│  Problem 3.1    │ ◄──────────────── │    Problem 3.2      │
│  Explicit IKO   │                   │  Explicit isomorphism│
└─────────────────┘                   └─────────────────────┘
     │    ▲                                      ▲
 Theorem 6.9  Proposition 4.2              Proposition 3.6
     ▼    │                                      │
┌─────────────────┐                   ┌─────────────────────────┐
│  Problem 3.3    │                   │      Problem 3.4        │
│ Good endomorphism│                   │ Effective endomorphism ring│
│      ring        │                   │                         │
└─────────────────┘                   └─────────────────────────┘
```

$\square$
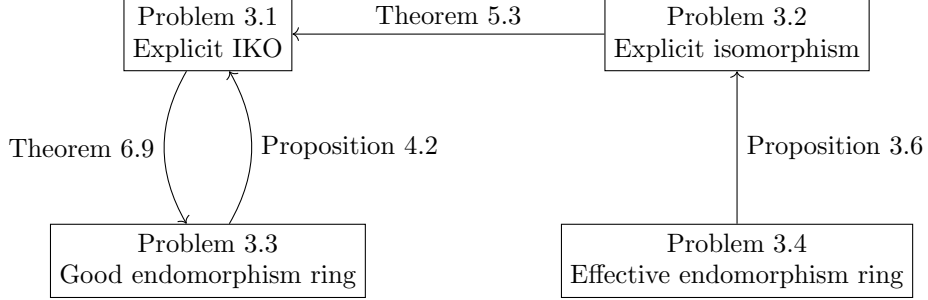
Proposition 3.6. *Problem 3.4 reduces to Problem 3.2.*

Proof. Let A be a given superspecial abelian surface. Let $\varphi\colon A_0 \to A$ be an isomorphism. Then from an efficient representation of φ and efficient representations of endomorphisms $f_1, \ldots, f_{16}$ forming a basis of $\mathrm{End}(A_0)$, we may immediately deduce efficient representations of endomorphisms $\varphi_*(f_1), \ldots, \varphi_*(f_{16})$, which form a basis of $\mathrm{End}(A)$. $\square$

4. Reductions of Endomorphism Ring Computation

We treat here two problems regarding the knowledge of the endomorphism ring of a superspecial abelian surface. If the surface is a product, we prove that good endomorphism ring computation reduces to efficient endomorphism ring computation. If the surface is a Jacobian, we instead prove a reduction to the Explicit Ibukiyama-Katsura-Oort correspondence.

4.1. **Endomorphism Ring Computation for a product of supersingular elliptic curves.** Let E_1, E_2 be supersingular elliptic curves.

For the abelian surface $A = E_1 \times E_2$ with its product polarisation. We will reduce the problem to the case of elliptic curves and then apply Lemma 2.19.

Proposition 4.1. *Under GRH, if the endomorphism ring of A is weakly known, then a good representation of it may be computed in polynomial time.*

Proof. Using Lemma 2.26, efficient representations of the endomorphism rings of E_1 and E_2 may be computed in polynomial time. Then, using Lemma 2.19, good representations of these endomorphism rings may be computed. It follows from the discussion in Example 2.15 that if the endomorphism rings of E_1 and E_2 are known, then so is the endomorphism ring of A. □

4.2. **Endomorphism Ring Computation from the Ibukiyama-Katsura-Oort matrix.**

Proposition 4.2. *Problem 3.3 reduces to Problem 3.1.*

Proof. Let A be a PPSAS, whose Ibukiyama-Katsura-Oort matrix $\mu(A)$ is knwon. By Theorem 5.3, we may compute an isomorphism $\varphi\colon A_0 \to A$. Using the proof of Proposition 3.6, we may compute a basis B of $\mathrm{End}(A)$ and efficient representations of its element, given as $\varphi_*(b_i)$, where the b_i form a basis of $\mathrm{End}(A_0)$. The Rosati involution corresponding to $\mu(A)$ may be computed using Lemma 2.10, and then carried to $\mathrm{End}(A)$. Likewise, upperbounds for the $\langle \theta(b_i), \theta(b_i) \rangle_A$ may be computed. Since φ induces an isomorphism between $H^0(A, \Omega_A)$ and $H^0(A_0, \Omega_{A_0})$, we may also use the matrices b_i^* to complete the good representations of the elements of B. □

Remark 4.3. This only guarantees that the Rosati involution computed on $\mathrm{End}(A)$ is induced by a principal polarisation which is merely equivalent to the natural polarisation on A as introduced in Example 2.4. This is not a problem, since we only represent PPSASs up to polarised isomorphism.

5. Computing unpolarised isomorphisms

In this section, we aim to prove that Problem 3.2 reduces to Problem 3.1. That is, we shall prove that if A_1, A_2 are PPSASs with known Ibukiyama-Katsura-Oort matrices, an isomorphism $\varphi\colon A_1 \to A_2$ and its inverse can be computed in polynomial time.

The case where A_1 and A_2 are products of elliptic curves is treated in [9]. The fact that an isomorphism may easily be inverted in this case is not stated, but follows directly from Lemma 2.21.

In order to complete this result, it is enough to provide a polynomial algorithm which, given a superspecial Jacobian surface A and the matrix $\mu(A)$, outputs two superspecial elliptic curves E_1 and E_2, their endomorphism rings, and an isomorphism $\varphi\colon E_1 \times E_2 \to A$. Our strategy is inspired from the technique used in proving [19, Theorem 2] (a superspecial Jacobian surface is isomorphic to a product of supersingular elliptic curves), although some work is required to make the proof computational.

Knowing the matrix $\mu(A)$, we may compute a chain of $(2,2)$-isogenies from $E_0 \times E_0$ to A. We shall work the chain one link at a time, and so we state the following lemma.

Lemma 5.1. *Let E_1, E_2 be elliptic curves with known endomorphism rings. Let $f\colon E_1 \times E_2 \to A$ be a $(2,2)$-isogeny with known kernel K. Then, assuming GRH, a pair of elliptic curves E_3, E_4, a $(2,2)$-isogeny $E_1 \times E_2 \to E_3 \times E_4$ and an unpolarised isomorphism $E_3 \times E_4 \to A$ can be computed in polynomial time.*

Proof. Let $P = (P_1, P_2)$ and $Q = (Q_1, Q_2)$ be generators of K. Since the endomorphism rings of E_1 and E_2 are known, we may compute an isogeny $f \colon E_1 \to E_2$ of odd degree [26]. Then, the isogenies f and $\widehat{f}$ act bijectively on the two-torsion sets of E_1 and E_2.

Since the ring of endomorphisms of an elliptic curve surjects onto $M_2(\mathbb{F}_2)$ when considering the action of endomorphisms on the two-torsion, it is straightforward to compute endomorphisms $\alpha_1 \in \mathrm{End}(E_1)$ and $\alpha_2(\mathrm{End}(E_2))$ such that

$$\alpha_2 \circ f(P_1) = P_2,$$
$$\alpha_2 \circ f(Q_1) = P_2 + Q_2,$$
$$\alpha_1 \circ \widehat{f}(P_2) = Q_1.$$

We set $\varphi = \alpha_2 \circ f$ and $\psi = \alpha_1 \circ \widehat{f}$.

We may then consider the unpolarised endomorphism

$$\theta = \begin{pmatrix} \mathrm{Id}_{E_1} + \psi \circ \varphi & \psi \\ \varphi & \mathrm{Id}_{E_2} \end{pmatrix}.$$

A straightforward computation shows that θ is an unpolarised automorphism with inverse

$$\theta^{-1} = \begin{pmatrix} \mathrm{Id}_{E_1} & -\psi \\ -\varphi & \mathrm{Id}_{E_2} + \varphi \circ \psi \end{pmatrix}$$

and such that $\theta(K)$ is the group generated by $(P_1, 0)$ and $(0, P_2)$.

Setting $E_3 = E_1/\langle P_1 \rangle$ and $E_4 = E_2/\langle P_2 \rangle$, we may explicitly compute the isogeny $g \colon E_1 \times E_2 \to E_3 \times E_4$ with kernel $\theta(K)$. Furthermore, since $\mathrm{Ker}(g) = \mathrm{Ker}(f \circ \theta^{-1})$, there exist an unpolarised isogeny $\tau \colon E_3 \times E_4$ such that the following diagram commutes:

We get the following diagram:

$$
\begin{array}{ccc}
E_1 \times E_2 & \xrightarrow{\ f\ } & A \\
\downarrow{\scriptstyle \theta} & & \uparrow{\scriptstyle \tau} \\
E_1 \times E_2 & \xrightarrow{\ g\ } & E_3 \times E_4
\end{array}
$$

Since $\deg(\theta) = 1$, and $\deg(f) = \deg(g) = 4$, it follows that τ is an unpolarised isomorphism.

If $P \in E_3 \times E_4$, $\tau(P)$ may be computed as $f \circ \theta^{-1}(Q)$, where Q is any preimage of P by g, which may itself be computed using Lemma 2.22. The inverse isomorphism τ^{-1} may be computed in the same manner. $\qquad\square$

Proposition 5.2. *Algorithm 1 is correct and runs in polynomial time.*

Proof. The computation in Line 1 is achieved in polynomial time by applying KLPT^2 as discussed in Lemma 2.23, using the fact that $\mu(E_0^2)$ is the identity matrix. Likewise, the number e of links in the chain is polynomial in the input. The loop invariant is satisfied by Lemma 5.1, and the invariant itself ensures both that the algorithm of Lemma 5.1 can be applied within the loop, and that the output of the algorithm is correct, considering that $A_e = A$. Finally, each iteration of the loop runs in polynomial time by the same lemma. $\qquad\square$

Theorem 5.3. *Under the assumptions for applying* KLPT^2, *Problem 3.2 reduces to Problem 3.1.*

Algorithm 1: Unpolarised isomorphism from product to Jacobian

---

Input: A superspecial Jacobian surface A
Input: Its Ibukiyama-Katsura-Oort matrix $\mu(A)$
Output: Supersingular elliptic curves E_3, E_4
Output: An unpolarised isomorphism $\tau \colon E_3 \times E_4 \to A$
Output: τ^{-1}
Output: The endomorphism rings of E_3 and E_4

1   $(A_0 \xrightarrow{f_0} A_1 \xrightarrow{f1} \ldots \xrightarrow{f_e} A_e) \leftarrow$ Chain of $(2,2)$ isogenies from E_0^2 to A ;
2   $f \leftarrow f_0$;
3   $E \leftarrow E_0$;
4   $E' \leftarrow E_0$;
5   **for** $1 \leq i \leq e$ **do**

       /* Invariant: f is a $(2,2)$-isogeny from $E \times E'$ to A_i and the
          endomorphism rings of E and E' are known.   */
       /* Apply Lemma 5.1 to f: */

6       $E, E' \leftarrow$ supersingular elliptic curves;
7       $\tau \leftarrow E \times E' \simeq A_i$;
8       $R_E, R_{E'} \leftarrow \mathrm{End}(E), \mathrm{End}(E')$;
9       $f \leftarrow f_i \circ \tau^{-1}$;
10 **end**
11 **return** $(E, E', \tau, \tau^{-1}, R_E, R_{E'})$;

Proof. Let A_1, A_2 be PPSASs, with known Ibukiyama-Katsura-Oort matrices $\mu(A_1)$ and $\mu(A_2)$. If $A_i = E_1^{(i)} \times E_2^{(i)}$ is a product of elliptic curves, we compute $\mathrm{End}(E_1^{(i)})$ and $\mathrm{End}(E_2^{(i)})$ using Lemma 2.26. Otherwise, we compute supersingular $E_1^{(i)}$ and $E_2^{(i)}$, their endomorphism rings, and an unpolarised isomorphism $E_1^{(i)} \times E_2^{(i)} \to A_i$ using Algorithm 1.

We may then apply [9, Theorem 3.2] to compute an isomorphism from $E_1^{(1)} \times E_2^{(1)} \to E_1^{(2)} \times E_2^{(2)}$, whose inverse may be computed using Lemma 2.21.

Putting everything together, this solves Problem 3.2. $\square$

6. Recovering the Ibukiyama-Katsura-Oort matrix from the endomorphism ring

In this section, we show how the Ibukiyama-Katsura-Oort matrix of a principally polarised superspecial abelian surface A may be computed from the knowledge of its endomorphism ring. Essentially, the strategy is to compute an isomorphism from $\mathrm{End}(A)$ to $M_2(O_0)$, transport the Rosati involution from $\mathrm{End}(A)$ to $M_2(O_0)$, and use it to recover the Ibukiyama-Katsura-Oort matrix. Difficulties arise as an isomorphism between endomorphism rings of superspecial abelian surfaces is not necessarily induced by an unpolarised isomorphism between the surfaces, which may lead to the computation of the wrong Rosati involution and therefore the wrong matrix. Fortunately, a "wrong" isomorphism of endomorphism rings may be identified by checking whether its action modulo p respects the action of endomorphisms on differentials, and it may then be corrected by post-composition with a fixed automorphism of A_0.

6.1. **Isomorphisms of varieties and isomorphisms of endomorphism rings.**
If $f\colon A \to A'$ is an unpolarised isomorhism of abelian varieties, it induces an
isomorphim f_* from $\mathrm{End}(A)$ to $\mathrm{End}(A')$. We show below that an isomorphism
$\mathrm{End}(A) \to \mathrm{End}(A')$ is of the form f_* if and only if it respects the so-called orien-
tations induced by A on $\mathrm{End}(A)$ and A' on $\mathrm{End}(A')$. This is a generalisation of
results on endomorphisms on supersingular elliptic curves exposed in [25, Section
42.4] and ultimately credited to Mestre and Oesterlé.

Remark 6.1. While the term *orientation* is widely used in the field of isogeny-based
cryptography to mean an embedding of a quadratic number ring into a quaternion
order, it refers here to a widely different notion and there should be no confusion
between the two. We keep the term "orientation" so that our exposition mirrors
that of [25, Section 42.4] better.

Remark 6.2. The focus of our work is superspecial abelian surfaces. Most of the
theory of orientations that we develop below is however valid in arbitrary dimension
greater than 1. For the sake of simplicity, we state the results for surfaces only.

We clarify this strategy with the following lemma:

Lemma 6.3. *Let A, A' be abelian varieties such that there exists an unpolarised
isomorphism $\varphi_0\colon A' \to A$. Then, for any unpolarised isomorphism, $\varphi\colon A \to A'$,
the induced automorphism $(\varphi_0)_* \circ \varphi_*$ of $\mathrm{End}(A)$ is inner.*

Proof. This is clear as $(\varphi_0)_* \circ \varphi_* = (\varphi_0 \circ \varphi)_*$ is the inner automorphism of $\mathrm{End}(A)$
induced by $\varphi_0 \circ \varphi$. $\square$

Below, we prove that the converse is true. We also show that the group of outer
automorphisms of $\mathrm{End}(A)$ has order two, and we provide an explicit criterion for
an isomorphism of endomorphism rings to be induced by an isomorphism of abelian
varieties.

6.1.1. *Orientations.*

Definition 6.4. Let R be a ring isomorphic to a maximal order in $M_2(B_{p,\infty})$.
An *orientation* of R is a surjective homomorphism $\zeta\colon R \to M_2(\overline{\mathbb{F}_q})$ such that
$\mathrm{Ker}(\zeta) = P$, where P is the intersection of R and the unique two-sided ideal of
R_p (see [21, Theorem 18.3]).
  Two orientations ζ and ζ' are *equivalent*, denoted by $\zeta \sim \zeta'$, if $\det \circ \zeta = \det \circ \zeta'$.
  An *oriented maximal order* is the data of a ring R as above, together with
an equivalence class of orientations. An *isomorphism of oriented maximal orders*
$\varphi\colon (R, [\zeta]) \to (R', [\zeta'])$ is then a ring isomorphism from R to R' such that $\zeta \sim \zeta' \circ \varphi$.
We also say that a ring isomorphism is *oriented* if it is an isomorphism of oriented
maximal orders, when the orientations are clear from context.

  The facts we state below about the ideal P are stated in [21, Chapter 5].
  Let R be as in Definition 6.4. There are exactly two classes of orientations on
R, and they are related in a straightforward manner by any outer automorphism
of R, which we describe in the two lemmas below.
  We write $\mathrm{Aut}(R)$ for the group of automorphisms of R, $\mathrm{Inn}(R)$ for the group
of inner automorphisms of R and $\mathrm{Out}(R)$ for the group $\mathrm{Aut}(R)/\mathrm{Inn}(R)$ of *outer
automorphisms* of R.

Lemma 6.5. *The group $\mathrm{Out}(R)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Its non-trivial class contains, in particular, any automorphism defined as conjugation by a generator of P as a left ideal.*

Proof. Since $M_2(B_{p,\infty})$ has discriminant p^2, [21, Corollary 37.32] implies that the Picard group of R has order 2, and is generated by P as a two-sided ideal. Since the class group of R is trivial [11, Theorem 2.1], it then follows from [21, Corollary 37.34] that $\mathrm{Out}(R) \simeq \mathrm{Pic}(R)$ and therefore has order 2. To avoid any confusion, we direct the attention of the reader to the fact that the ring that we call R is denoted by Λ in [21], while the ring denoted there by R is simply $\mathbb{Z}$ in our case.

Now, since all maximal orders in $M_2(B_{p,\infty})$ are isomorphic (this follows from [21, Theorem 21.6 and Theorem 27.8] together with the fact that the class group of R is trivial), we may assume that $R = M_2(O)$, where O is a maximal order of $M_2(B_{p,\infty})$ containing some j such that $\mathrm{nrd}(j) = p$. Then, by the discussion aboce [25, Corollary 42.4.12], conjugation by j induces an outer automorphism of O, and therefore conjugation by jI_2 induces an outer automorphism of R. It is clear in this case that jI_2 is a generator of P as a left ideal. $\qquad\square$

Lemma 6.6. *Let R be as in Definition 6.4. There are exactly 2 equivalence classes of orientations on R. If $f \in \mathrm{Aut}(R)$ and ζ is an orientation of R, then $\zeta \sim \zeta \circ f$ if and only if $f \in \mathrm{Inn}(R)$.*

Proof. By definition, an orientation ζ factors through the map $\pi\colon R \to R/P \simeq M_2(\mathbb{F}_q)$. Since an orientation is surjective, it is fully described by the choice of an automorphism φ of $M_2(\mathbb{F}_q)$, through the relation $\zeta = \varphi \circ \pi$. Such an automorphism φ factors uniquely as $\iota \circ \sigma^\varepsilon$, where $\iota \in \mathrm{Inn}(M_2(\mathbb{F}_{p^2}))$, σ is induced by the non-trivial automorphism of $\mathbb{F}_{p^2}$ and $\varepsilon \in \{0,1\}$. It is clear that two orientations are equivalent if and only if the ε variables as they appear in their representations as above are equal.

If $u \in R^\times$, and ι_u the inner automorphism of R induced by u, we have $\zeta \circ \iota_u\colon a \mapsto \zeta(u)\zeta(a)\zeta(u)^{-1}$, and therefore $\zeta \sim \zeta \circ \iota_u$. Conversely, if $f \in \mathrm{Aut}(R) \setminus \mathrm{Inn}(R)$, we identify R with $M_2(O)$ as in the proof of Lemma 6.5. Then, we may assume that f is conjugation by jI_2, which induces the Galois conjugation on $R/P \simeq M_2(\mathbb{F}_{p^2})$. It is then clear that $\zeta \not\sim \zeta \circ f$. $\qquad\square$

6.1.2. *Orientations and superspecial abelian surfaces.* Let A be a superspecial abelian surface, so that $\mathrm{End}(A)$ is isomorphic to a maximal order in $M_2(B_{p,\infty})$. We define an orientation on $\mathrm{End}(A)$ induced by A using the action of endomorphisms of A on its space of global differentials $H^0(A, \Omega_A)$.

Recall that the space $D(A) \coloneqq H^0(A, \Omega_{A/\mathbb{F}_q})$ is a 2 dimensional $\mathbb{F}_q$-vector space. An endomorphism of A acts on $D(A)$ as a pullback map f^*. It follows that a choice of basis of $H^0(A, \Omega_A)$ yields a map

$$\zeta_A\colon \quad \begin{aligned} \mathrm{End}(A) &\to M_2(\mathbb{F}_q) \\ f &\mapsto f^*. \end{aligned}$$

The map ζ_A is well defined up to post-composition by an inner automorphism of $M_2(\mathbb{F}_q)$, which is enough to give $\mathrm{End}(A)$ a natural structure of oriented maximal order, after we prove the following lemma.

Lemma 6.7. *The map ζ_A defined above induces an orientation of the order R_A identified with $\mathrm{End}(A)$.*

Proof. We must check that the ring homomorphism ζ_A is surjective, and that it kills endomorphisms with degree divisible by p.

Since polarisations are uninvolved in this result, we may assume that $A = E^2$ is a product of supersingular elliptic curves. Then we may identify $\mathrm{End}(A)$ with $M_2(\mathrm{End}(E))$, and $D(A) = D(E)^2$. Now, let ζ_E be the map $\mathrm{End}(E) \to \mathbb{F}_q$ induced by the action of $\mathrm{End}(E)$ on $D(E)$. It is clear that the matrix $(f_{ij})_{1 \leq i,j \leq 2} \in M_2(\mathrm{End}(E))$ acts on $D(A)$ as the matrix $(f_{ij}^*)_{1 \leq i,j \leq 2}$. In particular, the map ζ_A is surjective.

Furthermore, if an endomorphism of $\mathrm{End}(A)$ lying in P, is written as a matrix of isogenies, each of its component is inseparable. Indeed, they all have degree divisible by p and are therefore inseparable because the curve E is supersingular. Then, it is known that such isogenies act as zero on the global differentials of E (see [24, Corollary 5.6.(c)]), and therefore f as a whole acts as 0 on all global differentials of A. $\qquad\square$

The point of introducing orientations is that, as in the genus 1 case, isomorphisms of varieties induce isomorphisms of oriented endomorphism rings:

Theorem 6.8. *Let A, A' be superspecial abelian surfaces, and let $\tau\colon \mathrm{End}(A) \to \mathrm{End}(A')$ be an isomorphism of rings.*

Then there exists some unpolarised isomorphism $\varphi\colon A \to A'$ such that $\tau = \varphi_*$ if and only if τ is a morphism of oriented maximal orders from $\mathrm{End}(A), \zeta_A$ to $\mathrm{End}(A'), \zeta_{A'}$.

Proof. Let $\varphi\colon A \to A'$ be an isomorphism, and consider the isomorphism $\varphi^*\colon D(A') \to D(A)$. It is clear from the definitions that if $f \in \mathrm{End}(A)$, then

$$\zeta_{A'} \circ \varphi_*(f) = (\varphi^{-1})^* \circ \zeta_A(f) \circ \varphi^*.$$

It follows that the isomorphism φ_* is oriented as required.

Let $\tau\colon \mathrm{End}(A) \to \mathrm{End}(A')$ be a non-oriented isomorphism. Now, fix an isomorphism $\varphi_0\colon A' \to A$ and set $\tau_0 = (\varphi_0)_*$ the induced morphism of oriented maximal orders. Since τ_0 is oriented, it follows that $\tau_0 \circ \tau$ is not, as clearly the composition of two oriented isomorphisms is itself oriented. By Lemma 6.6, it follows that $\tau_0 \circ \tau$ is not an inner automorhism of $\mathrm{End}(A)$. By Lemma 6.3, it follows that τ is not induced by any isomorphism of abelian varieties.

$\qquad\square$

6.2. **The reduction.** We may now state the reduction from Problem 3.1 to Problem 3.3. We let ζ_0 be the orientation of $M_2(O_0)$ induced by A_0. We also let $\pi \in M_2(O_0)$ be a generator of the right ideal $P_0 = \{a \in M_2(O_0) \colon p \mid \mathrm{nrd}(a)\}$.

Theorem 6.9. *Assuming GRH, Algorithm 2 is correct and runs in polynomial time.*

Proof. We first prove that the theorem runs in polynomial time. Since there are no loops or recursive calls, we only need to check that each line runs in polynomial time. Lines 2, 5 and 7 are straightforward computations involving linear algebra over $\mathbb{Q}$. As the inputs for these computations are either part of the input of the algorithm or outputs of other lines, these lines may be executed in polynomial time if the rest of the algorithm does as well. The problem in Line 1 may be solved using Lemmas 2.24 and 2.25. The problem in Line 3 is an instance of a principal ideal problem, which is solved by [20, Theorem 3.13]. The only difficulty in Line

---

Algorithm 2: Computing the Ibukiyama-Katsura-Oort matrix from the endomorphism ring

---

Input: A superspecial abelian surface A with known endomorphism ring
Output: The Ibukiyama-Katsura-Oort matrix $\mu(A)$

1 $\tau \leftarrow$ isomorphism from $\mathrm{End}^0(A)$ to $M_2(B_{p,\infty})$;

2 $R \leftarrow \tau(\mathrm{End}(A))$;

3 $\gamma \leftarrow$ generator of the right $M_2(O_0)$-ideal $RM_2(O_0)$;

4 if $\exists b \in \mathrm{End}(A) \mid \det(\zeta_A(b)) \neq \det(\zeta_{A_0}(\gamma^{-1}\tau(b)\gamma))$ **then**

5 $\quad \gamma \leftarrow \gamma\pi$;

6 end

7 $\sigma \leftarrow \begin{pmatrix} M_2(B_{p,\infty}) & \to & M_2(B_{p,\infty}) \\ \alpha & \mapsto & \gamma^{-1}(\tau \circ r_A \circ \tau^{-1})(\gamma\alpha\gamma^{-1})\gamma \end{pmatrix}$;

8 Compute $g \in Mat(A_0)$ corresponding to the involution σ;

9 return g;

---

4 would be to compute ζ_A, but it is known since good representations of the basis elements of $\mathrm{End}(A)$ are known. Finally, the computation in Line 8 may be done using Lemma 2.11.

Now, the ideal $I = RM_2(O_0)$ is both a right $M_2(O_0)$-ideal and a left R-ideal. If γ is a generator of I as a right $M_2(O_0)$-ideal, then for any $a \in R$ and $b \in M_2(O_0)$, we have $a\gamma b = \gamma c$ for some $c \in M_2(O_0)$. Since R is a maximal order, it follows that $R = \gamma M_2(O_0)\gamma^{-1}$, and that conjugation by γ induces an isomorphism between the two rings.

Therefore, the map $b \mapsto \gamma^{-1}\tau(b)\gamma$ is an isomorphism from $\mathrm{End}(A)$ to $M_2(O_0) = \mathrm{End}(A_0)$. It then follows from Lemmas 6.5 and 6.6 that after Line 6, the map $b \mapsto \gamma^{-1}\tau(b)\gamma$ is an oriented isomorphism. By Theorem 6.8, there is an unpolarised isomorphism $\varphi \colon A \to A_0$ such that for all $b \in \mathrm{End}(A)$, $\varphi_*(b) = \gamma^{-1}\tau(b)\gamma$. Now, let $\lambda = \widehat{\varphi^{-1}} \circ \lambda_A \circ \varphi^{-1}$ be the polarisation on A_0 such that φ is a polarised isomorphism from (A, λ_A) to (A_0, λ). It is straightforward to check that the map σ computed in Line 7 is in fact the Rosati involution r_λ, and that the algorithm therefore outputs $\mu(\lambda) = \mu(A)$. $\qquad\square$

REFERENCES

[1] Samuele Anni, Gaetan Bisson, Annamaria Iezzi, Elisa Lorenzo García, and Benjamin Wesolowski. On the computation of endomorphism rings of abelian surfaces over finite fields. Preprint, arXiv:2503.08925 [math.NT] (2025), 2025.

[2] Wouter Castryck and Thomas Decru. An efficient key recovery attack on sidh. In *Annual international conference on the theory and applications of cryptographic techniques*, pages 423–447. Springer, 2023.

[3] Wouter Castryck, Thomas Decru, Péter Kutas, Abel Laval, Christophe Petit, and Yan Bo Ti. Klpt 2: algebraic pathfinding in dimension two and applications. In *Annual International Cryptology Conference*, pages 167–200. Springer, 2025.

[4] Wouter Castryck, Thomas Decru, and Benjamin Smith. Hash functions from superspecial genus-2 curves using richelot isogenies. *Journal of Mathematical Cryptology*, 14(1):268–292, 2020.

[5] Tímea Csahók, Péter Kutas, Micka ël Montessinos, and Gergely Zábrádi. Explicit isomorphisms of quaternion algebras over quadratic global fields. *Res. Number Theory*, 8(4):24, 2022. Id/No 77.

[6] Bas Edixhoven, Gerard van der Geer, and Ben Moonen. Abelian varieties. `http://van-der-geer.nl/~gerard/AV.pdf`. Last consulted on 08/01/2026.

[7] Kirsten Eisenträger, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit. Supersingular isogeny graphs and endomorphism rings: reductions and solutions. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 329–368. Springer, 2018.

[8] E Victor Flynn and Yan Bo Ti. Genus two isogeny cryptography. In *International Conference on Post-Quantum Cryptography*, pages 286–306. Springer, 2019.

[9] Pierrick Gaudry, Julien Soumier, and Pierre-Jean Spaenlehauer. Computing isomorphisms between products of supersingular elliptic curves, 2025.

[10] Everett W. Howe, Franck Leprévost, and Bjorn Poonen. Large torsion subgroups of split Jacobians of curves of genus two or three. *Forum Math.*, 12(3):315–364, 2000.

[11] Tomoyoshi Ibukiyama, Toshiyuki Katsura, and Frans Oort. Supersingular curves of genus two and class numbers. *Compos. Math.*, 57:127–152, 1986.

[12] Jun-Ichi Igusa. Arithmetic variety of moduli for genus two. *Annals of Mathematics*, 72(3):612–649, 1960.

[13] 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. *Compos. Math.*, 154(5):934–959, 2018.

[14] David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol. On the quaternion-isogeny path problem. *LMS Journal of Computation and Mathematics*, 17(A):418–432, 2014.

[15] 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*, pages 448–471. Springer, 2023.

[16] Arthur Herlédan Le Merdy and Benjamin Wesolowski. Unconditional foundations for super-singular isogeny-based cryptography. Cryptology ePrint Archive, Paper 2025/271, 2025.

[17] J. S. Milne. *Arithmetic Geometry*, chapter Abelian Varieties, pages 103–150. Springer-Verlag, New York, 1984.

[18] J. S. Milne. *Arithmetic Geometry*, chapter Jacobian Varieties, pages 167–212. Springer-Verlag, New York, 1984.

[19] Frans Oort. Which abelian surfaces are products of elliptic curves? *Math. Ann.*, 214:35–47, 1975.

[20] Aurel Page, Damien Robert, and Julien Soumier. On the conversion of module representations for higher dimensional supersingular isogenies. (in preparation).

[21] Irving Reiner. *Maximal orders*, volume 5 of *Lond. Math. Soc. Monogr.* Academic Press, London, 1975.

[22] Damien Robert. Breaking sidh in polynomial time. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 472–503. Springer, 2023.

[23] Damien Robert. The module action for isogeny based cryptography. Cryptology ePrint Archive, Paper 2024/1556, 2024.

[24] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Grad. Texts Math.* New York, NY: Springer, 2nd ed. edition, 2009.

[25] John Voight. *Quaternion algebras*, volume 288 of *Grad. Texts Math.* Cham: Springer, 2021.

[26] Benjamin Wesolowski. The supersingular isogeny path and endomorphism ring problems are equivalent. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1100–1111, 2022.

ELTE, Faculty of Informatics, H-1053 Budapest, Egyetem tér 1-3, Hungary
Email address: `mickael@montessinos.fr`